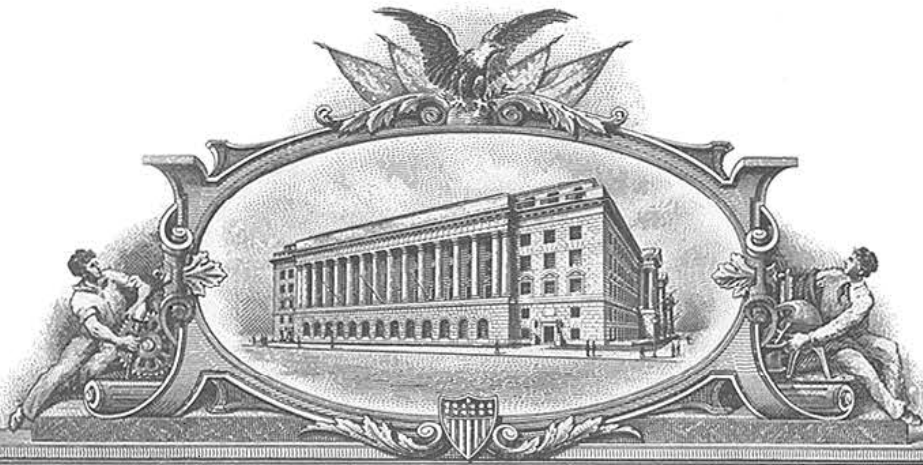


8170010



# THE UNITED STATES OF AMERICA

**TO ALL TO WHOM THESE PRESENTS SHALL COME:**

UNITED STATES DEPARTMENT OF COMMERCE

United States Patent and Trademark Office

*October 19, 2021*

**THIS IS TO CERTIFY THAT ANNEXED IS A TRUE COPY FROM THE RECORDS OF THIS OFFICE OF THE FILE WRAPPER AND CONTENTS OF:**

**APPLICATION NUMBER:** *11/104,202*  
**FILING DATE:** *April 12, 2005*  
**PATENT NUMBER:** *7565695*  
**ISSUE DATE:** *July 21, 2009*



Certified by

Performing the Functions and Duties of the  
Under Secretary of Commerce  
for Intellectual Property  
and Director of the United States  
Patent and Trademark Office

041205  
1/638 U.S. PTO

**Attorney Docket No. WEBR-011/00US**

**PATENT**

Express Mail Label Number: EV459983512US  
Date of Deposit: April 12, 2005

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as Express Mail in an envelope addressed to the Mail Stop Patent Application, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on April 12, 2005.

By: \_\_\_\_\_

Daxmara Sanchez

**Mail Stop Patent Application**  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

113261 U.S. PTO  
11/104202  
041205

### UTILITY PATENT APPLICATION TRANSMITTAL

Transmitted herewith for filing is a U.S. Non-Provisional Utility Patent Application entitled: "SYSTEM AND METHOD FOR DIRECTLY ACCESSING DATA FROM A DATA STORAGE MEDIUM"

naming as inventor(s): Michael Burtscher

and including:

- (13) pages of description (before the claims);
- (05) pages of claims ((17) total claims; (03) independent claims);
- One (1) Sheet of Abstract;
- (03) sheets of drawing(s) including Figures 1-3.

1. Also enclosed are:

- Executed Declaration
- Application Data Sheet
- Executed Assignment and Assignment Recordation Cover Sheet
- Executed Power by Assignee
- Assertion of Entitlement to Small Entity Status
- Information Disclosure Statement
- Preliminary Amendment
- CD-ROM or CD-R in duplicate, large table or Computer Program (Appendix)
- Nucleotide and/or Amino Acid Sequence Submission
  - Computer Readable Form (CRF) on 3 1/2" floppy disk
  - Specification Sequence Listing on:
    - CD-ROM or CD-R (2 copies); or
    - paper

The content of the copy in computer readable form is identical to the content of the paper, CD-ROM, or CD-R copy of the Sequence Listing.

Nonpublication Request and Certification

Check No. XXX in the amount of \$XXX for the total fee as calculated below

Return receipt postcard

Other: XXX

2.  Please amend the specification by inserting before the first heading the following paragraph:

This application claims priority under 35 U.S.C. §§119 and/or 365 to \_\_\_ filed in \_\_\_ on \_\_\_, the entire content of which is hereby incorporated by reference.

A certified copy of the priority application  is enclosed  will follow.

3.  Please amend the specification by inserting before the first heading the following paragraph:

This application claims priority under 35 U.S.C. §119(e) to U.S. Provisional Application No. \_\_\_, filed \_\_\_, the entire content of which is hereby incorporated by reference.

4.  Please amend the specification by inserting before the first heading the following paragraph:

This application is a \_\_\_ of and claims priority under 35 U.S.C. §120 of U.S. Patent Application No. \_\_\_, filed \_\_\_, the entire contents of which are hereby incorporated by reference.

5. The filing fee has been calculated as follows  and in accordance with the enclosed preliminary amendment:

|  | NO. OF CLAIMS |        | EXTRA CLAIMS | RATE       | FEE               |
|--|---------------|--------|--------------|------------|-------------------|
| Basic Application Fee (includes Basic Filing Fee, Search and Examination Fees)                           |               |        |              |            | \$1,000.00        |
| Total Claims   | 17            | - 20 = | 0            | x \$50.00  | \$50.00           |
| Independent Claims   | 03            | - 3 =  | 0            | x \$200.00 | \$200.00          |
| If multiple dependent claims are presented, add \$360.00   |               |        |              |            | 0                 |
| Total Application Fee  |               |        |              |            | \$1,250.00        |
| If an Assertion of Entitlement to Small Entity Status is enclosed, subtract 50% of Total Application Fee |               |        |              |            | 0                 |
| Other fees: (specify)  |               |        |              |            | 0                 |
| <b>TOTAL FEE DUE</b>   |               |        |              |            | <b>\$1,250.00</b> |

- This application is being filed without a filing fee. Issuance of a Notice to File Missing Parts of Application is respectfully requested.
- A check for the total fee is attached.
- Please charge \$1,250.00 to Deposit Account No. 50-1283 for the total fee. This paper is being submitted in duplicate.
- The Commissioner is hereby authorized to charge any appropriate fees under 37 C.F.R. §§1.16, 1.17, and 1.21 that may be required by this paper, and to credit any overpayment, to Deposit Account No. 50-1283.

6. Please direct all correspondence concerning this application to:


Cooley Godward LLP  
ATTN: Patent Group  
One Freedom Square  
Reston Town Center  
11951 Freedom Drive  
Reston, VA 20190-5656  
Tel: (703) 456-8000 or (720) 566-4035  
Fax: (703) 456-8100 or (720) 566-4099

CUSTOMER NUMBER: **22903**

Cooley Godward LLP  
ATTN: Patent Group  
One Freedom Square  
Reston Town Center  
11951 Freedom Drive  
Reston, VA 20190-5656  
Tel: (703) 456-8000 or (720) 566-4035  
Fax: (703) 456-8100 or (720) 566-4099

Respectfully submitted,  
**COOLEY GODWARD LLP**

By:

A handwritten signature in black ink, appearing to read 'S. O'Dowd', written over a horizontal line.

Sean R. O'Dowd, Esq.  
Reg. No. 53,403

COOLEY GODWARD LLP  
ATTORNEY DOCKET No.: WEBR-011/00US  
CLIENT No.: 303666-2011

EXPRESS MAIL NO. EV459983512US

**APPLICATION FOR PATENT**

**TITLE:           SYSTEM AND METHOD FOR DIRECTLY ACCESSING DATA FROM A DATA  
STORAGE MEDIUM**

**RELATED APPLICATIONS**

[0001] The present application is related to the following commonly owned and assigned applications: application no. (unassigned), Attorney Docket No. WEBR-002/00US, entitled *System and Method for Monitoring Network Communications for Pestware*; application no. (unassigned), Attorney Docket No. WEBR-003/00US, entitled *System and Method For Heuristic Analysis to Identify Pestware*, application no.(unassigned), Attorney Docket No. WEBR-005/00US, entitled *System and Method for Pestware Detection and Removal*, and application no. (unassigned), Attorney Docket No. WEBR-011/00US, filed herewith, entitled *System and Method for Directly Accessing Data From a Data Storage Medium* each of which is incorporated by reference in their entirety.

**COPYRIGHT**

[0002] A portion of the disclosure of this patent document contains material that is subject to copyright protection. The copyright owner has no objection to the facsimile reproduction by anyone of the patent disclosure, as it appears in the Patent and Trademark Office patent files or records, but otherwise reserves all copyright rights whatsoever.

**FIELD OF THE INVENTION**

[0003] The present invention relates to computer system management. In particular, but not by way of limitation, the present invention relates to systems and methods for controlling pestware or malware.

**BACKGROUND OF THE INVENTION**

[0004] Personal computers and business computers are continually attacked by trojans, spyware, and adware, collectively referred to as “malware” or “pestware.” These types of programs generally act to gather information about a person or organization—often without the person or organization’s knowledge. Some pestware is highly malicious. Other pestware is non-malicious but may cause issues with privacy or system performance. And yet other pestware is actual beneficial or wanted by the user. Wanted pestware is sometimes not characterized as “pestware” or “spyware.” But, unless specified otherwise, “pestware” as used herein refers to any program that collects and/or reports information about a person or an organization and any “watcher processes” related to the pestware.

[0005] Software is available to detect pestware, but scanning a system for pestware typically requires a system to look at files stored in a data storage device (e.g., disk) on a file by file basis. This process of scanning files is frequently time consuming, and as a consequence, users must wait a substantial amount of time to find out the results of a system scan. Even worse, some users elect not to perform a system scan because they do not want to, or cannot, wait for a scan to be completed. Accordingly, current software is



not always able to scan and remove pestware in a convenient manner and will most certainly not be satisfactory in the future.

### **SUMMARY OF THE INVENTION**

[0006] Exemplary embodiments of the present invention that are shown in the drawings are summarized below. These and other embodiments are more fully described in the Detailed Description section. It is to be understood, however, that there is no intention to limit the invention to the forms described in this Summary of the Invention or in the Detailed Description. One skilled in the art can recognize that there are numerous modifications, equivalents and alternative constructions that fall within the spirit and scope of the invention as expressed in the claims.

[0007] Embodiments of the present invention include systems methods for scanning files for pestware on a protected computer. One embodiment is configured to identify a location of each of at least a first file, a second file and a third file in a file storage device of the protected computer, and retrieve, while substantially circumventing an operating system of the protected computer, information from at least the first file. In this embodiment, the information from the first file is analyzed to determine whether the first file is a potential pestware file. In variations, the operating system is also circumvented while the locations of the first, second and third files are identified.

[0008] In another embodiment, the invention may be characterized as a system for managing pestware, which includes a pestware detection module configured to detect

pestware on a protected computer. The protected computer in this embodiment includes at least one file storage device and a program memory. The protected computer also includes a sweep speedup module, which is configured to identify, while substantially circumventing an operating system of the protected computer, a location of each of a plurality of files in the at least one file storage device of the protected computer, and to retrieve information from each of the plurality of files. The information is analyzed by the pestware detection module so as to determine whether any of the plurality of files are potential pestware files. In variations, the operating system of the protected computer is also circumvented while the information from each of the plurality of files is retrieved. These and other embodiments are described in more detail herein.

### **BRIEF DESCRIPTION OF THE DRAWINGS**

[0009] Various objects and advantages and a more complete understanding of the present invention are apparent and more readily appreciated by reference to the following Detailed Description and to the appended claims when taken in conjunction with the accompanying Drawings where like or similar elements are designated with identical reference numerals throughout the several views and wherein:

FIGURE 1 illustrates a block diagram of a protected computer in accordance with one implementation of the present invention;

FIGURE 2 is a flowchart of one method for accessing information from a plurality of files in accordance with an embodiment of the present invention; and

FIGURE 3 is a flowchart of a method for enumerating and accessing information from the plurality of files while circumventing the operating system of the protected computer in accordance with another embodiment of the present invention.

### **DETAILED DESCRIPTION**

[0010] According to several embodiments, the present invention decreases the amount of time required to retrieve information from files stored in a computer system's storage device (e.g., hard drive).

[0011] In prior art computer systems, when a file is accessed (e.g., to retrieve information from the files), the computer's operating system is typically utilized to access the file. The operating system, however, typically performs several logistical operations before and/or while accessing a particular file. For example, before a typical operating system accesses a file, the operating system checks to make sure that accessing the file does not violate any established security provisions. In addition, the operating system must make sure the file is not already in use, and if it is, the operating system typically denies access to the file. And once the operating system does access a file, it flags the file so that it cannot be subsequently accessed while it is in use.

[0012] Although these logistical operations may be unnoticeable when just a few files are accessed, when several files are accessed, the logistical operations, in aggregate, take a substantial amount of time to carry out, and as a consequence, become very noticeable to the user.

[0013] In addition, when a user desires to perform a general scan of a collection of files (e.g., for pestware), prior art scanning software typically utilizes the operating system to enumerate (i.e., identify) each file in the collection of files to be scanned. Once the files are enumerated, the prior art scanning software then accesses, utilizing the operating system, each enumerated file, file by file, in the order the files are enumerated by the operating system.

[0014] Unfortunately, the order in which typical operating systems enumerate files may be determined by the directory tree that the files are organized by instead of the physical location of the files in the computer system's file storage device. In the context of a disk drive for example, the order in which files are enumerated may have very little, if any, relation to the location of the files on the disk. As a consequence, the head of a disk drive may have to move across opposite ends of the disk surface to access two files that were juxtaposed in the list of files enumerated by the operating system.

[0015] Although the time it takes the head to jump between two disparate locations on a disk surface to access two enumerated files may be insignificant, when several enumerated files (e.g., several hundred or thousand files) are accessed, the amount of time required for the disk heads to traverse the disk surface, in aggregate, is substantial.

[0016] Referring first to FIGURE 1, shown is a block diagram 100 of a protected computer/system in accordance with one implementation of the present invention. The term "protected computer" is used herein to refer to any type of computer system,

including personal computers, handheld computers, servers, firewalls, etc. This implementation includes a CPU 102 coupled to memory 104 (e.g., random access memory (RAM)), a file storage device 106, ROM 108 and network communication 110.

[0017] As shown, the storage device 106 provides storage for a collection of  $N$  files 124, which includes a pestware file 126. The storage device 106 is described herein in several implementations as hard disk drive for convenience, but this is certainly not required, and one of ordinary skill in the art will recognize that other storage media may be utilized without departing from the scope of the present invention. In addition, one of ordinary skill in the art will recognize that the storage device 106, which is depicted for convenience as a single storage device, may be realized by multiple (e.g., distributed) storage devices.

[0018] As shown, an anti-spyware application 112 includes a detection module 114, a shield module 116, a removal module 118 and a sweep speedup module 120, which are implemented in software and are executed from the memory 104 by the CPU 102. In addition, an operating system 122 is also depicted as running from memory 104.

[0019] The software 112 can be configured to operate on personal computers (e.g., handheld, notebook or desktop), servers or any device capable of processing instructions embodied in executable code. Moreover, one of ordinary skill in the art will recognize that alternative embodiments, which implement one or more components (e.g., the anti-spyware 112) in hardware, are well within the scope of the present invention.

[0020] In the present embodiment, the operating system 122 is not limited to any particular type of operating system and may be operating systems provided by Microsoft Corp. under the trade name WINDOWS (e.g., WINDOWS 2000, WINDOWS XP, and WINDOWS NT). Additionally, the operating system may be an open source operating system such operating systems distributed under the LINUX trade name. For convenience, however, embodiments of the present invention are generally described herein with relation to WINDOWS-based systems. Those of skill in the art can easily adapt these implementations for other types of operating systems or computer systems.

[0021] In accordance with some embodiments of the present invention, the sweep speedup module 120 expedites the scanning of the  $N$  files 124 for pestware (e.g., the pestware file 126) in the data storage device 106 by scanning the files 124 according to their physical location in the data storage device 106 instead of the order the files are enumerated by the operating system. In this way, the time required for the mechanism(s) within the file storage device (e.g., a disk head) to access each file is substantially reduced.

[0022] In other embodiments, as discussed further with reference to FIGURE 3, the sweep speedup module 120 expedites the scanning of the  $N$  files 124 for pestware (e.g., the pestware file 126) in the data storage device 106 by circumventing the operating system 122 and directly accessing the files in the data storage device.

[0023] In yet other embodiments, the sweep speedup module 120 both directly accesses the data storage device 106 to locate and identify files in the data storage device 120 and accesses the files according to their location in the data storage device so as to further expedite the scanning of the  $N$  files 124 for any pestware.

[0024] Referring next to FIGURE 2, shown is a flowchart depicting steps traversed in accordance with a method for accessing files in the data storage device 106 according to the files physical location. Initially, the name of each of the  $N$  files 124 that are in the data storage device 106 are identified (Blocks 202, 204). In addition, the location of each of the  $N$  files within the data storage device 106 is also identified (Block 206). In some embodiments, the operating system 122 is utilized to both enumerate and identify the locations of the  $N$  files 124. In other embodiments, however, the names and locations of the  $N$  files 124 are identified by directly accessing the data storage device as discussed further herein with reference to FIGURE 3.

[0025] As shown, a listing of the names and locations of the  $N$  files 124 is then saved (Block 208), and the stored listing of the  $N$  files 124 is sorted by the physical location of the  $N$  files 124 (Block 210). In the case where the physical storage device 106 is a disk drive, for example, the  $N$  files 124 are sorted by the cluster numbers of the files.

[0026] After the  $N$  files 124 are sorted so as to generated a sorted listing of the  $N$  files 124, information is retrieved from each of the  $N$  files 124, file-by-file, in accordance with the sorted listing (Block 212). For example, information may be retrieved from the  $N$

files 124 by accessing them in a sequential manner starting at either the top or the bottom of the sorted list. In this way, each file that is accessed is in close proximity to the file previously accessed. As a consequence, the time required to retrieve information from the  $N$  files 124 is substantially reduced relative to accessing the  $N$  files 124 in accordance with the location of the  $N$  files 124 in the directory tree. After information is retrieved from each of the  $N$  files 124, the information is analyzed to determine whether each file is potentially a pestware file, and the scanning processes is ended after information from each of the  $N$  files 124 is analyzed (Blocks 214 and 216). It should be recognized, that the information received from each file may be analyzed (Block 214) while information from other files is being retrieved (Block 212) so as to expedite the entire process of retrieving and analyzing information from the  $N$  files 124.

[0027] In several embodiments, the detection module 114, it is responsible for detecting pestware or pestware activity on the protected computer 100 based upon the information received from the  $N$  files 124. In one embodiment for example, the detection module compares a representation of known pestware files (e.g., a cyclical redundancy code (CRC) of a portion of the pestware file) with a representation (e.g., CRC) of a portion of each of the  $N$  files 124. In one variation, only 500 Bytes of information are retrieved from each of the  $N$  files 124 and a CRC of the 500 Bytes of information retrieved from each file is compared with the known pestware definitions. If the 500 Bytes of retrieved information indicates the file is a potential pestware file, then a more thorough analysis (e.g., an analysis of the entire file) is conducted. In this way, the comparison of each file with definitions of pestware files is expedited.



[0028] Pestware and pestware activity can also be detected by the shield module 116, which generally runs in the background on the computer system. Shields can generally be divided into two categories: those that use definitions to identify known pestware and those that look for behavior common to pestware. This combination of shield types acts to prevent known pestware and unknown pestware from running or being installed on a protected computer.

[0029] In many cases, the detection and shield modules (114 and 116) detect pestware by matching files on the protected computer with definitions of pestware, which are collected from a variety of sources. For example, a host computers, protected computers and other systems can crawl the Web to actively identify pestware. These systems often download programs and search for exploits. The operation of these exploits can then be monitored and used to create pestware definitions. Various techniques for detecting pestware are disclosed in the above-identified and related application entitled: *System and Method for Monitoring Network Communications for Pestware*.

[0030] Referring next to FIGURE 3, shown is a flowchart 300 depicting steps carried out by the sweep speedup module 120 when directly accessing information from the file storage device 106 of FIGURE 1 in accordance with several embodiments of the present invention. As shown, initially a file table (e.g., a master file table (MFT)) that is associated with a collection of the  $N$  files 124 in the files storage device 106 is located (Blocks 302 and 304). In one embodiment, the operating system is initially utilized to help locate the file table. For example, if the file storage device 106 is a hard drive that

has been partitioned into two or more drives, the operating system is utilized to identify the partitioned drives.

[0031] After the file table for a collection of the  $N$  files 124 is located, the file table is accessed, while circumventing the operating system (Block 306), and the file table is read so as to identify names, locations and other attributes of the files (e.g., file size, compression flags and encryption flags) of the collection of the  $N$  files 124 in the file storage device 106 (Block 308). In some embodiments, the entire file structure of the collection of the  $N$  files 124 is built and stored so that the location of every one of the  $N$  files 124 is known. Thus, the steps identified in Blocks 304, 306 and 308 may be utilized to generate the listing of names and locations, discussed with reference to Block 208 of FIGURE 2, by directly accessing the file storage device 106.

[0032] After the names and locations of the  $N$  files 124 are identified (Block 308), information from each of the  $N$  files 124 is retrieved, while circumventing the operating system, until each of the  $N$  files 124 has been accessed (Blocks 310 and 312). This information may be utilized, as previously discussed, to identify pestware (e.g., the pestware 126) among the  $N$  files 124 (Block 214).

[0033] It should be recognized that the processes depicted in FIGURES 2 and 3 are shown in separate drawings merely to show that each process may be implemented separately to achieve substantial decreases in the amount of time that is required to scan files. In accordance with some embodiments, the processes depicted in FIGURES 2 and

3 may be combined so as to achieve even faster file scans. Specifically, the direct access techniques discussed with reference to FIGURE 3 may be utilized to enumerate the  $N$  files 124 as depicted in Blocks 204 and 206. Moreover, after the listing of the  $N$  files 124 is sorted (Block 210), the files may be directly accessed at block 212, by circumventing the operating system 122.

[0034] In conclusion, the present invention provides, among other things, a system and method for managing pestware. Those skilled in the art can readily recognize that numerous variations and substitutions may be made in the invention, its use and its configuration to achieve substantially the same results as achieved by the embodiments described herein. Accordingly, there is no intention to limit the invention to the disclosed exemplary forms. Many variations, modifications and alternative constructions fall within the scope and spirit of the disclosed invention as expressed in the claims.

**WHAT IS CLAIMED IS:**

1. A method for scanning files on a protected computer for pestware comprising:  
identifying a location of each of at least a first file, a second file and a third file in  
a file storage device of the protected computer;

retrieving, while substantially circumventing an operating system of the protected  
computer, information from the first file; and

analyzing the information from the first file to determine whether the first file is a  
potential pestware file.

2. The method of claim 1 wherein the identifying includes identifying the location  
of each of at least the first file, the second file and the third file while substantially  
circumventing the operating system.

3. The method of claim 2 wherein the identifying includes:  
accessing a master file table of the file storage device, while substantially  
circumventing the operating system; and

identifying the location of each of at least the first file, the second file and the  
third file by analyzing the data of the master file table.

4. The method of claim 1 wherein the identifying includes utilizing the operating  
system to identify the first file, the second file and the third file.

5. The method of claim 1 wherein the identifying includes identifying a cluster number of each of the a first file, a second file and a third file in a disk drive of the protected computer.

6. The method of claim 1 including:

sorting, by location on the file storage device, the first, second and third files so as to generated a sorted list, wherein the retrieving includes retrieving information from the first, the second and the third files by sequentially accessing the first, second and third files in the order the first, second and third files are listed in the sorted list.

7. A method for scanning files on a protected computer for pestware comprising:

identifying, while substantially circumventing an operating system of the protected computer, a location of each of a plurality of files in a file storage device of the protected computer;

retrieving information from each of the plurality of files; and

analyzing the information from each of the plurality of files so as to determine whether any of the plurality of files are potential pestware files.

8. The method of claim 7 wherein the identifying includes:

accessing a master file table of the file storage device, while substantially circumventing the operating system; and

identifying the location of each of the plurality of files by analyzing the data of the master file table.

9. The method of claim 7 wherein the retrieving includes utilizing the operating system to retrieve information from each of the plurality of files.

10. The method of claim 7 wherein the identifying includes identifying a cluster number of each of the plurality of files in a disk drive of the protected computer.

11. The method of claim 7 including:

sorting, by location on the file storage device, the plurality of files so as to generate a sorted list, wherein the retrieving includes retrieving information from each of the plurality of files by sequentially accessing each of the plurality of files in the order the plurality of files are listed in the sorted list.

12. A system for managing pestware comprising:

a pestware detection module configured to detect pestware on a protected computer, the protected computer including at least one file storage device and a program memory; and

a sweep speedup module configured to:

identify, while substantially circumventing an operating system of the protected computer, a location of each of a plurality of files in the at least one file storage device of the protected computer;

retrieve information from each of the plurality of files;

wherein the pestware detection module is configured to analyze the information from each of the plurality of files so as to determine whether any of the plurality of files are potential pestware files.

13. The system of claim 12 wherein the sweep speedup module is configured to access, while substantially circumventing the operating system, a master file table of the file storage device; and

identify the location of each of the plurality of files by analyzing the data of the master file table.

14. The system of claim 12 wherein the sweep speedup module is configured to utilize the operating system to retrieve information from each of the plurality of files.

15. The system of claim 12 wherein the sweep speedup module is configured to identify a cluster number of each of the plurality of files in a disk drive of the protected computer.

16. The system of claim 12 wherein the sweep speedup module is further configured to:

sort, by location on the file storage device, the plurality of files so as to generate a sorted list, wherein the sweep speedup module is configured to retrieve information from

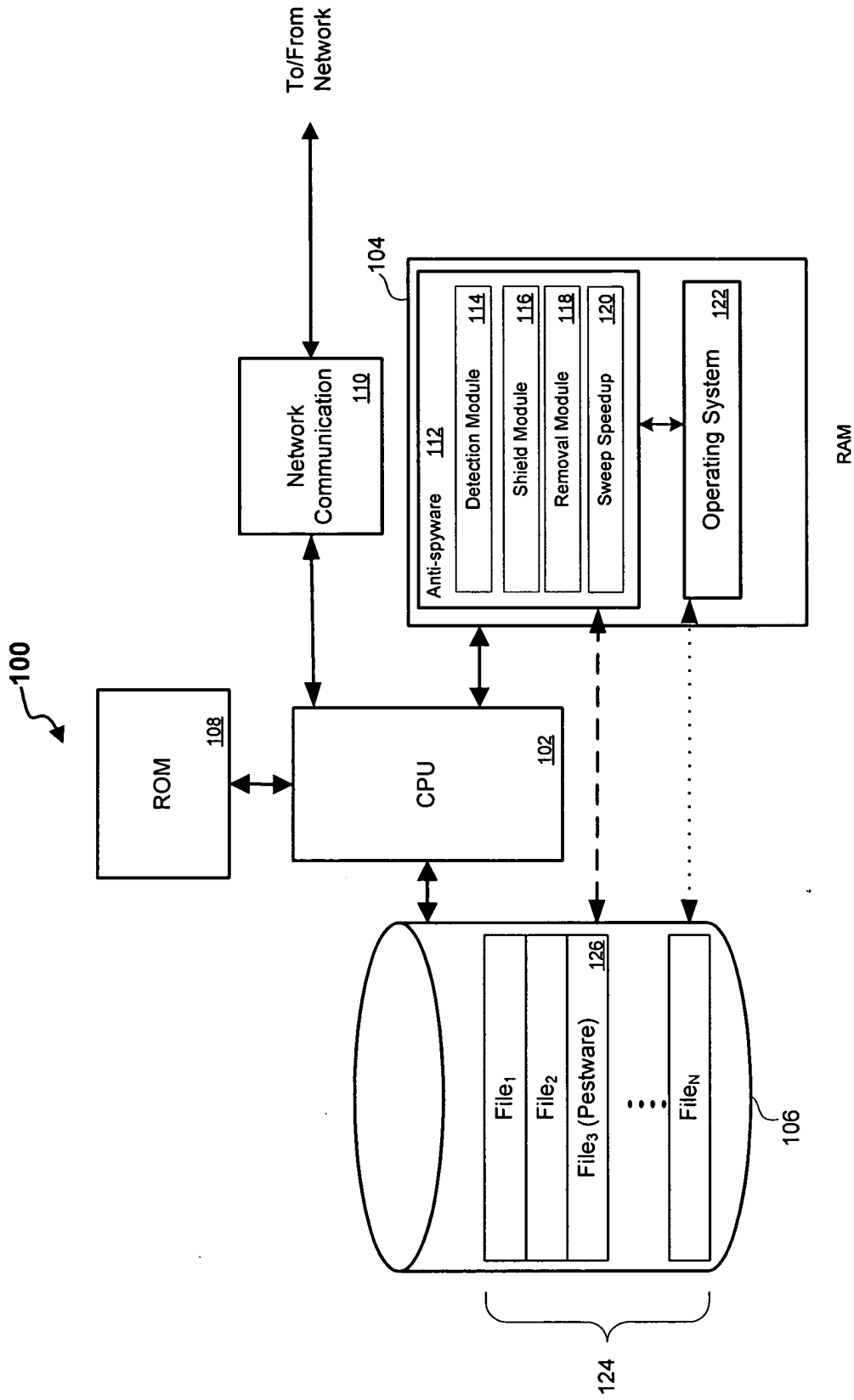
each of the plurality of files by sequentially accessing each of the plurality of files in the order the plurality of files are listed in the sorted list.

17. The system of claim 12 wherein the protected computer includes a plurality of storage devices, and wherein the plurality of files are distributed among the plurality of storage device.

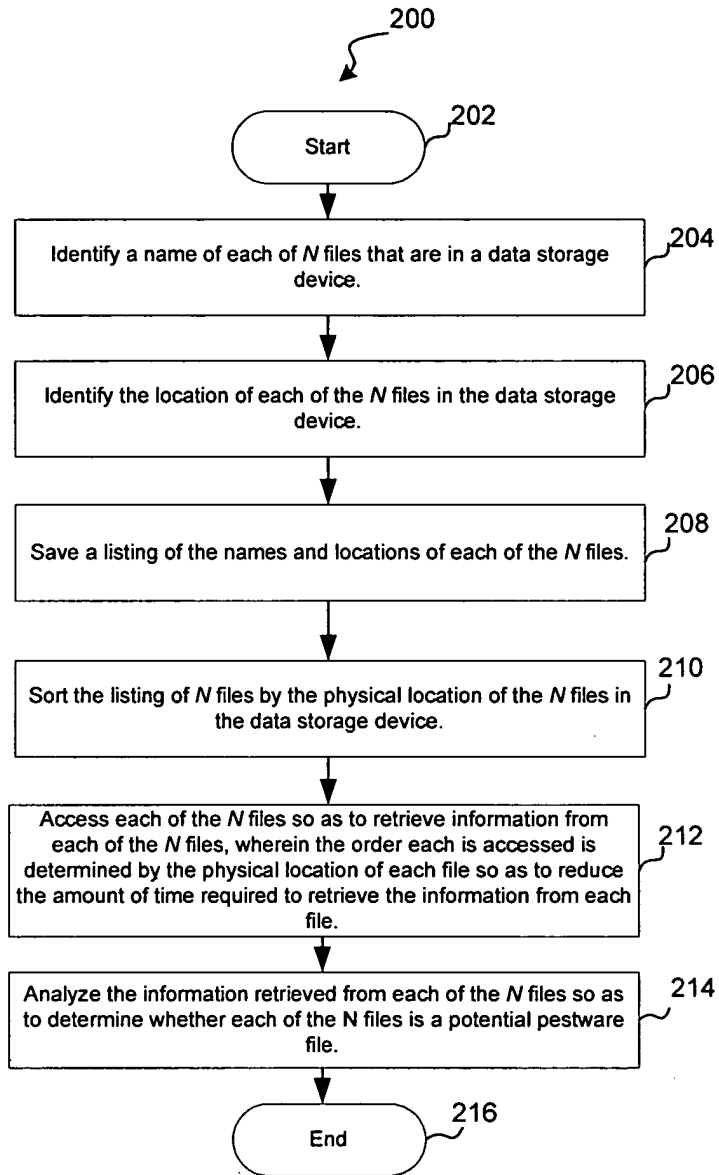


**ABSTRACT**

Systems and methods for scanning files for pestware on a protected computer are described. In one variation, locations of each of a plurality of files in a file storage device of the protected computer are identified while substantially circumventing an operating system of the protected computer. Information from each of the plurality of files is retrieved and analyzed so as to determine whether any of the plurality of files are potential pestware files. In variations, the operating system is circumvented while the information from each of the plurality of files is retrieved. In other variations, before information is retrieved from each of the plurality of files, a listing of the plurality of files is sorted according to the locations of the files on the storage device so as to reduce, even further, the time required to access the plurality of files.

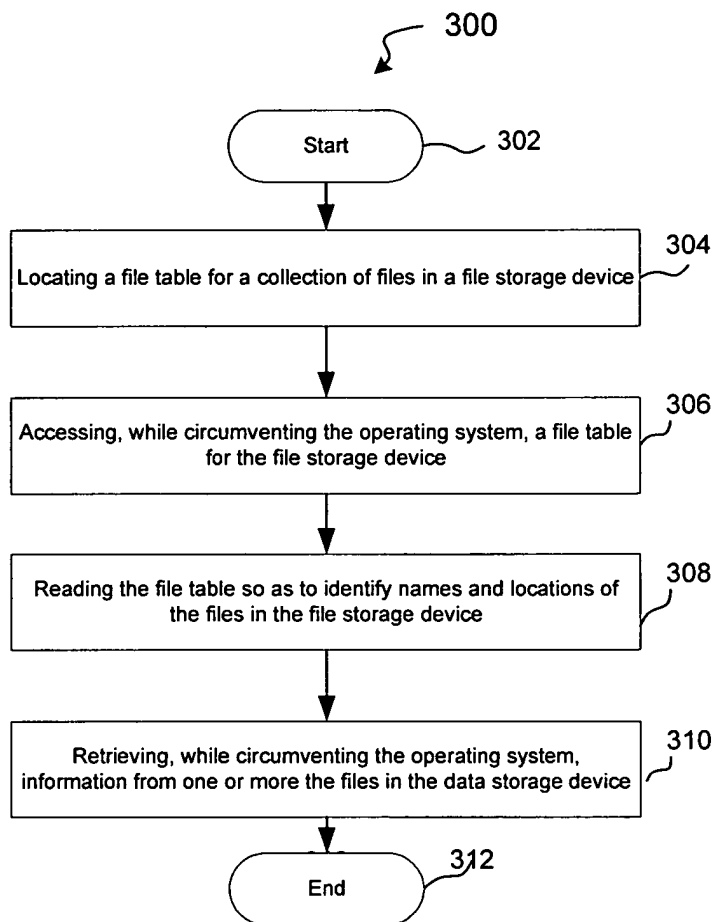


Attorney Docket No.: WEBR-011/00US  
 Express Mail No.: EV459983512US  
 FIGURE 1



Attorney Docket No.: WEBR-011/00US  
 Express Mail No.: EV459983512US

FIGURE 2



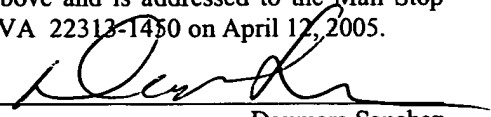
Attorney Docket No.: WEBR-011/00US  
Express Mail No.: EV459983512US

FIGURE 3

Attorney Docket No. WEBR-011/00US  
Express Mail Label Number: EV459983512US

PATENT  
Date of Deposit: April 12, 2005

I hereby certify that this paper or fee is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 CFR 1.10 on the date indicated above and is addressed to the Mail Stop Patent Application, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on April 12, 2005.

By:   
Daxmara Sanchez

### DECLARATION

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated next to my name;

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled:

SYSTEM AND METHOD FOR DIRECTLY ACCESSING DATA FROM A DATA STORAGE MEDIUM

the specification of which:

(check one)

is attached hereto;

was filed as United States Application Serial No. \_\_\_ on \_\_\_, and was amended on (if applicable);

was filed as PCT International Application No. \_\_\_ on \_\_\_ and was amended under PCT Article 19 or Article 34 on \_\_\_ (if applicable);

I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above;

I acknowledge the duty to disclose to the U.S. Patent and Trademark Office all information which is known to me to be material to the patentability of said invention in accordance with 37 C.F.R. §1.56;

I hereby claim foreign priority benefits under 35 U.S.C. §119 and/or §365 of any foreign application for patent, any foreign application for inventor's certificate, or any PCT international application designating at least one country other than the United States of America listed below; I have also identified below any foreign application for patent, any foreign application for inventor's certificate, or any PCT international application designating at least one country other than the United States of America filed by me on the same subject matter having a filing date before that of the application of which priority is claimed:

Prior Foreign Application

| COUNTRY/INTERNATIONAL | APPLICATION NUMBER | DATE OF FILING<br>(day, month, year) | PRIORITY CLAIMED   |
|-----------------------|--------------------|--------------------------------------|--|
|                       |                    |                                      | <input type="checkbox"/> YES <input type="checkbox"/> NO |
|                       |                    |                                      | <input type="checkbox"/> YES <input type="checkbox"/> NO |

I hereby claim the benefit under 35 U.S.C. §119(e) of any United States provisional application listed below:

\_\_\_\_\_  
(Application Number)

\_\_\_\_\_  
(Filing Date) (day, month, year)

\_\_\_\_\_  
(Application Number)

\_\_\_\_\_  
(Filing Date) (day, month, year)

I hereby claim the benefit under 35 U.S.C. §120 and/or §365 of any United States application or of any international application designating the United States of America that is/are listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior application in the manner provided by the first paragraph of 35 U.S.C. §112, I acknowledge the duty to disclose to the U.S. Patent and Trademark Office all information known to me to be material to patentability as defined in 37 C.F.R. §1.56 which became available between the filing date(s) of the prior application and the national or PCT international filing date of this application:

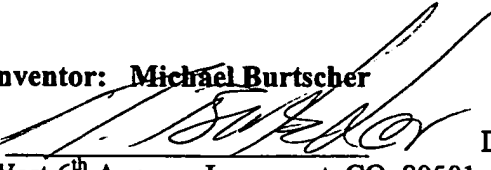
Prior U.S. Application or PCT International Applications Designating the U.S. for benefit under 35 U.S.C. §120

| U.S. APPLICATIONS                     |                                     |                                | STATUS (check one)       |                          |                          |
|---------------------------------------|-------------------------------------|--------------------------------|--------------------------|--------------------------|--------------------------|
| U.S. APPLICATION NO.                  | U.S. FILING DATE (day, month, year) |                                | Pending                  | Patented                 | Abandoned                |
|                                       |                                     |                                | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
|                                       |                                     |                                | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| PCT APPLICATIONS DESIGNATING THE U.S. |                                     |                                |                          |                          |                          |
| PCT APPLICATION NO.                   | PCT FILING DATE (day, month, year)  | U.S. APPLICATION NOS. (if any) |                          |                          |                          |
|                                       |                                     |                                | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
|                                       |                                     |                                | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

**Full name of first inventor: Michael Burtscher**

Inventor's signature



Date

4/5/2005

Residence: 914 West 6<sup>th</sup> Avenue, Longmont, CO 80501

Citizen of: Austria

Post Office Address: Same as above

231371 v1/CO

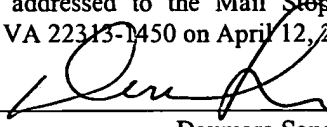
Attorney Docket No. WEBR-011/00US

PATENT

Express Mail Label Number: EV459983512US

Date of Deposit: April 12, 2005

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as Express Mail in an envelope addressed to the Mail Stop Patent Application, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on April 12, 2005.

By:   
Daxmara Sanchez

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

**In re application of:** Michael BURTSCHER      **Confirmation No.:** Not Yet Assigned

**Serial No.:** Not Yet Assigned      **Art Unit No.:** Not Yet Assigned

**Filed:** April 12, 2005      **Examiner:** Not Yet Assigned

**TITLE:**      **SYSTEM AND METHOD FOR DIRECTLY ACCESSING DATA FROM A DATA STORAGE MEDIUM**

Mail Stop Patent Application  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

**POWER BY ASSIGNEE  
AND STATEMENT UNDER 37 C.F.R. §3.73(b)**

The Assignee of the entire right, title, and interest in the above-identified application hereby grants the registered practitioners of Cooley Godward LLP included in the Customer Number provided below power to act, prosecute, and transact all business in the U.S. Patent and Trademark Office in connection with this application, any applications claiming priority to this application, and any patents issuing therefrom.

The Assignee certifies that to the best of its knowledge and belief it is the owner of the entire right, title, and interest in and to the above-identified application as evidenced by:

- An assignment document, a copy of which is enclosed herewith;
- An assignment previously recorded in the U.S. Patent and Trademark Office at Reel \_\_, Frame \_\_.



Please direct all telephone calls and correspondence to:

Cooley Godward LLP  
ATTN: Patent Group  
One Freedom Square  
Reston Town Center  
11951 Freedom Drive  
Reston, VA 20190-5656  
Tel: (720) 566-4035  
Fax: (720) 566-4099

CUSTOMER NUMBER: **22903**

The undersigned (whose title is supplied below) is empowered to sign this statement on behalf of the Assignee.

Date: \_\_\_\_\_

Signature: \_\_\_\_\_

Name:

Michael K. Irwin

Title:

Chief Financial Officer

Company:

Webroot Software, Inc.

231366 v1/CO

**BEST AVAILABLE COPY**

# PATENT APPLICATION FEE DETERMINATION RECORD

Effective December 8, 2004

11/10/2002

## CLAIMS AS FILED - PART I

(Column 1)                      (Column 2)

|   |               |              |
|---|---------------|--------------|
| TOTAL CLAIMS  | 17            |              |
| FOR   | NUMBER FILED  | NUMBER EXTRA |
| TOTAL CHARGEABLE CLAIMS                                   | 17 minus 20 = | * -          |
| INDEPENDENT CLAIMS  | 3 minus 3 =   | * -          |
| MULTIPLE DEPENDENT CLAIM PRESENT <input type="checkbox"/> |               |              |

\* If the difference in column 1 is less than zero, enter "0" in column 2

**SMALL ENTITY TYPE**

**OR OTHER THAN SMALL ENTITY**

| RATE         | FEE    |
|--------------|--------|
| BASIC FEE    | 150.00 |
| X\$ 25=      |        |
| X100=        |        |
| +180=        |        |
| <b>TOTAL</b> |        |

| RATE         | FEE    |
|--------------|--------|
| BASIC FEE    | 300.00 |
| X\$50=       |        |
| X200=        |        |
| +360=        |        |
| <b>TOTAL</b> |        |

## CLAIMS AS AMENDED - PART II

(Column 1)                      (Column 2)                      (Column 3)

| AMENDMENT A | CLAIMS REMAINING AFTER AMENDMENT  |   | HIGHEST NUMBER PREVIOUSLY PAID FOR | PRESENT EXTRA |
|-------------|---|---|------------------------------------|---------------|
|             | Total   | * | Minus                              | ** =          |
|             | Independent   | * | Minus                              | *** =         |
|             | FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM <input type="checkbox"/> |   |                                    |               |

( 7, 12 )

**SMALL ENTITY**

**OR OTHER THAN SMALL ENTITY**

| RATE                    | ADDITIONAL FEE |
|-------------------------|----------------|
| X\$ 25=                 |                |
| X100=                   |                |
| +180=                   |                |
| <b>TOTAL ADDIT. FEE</b> |                |

| RATE                    | ADDITIONAL FEE |
|-------------------------|----------------|
| X\$50=                  |                |
| X200=                   |                |
| +360=                   |                |
| <b>TOTAL ADDIT. FEE</b> |                |

| AMENDMENT B | CLAIMS REMAINING AFTER AMENDMENT  |   | HIGHEST NUMBER PREVIOUSLY PAID FOR | PRESENT EXTRA |
|-------------|---|---|------------------------------------|---------------|
|             | Total   | * | Minus                              | ** =          |
|             | Independent   | * | Minus                              | *** =         |
|             | FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM <input type="checkbox"/> |   |                                    |               |

| RATE                    | ADDITIONAL FEE |
|-------------------------|----------------|
| X\$ 25=                 |                |
| X100=                   |                |
| +180=                   |                |
| <b>TOTAL ADDIT. FEE</b> |                |

| RATE                    | ADDITIONAL FEE |
|-------------------------|----------------|
| X\$50=                  |                |
| X200=                   |                |
| +360=                   |                |
| <b>TOTAL ADDIT. FEE</b> |                |

| AMENDMENT C | CLAIMS REMAINING AFTER AMENDMENT  |   | HIGHEST NUMBER PREVIOUSLY PAID FOR | PRESENT EXTRA |
|-------------|---|---|------------------------------------|---------------|
|             | Total   | * | Minus                              | ** =          |
|             | Independent   | * | Minus                              | *** =         |
|             | FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM <input type="checkbox"/> |   |                                    |               |

| RATE                    | ADDITIONAL FEE |
|-------------------------|----------------|
| X\$ 25=                 |                |
| X100=                   |                |
| +180=                   |                |
| <b>TOTAL ADDIT. FEE</b> |                |

| RATE                    | ADDITIONAL FEE |
|-------------------------|----------------|
| X\$50=                  |                |
| X200=                   |                |
| +360=                   |                |
| <b>TOTAL ADDIT. FEE</b> |                |

\* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.  
 \*\* If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20."  
 \*\*\* If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3."  
 The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

PATENT APPLICATION SERIAL NO. \_\_\_\_\_

U.S. DEPARTMENT OF COMMERCE  
PATENT AND TRADEMARK OFFICE  
FEE RECORD SHEET

04/14/2005 JBALINAN 00000029 501283 11104202

|            |           |
|------------|-----------|
| 01 FC:1011 | 300.00 DA |
| 02 FC:1111 | 500.00 DA |
| 03 FC:1311 | 200.00 DA |

PTO-1556  
(5/87)

**BEST AVAILABLE COPY**

041205  
1/638 U.S. PTO

**Attorney Docket No. WEBR-011/00US**

**PATENT**

Express Mail Label Number: EV459983512US  
Date of Deposit: April 12, 2005

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as Express Mail in an envelope addressed to the Mail Stop Patent Application, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on April 12, 2005.

By: \_\_\_\_\_

Daxmara Sanchez

**Mail Stop Patent Application**  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

113261 U.S. PTO  
11/104202  
041205

### UTILITY PATENT APPLICATION TRANSMITTAL

Transmitted herewith for filing is a U.S. Non-Provisional Utility Patent Application entitled: "SYSTEM AND METHOD FOR DIRECTLY ACCESSING DATA FROM A DATA STORAGE MEDIUM"

naming as inventor(s): Michael Burtscher

and including:

- (13) pages of description (before the claims);
- (05) pages of claims ((17) total claims; (03) independent claims);
- One (1) Sheet of Abstract;
- (03) sheets of drawing(s) including Figures 1-3.

1. Also enclosed are:

- Executed Declaration
- Application Data Sheet
- Executed Assignment and Assignment Recordation Cover Sheet
- Executed Power by Assignee
- Assertion of Entitlement to Small Entity Status
- Information Disclosure Statement
- Preliminary Amendment
- CD-ROM or CD-R in duplicate, large table or Computer Program (Appendix)
- Nucleotide and/or Amino Acid Sequence Submission
  - Computer Readable Form (CRF) on 3 1/2" floppy disk
  - Specification Sequence Listing on:
    - CD-ROM or CD-R (2 copies); or
    - paper

The content of the copy in computer readable form is identical to the content of the paper, CD-ROM, or CD-R copy of the Sequence Listing.

Nonpublication Request and Certification

Check No. XXX in the amount of \$XXX for the total fee as calculated below

Return receipt postcard

Other: XXX

2.  Please amend the specification by inserting before the first heading the following paragraph:

This application claims priority under 35 U.S.C. §§119 and/or 365 to \_\_\_ filed in \_\_\_ on \_\_\_, the entire content of which is hereby incorporated by reference.

A certified copy of the priority application  is enclosed  will follow.

3.  Please amend the specification by inserting before the first heading the following paragraph:

This application claims priority under 35 U.S.C. §119(e) to U.S. Provisional Application No. \_\_\_, filed \_\_\_, the entire content of which is hereby incorporated by reference.

4.  Please amend the specification by inserting before the first heading the following paragraph:

This application is a \_\_\_ of and claims priority under 35 U.S.C. §120 of U.S. Patent Application No. \_\_\_, filed \_\_\_, the entire contents of which are hereby incorporated by reference.

5. The filing fee has been calculated as follows  and in accordance with the enclosed preliminary amendment:

|  | NO. OF CLAIMS |        | EXTRA CLAIMS | RATE       | FEE               |
|--|---------------|--------|--------------|------------|-------------------|
| Basic Application Fee (includes Basic Filing Fee, Search and Examination Fees)                           |               |        |              |            | \$1,000.00        |
| Total Claims   | 17            | - 20 = | 0            | x \$50.00  | \$50.00           |
| Independent Claims   | 03            | - 3 =  | 0            | x \$200.00 | \$200.00          |
| If multiple dependent claims are presented, add \$360.00   |               |        |              |            | 0                 |
| Total Application Fee  |               |        |              |            | \$1,250.00        |
| If an Assertion of Entitlement to Small Entity Status is enclosed, subtract 50% of Total Application Fee |               |        |              |            | 0                 |
| Other fees: (specify)  |               |        |              |            | 0                 |
| <b>TOTAL FEE DUE</b>   |               |        |              |            | <b>\$1,250.00</b> |

- This application is being filed without a filing fee. Issuance of a Notice to File Missing Parts of Application is respectfully requested.
- A check for the total fee is attached.
- Please charge \$1,250.00 to Deposit Account No. 50-1283 for the total fee. This paper is being submitted in duplicate.
- The Commissioner is hereby authorized to charge any appropriate fees under 37 C.F.R. §§1.16, 1.17, and 1.21 that may be required by this paper, and to credit any overpayment, to Deposit Account No. 50-1283.

6. Please direct all correspondence concerning this application to:

Cooley Godward LLP  
ATTN: Patent Group  
One Freedom Square  
Reston Town Center  
11951 Freedom Drive  
Reston, VA 20190-5656  
Tel: (703) 456-8000 or (720) 566-4035  
Fax: (703) 456-8100 or (720) 566-4099

CUSTOMER NUMBER: **22903**

Cooley Godward LLP  
ATTN: Patent Group  
One Freedom Square  
Reston Town Center  
11951 Freedom Drive  
Reston, VA 20190-5656  
Tel: (703) 456-8000 or (720) 566-4035  
Fax: (703) 456-8100 or (720) 566-4099

Respectfully submitted,  
**COOLEY GODWARD LLP**

By:



Sean R. O'Dowd, Esq.  
Reg. No. 53,403

07-06-05

PATENT

Attorney Docket No: WEBR-011/00US

Express Mail No.: EV459983659US

hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as Express Mail in an envelope addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on July 5, 2005.

By: [Signature]  
Daxmara Sanchez

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

|                              |                   |                          |                  |
|------------------------------|-------------------|--------------------------|------------------|
| <b>In re application of:</b> | Michael Burtscher | <b>Confirmation No.:</b> | Not Yet Assigned |
| <b>Serial No.:</b>           | 11/104,202        | <b>Art Unit No.:</b>     | Not Yet Assigned |
| <b>Filed:</b>                | April 12, 2005    | <b>Examiner:</b>         | Not Yet Assigned |

**Title: "SYSTEM AND METHOD FOR DIRECTLY ACCESSING DATA FROM A DATA STORAGE MEDIUM"**

Mail Stop: Petitions  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313

**PETITION TO CORRECT INVENTORSHIP UNDER 37 CFR § 1.48(a)**

Applicants respectfully request a correction of inventorship of the above-identified application. It is requested that Tony Nichols be added as an inventor.

This request is accompanied by:

1. Statement Of Lack Of Deceptive Intention from removed inventors,
2. Supplemental Declaration from actual inventor as required by § 1.63,
3. Postcard, and
4. A check for \$130.00 as required by 37 CFR § 1.17(i).

The Commissioner is hereby authorized to charge any underpayment of the fees associated with this communication, or credit any overpayment to Deposit Account No. 50-1283.

07/07/2005 CCHAU1 00000004 501283 11104202

01 FC:1464 130.00 DA

The PTO did not receive the following listed item(s) The Check

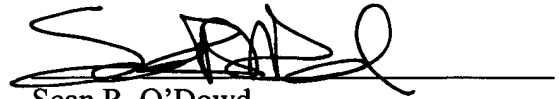


If in the opinion of the Examiner, a telephone conference would expedite the prosecution of the subject application, the Examiner is invited to call the undersigned.

Cooley Godward LLP  
Attn: Patent Group  
One Freedom Square  
Reston Town Center  
11951 Freedom Drive  
Reston, VA 20190  
Telephone: (720) 566-4035  
Facsimile: (720) 566-4099

Respectfully submitted,  
COOLEY GODWARD LLP

By:



Sean R. O'Dowd  
Reg. No. 53,403

Attorney Docket No: WEBR-011/00US  
Express Mail No.: EU459983659US

PATENT



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Michael Burtscher et al.

Confirmation No.:

Serial No.: 11/104202

Art Unit No.:

Filed: April 12, 2005

Examiner:

Title: "SYSTEM AND METHOD FOR DIRECTLY ACCESSING DATA FROM A DATA STORAGE MEDIUM"

Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313

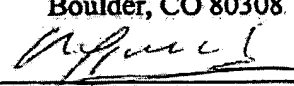
WRITTEN CONSENT OF ASSIGNEE

The undersigned assignee of the entire interest in the application for the Letters Patent identified above hereby consents to the addition of Tony Nichols as inventor.

Assignee's rights are evidenced by an assignment previously recorded on [date], [Reel No. and Frame No.], and a supplemental assignment being filed herewith.

Michael K. Irwin, signing on behalf of the assignee has the authority to act on behalf of the assignee.

Assignee: Webroot Software, Inc.  
2560 55<sup>th</sup> Street  
Boulder, CO 80308

Signature: 

Name: Michael K. Irwin

Title: Chief Financial Officer

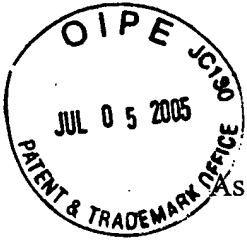
Date: 6/23/05

233065 v1/CO

BEST AVAILABLE COPY

Attorney Docket No: WEBR-011/00US  
Express Mail No.: EV459983659US

PATENT



**SUPPLEMENTAL DECLARATION**

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated next to my name;

I believe I am an original, joint inventor of the subject matter which is claimed and for which a patent is sought on the invention entitled: **“SYSTEM AND METHOD FOR DIRECTLY ACCESSING DATA FROM A DATA STORAGE MEDIUM”**

the specification of which:

(check one)

is attached hereto;

was filed as United States Application Serial No. 11/104,202 on April 12, 2005;

I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above;

I acknowledge the duty to disclose to the U.S. Patent and Trademark Office all information which is known to me to be material to the patentability of said invention in accordance with 37 C.F.R. §1.56;

I hereby claim the benefit under 35 U.S.C. §119(e) of any United States provisional application(s) listed below:

\_\_\_\_\_  
(Application Number)

\_\_\_\_\_  
(Filing Date) (day, month, year)

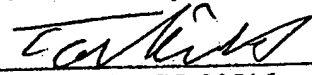
\_\_\_\_\_  
(Application Number)

\_\_\_\_\_  
(Filing Date) (day, month, year)

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

**Full name of first inventor: Tony Nichols**

**Full name of first inventor: Tony Nichols**

Inventor's signature 

Date June 23, 05

Residence: 436 Tynan Ct., Erie, CO 80516

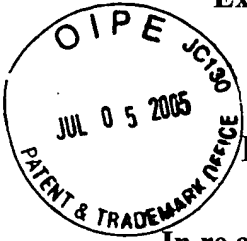
Citizen of: USA

Post Office Address: Same as residence

233066 vi/CO

Attorney Docket No: WEBR-011/00US  
Express Mail No.: EV459983659US

PATENT



**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

**In re application of:** Michael Burtscher et al.      **Confirmation No.:** Not Yet Assigned  
**Serial No.:** 11/104,202      **Art Unit No.:** Not Yet Assigned  
**Filed:** April 12, 2005      **Examiner:** Not Yet Assigned

**Title: "SYSTEM AND METHOD FOR DIRECTLY ACCESSING DATA FROM A DATA STORAGE MEDIUM"**

Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313

**STATEMENT OF LACK OF DECEPTIVE INTENTION**

The undersigned, Tony Nichols, hereby declares and states that:

1. This Statement is in support of the accompanying request to correct inventorship under 37 CFR § 1.48(a).
2. I have been employed by Webroot Software, Inc. since July, 2004. At the present time, I am a computer scientist.
3. The declaration previously filed on April 12, 2005 in connection with the above application incorrectly omitted myself as an inventor. Such omission was in error as it relates to the subject matter presently pending in the above application.
4. The error occurred without deceptive intention.

**Declaration**

I declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both under Section 1001 of Title 18 of

the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

  
\_\_\_\_\_  
Tony Nichols

Date: June 23, 05

233050 v1/CO

BEST AVAIL ABLE COPY

RECEIVED  
CENTRAL FAX CENTER

001/002

JUL 25 2006

# Cooley Godward LLP

ATTORNEYS AT LAW

## FAX

THIS FACSIMILE AND THE INFORMATION IT CONTAINS ARE INTENDED TO BE A CONFIDENTIAL COMMUNICATION ONLY TO THE PERSON OR ENTITY TO WHOM IT IS ADDRESSED. IF YOU HAVE RECEIVED THIS FACSIMILE IN ERROR, PLEASE NOTIFY US BY TELEPHONE AND RETURN THIS ORIGINAL FAX TO THIS OFFICE BY MAIL.

380 Interlocken Crescent  
Suite 900  
Broomfield, CO  
80021-8023

Offices:  
Broomfield, CO  
Palo Alto, CA  
Reston, VA  
San Diego, CA  
San Francisco, CA  
Washington, DC

MAIN (720) 566-4000  
FAX (720) 566-4099

DATE: July 25, 2006

| PLEASE DELIVER TO:  | PHONE No.: | FAX No.:       |
|---|------------|----------------|
| <b>Central Patent</b><br>U.S. Patent and Trademark Office |            | (571) 273-8300 |

FROM: Sean R. O'Dowd                      PHONE: (720) 566-4035      REPLY FAX: (720) 566-4099  
RE: Request for Official Filing Receipt

|  |                            |
|--|----------------------------|
| NUMBER OF PAGES, INCLUDING COVER PAGE: 2 | Client Number: 303666-2011 |
| Atty. Docket No. WEBR-011/00US           | Requestor #: 12567         |

### MESSAGE:

Please see the following correspondence from Sean O'Dowd.  
  
Thank you.

If you do not receive all of the pages, please call  
Daxmara Sanchez at (720) 566-4068 as soon as possible.

256840 v1/CO

RECEIVED  
CENTRAL FAX CENTER

JUL 25 2006

Attorney Docket No. WEBR-011/00US

PATENT

I hereby certify that this correspondence is being transmitted by facsimile addressed to Patent Central Facsimile Number (571) 273-8300, at United States Patent and Trademark Office, Alexandria, VA 22314 on July 25, 2006.

By:   
Daxmara Sanchez

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

|                              |                   |                          |                  |
|------------------------------|-------------------|--------------------------|------------------|
| <b>In re application of:</b> | Michael Burtscher | <b>Confirmation No.:</b> | Not Yet Assigned |
| <b>Serial No.:</b>           | 11/104,202        | <b>Art Unit No.:</b>     | Not Yet Assigned |
| <b>Filed:</b>                | 04/12/05          | <b>Examiner:</b>         | Not Yet Assigned |

**Title: SYSTEM AND METHOD FOR DIRECTLY ACCESSING DATA FROM A DATA STORAGE MEDIUM**

Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450


**REQUEST FOR OFFICIAL FILING RECEIPT**

A Patent Application was filed on April 12, 2005 and a date-stamped postcard was received indicating that the above-identified application was accepted on April 12, 2005 and was assigned Application Serial No. 11/104,202 for examination purposes. To date, the Official Filing Receipt has not been received.

Issuance of an Official Filing Receipt confirming the above-noted identifying information is respectfully requested.

COOLEY GODWARD LLP  
ATTN: Patent Group  
The Bowen Building  
875 15<sup>th</sup> Street NW, Suite 800  
Washington, DC 20005-2221  
Tel: (720) 566-4035  
Fax: (720) 566-4099

Respectfully submitted,  
COOLEY GODWARD LLP

By:   
Sean R. O'Dowd  
Reg. No. 44,051





09-05-06

HW

Attorney Docket No. WEBR-011/00US

PATENT

Express Mail Label Number: EV778912548US  
Date of Deposit: 9/1/06

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as Express Mail in an envelope addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

By: [Signature]  
Daxmara Sanchez

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

|                              |                   |                          |                  |
|------------------------------|-------------------|--------------------------|------------------|
| <b>In re application of:</b> | Michael Burtscher | <b>Confirmation No.:</b> | 1284             |
| <b>Serial No.:</b>           | 11/104,202        | <b>Art Unit No.:</b>     | 2161             |
| <b>Filed:</b>                | 04/12/05          | <b>Examiner:</b>         | Not Yet Assigned |

**Title: SYSTEM AND METHOD FOR DIRECTLY ACCESSING DATA FROM A DATA STORAGE MEDIUM**

Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

**INFORMATION DISCLOSURE STATEMENT  
UNDER 37 C.F.R. §1.97(b)**

In accordance with the duty of disclosure set forth in 37 C.F.R. §1.56, Applicant(s) hereby submits the following information in conformance with 37 C.F.R. §§1.97 and 1.98.

- Pursuant to 37 C.F.R. §1.98, a copy of each document cited in the attached Form PTO/SB/08 is enclosed.
- No copies of the publications listed on the attached Form PTO/SB/08A are being provided pursuant to 37 C.F.R. §1.98(d) because the publications were previously cited by or submitted to the Office in prior Application Serial No. \_\_\_ to which the above-identified application claims priority under 35 U.S.C. §120.
- No copies of any U.S. patents or U.S. patent application publications listed on the attached Form PTO/SB/08A are being provided pursuant to 37 C.F.R. §1.98 because this application was filed after June 30, 2003.

- Publication(s) \_\_\_ listed on the attached Form PTO/SB/08A were cited in a foreign search or examination report corresponding to \_\_\_ application serial no. \_\_\_ and mailed on \_\_\_.
- Enclosed is a copy of a non-English publication(s) \_\_\_. Pursuant to §609 of the M.P.E.P., Applicant submits the attached foreign search or examination report, which cites such non-English language publication(s).
- Enclosed is a copy of a non-English publication(s) \_\_\_. English language publication \_\_\_ (copy enclosed) claims priority from this non-English publication.

This Information Disclosure Statement is filed within any one of the following time periods:


- within three months from the filing date of this national application other than a CPA under 37 C.F.R. § 1.53(d);
- within three months from the date of entry of the national stage as set forth in 37 C.F.R. §1.491 in this international application;
- before the mailing date of a first office action on the merits; or
- before the mailing of a first office action after the filing of a request for continued examination under 37 C.F.R. § 1.114.

It is respectfully requested that the Examiner consider the above-noted information and return an initialed copy of the attached Form PTO/SB/08A to the undersigned.

Cooley Godward LLP  
COOLEY GODWARD LLP  
ATTN: Patent Group  
The Bowen Building  
875 15th Street NW, Suite 800  
Washington, DC 20005-2221  
Telephone: (720) 566-4035  
Facsimile: (720) 566-4099

Respectfully submitted,  
COOLEY GODWARD LLP

By:

  
Sean R. O'Dowd  
Reg. No. 53,403



Please type a plus sign (+) inside this box → +

|   |        |                          |                   |
|---|--------|--------------------------|-------------------|
| Substitute for form 1449A/PTO<br><b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b><br><i>(use as many sheets as necessary)</i> |        | <i>Complete if Known</i> |                   |
|   |        | Application Number       | 11/104,202        |
|   |        | Filing Date              | 04/12/05          |
|   |        | First Named Inventor     | Michael Burtscher |
|   |        | Group Art Unit           | 2161              |
|   |        | Examiner Name            | Not Yet Assigned  |
| Sheet   | 1 of 2 | Attorney Docket No.      | WEBR-011/00US     |

| U.S. PATENT DOCUMENTS |                       |                      |   |   |  |
|-----------------------|-----------------------|----------------------|---|---|--|
| Examiner Initials*    | Cite No. <sup>1</sup> | U.S. Patent Document |   | Name of Patentee or Applicant of Cited Document | Date of Publication of Cited Document MM-DD-YYYY |
|                       |                       | Number               | Kind Code <sup>2</sup><br><i>(if known)</i> |   |  |
|                       |                       | 5,623,600            |   | JI, ET AL.                                      | 04/22/97   |
|                       |                       | 6,069,628            |   | FARRY, ET AL.                                   | 05/30/00   |
|                       |                       | 6,073,241            |   | ROSENBERG, ET AL.                               | 06/06/00   |
|                       |                       | 6,092,194            |   | TOUBOUL   | 07/18/00   |
|                       |                       | 6,154,844            |   | TOUBOUL   | 11/28/00   |
|                       |                       | 6,167,520            |   | TOUBOUL   | 12/26/00   |
|                       |                       | 6,310,630            |   | KULKARNI, ET AL.                                | 10/30/01   |
|                       |                       | 6,397,264            |   | STASNICK, ET AL.                                | 05/28/02   |
|                       |                       | 6,460,060            |   | MADDALOZZO, JR., ET AL.                         | 10/01/02   |
|                       |                       | 6,480,962            |   | TOUBOUL   | 11/12/02   |
|                       |                       | 6,535,931            |   | CELI, JR.                                       | 03/18/03   |
|                       |                       | 6,611,878            |   | DE ARMAS, ET AL.                                | 08/26/03   |
|                       |                       | 6,633,835            |   | MORAN ET AL.                                    | 10/14/03   |
|                       |                       | 6,667,751            |   | WYNN, ET AL.                                    | 12/23/03   |
|                       |                       | 6,701,441            |   | BALASUBRAMANIAM, ET AL.                         | 03/02/04   |
|                       |                       | 6,785,732            |   | BATES, ET AL.                                   | 08/31/04   |
|                       |                       | 6,804,780            |   | TOUBOUL   | 10/12/04   |
|                       |                       | 6,813,711            |   | DIMENSTEIN                                      | 11/02/04   |
|                       |                       | 6,829,654            |   | JUNGEK  | 12/07/04   |
|                       |                       | 6,965,968            |   | TOUBOUL   | 11/15/05   |
|                       |                       | 7,058,822            |   | EDERY ET AL.                                    | 06/06/06   |
|                       |                       | US 2003/0217287      | A1  | KRUGLENKO                                       | 11/20/03   |
|                       |                       | US 2004/0030914      | A1  | KELLEY, ET AL.                                  | 02/12/04   |
|                       |                       | US 2004/0034794      | A1  | MAYER ET AL.                                    | 02/19/04   |
|                       |                       | US 2004/0064736      | A1  | OBRECHT, MARK ERIC, ET AL.                      | 04/01/04   |
|                       |                       | US 2004/0080529      | A1  | WOJCIK, PAUL KAZIMIERZ                          | 04/29/04   |
|                       |                       | US 2004/0143763      | A1  | RADATTI   | 07/22/04   |
|                       |                       | US 2004/0187023      | A1  | ALAGNA, MICHAEL ANTHONY, ET AL.                 | 09/23/04   |
|                       |                       | US 2004/0225877      | A1  | HUANG   | 11/11/04   |
|                       |                       | US 2005/0138433      | A1  | LINETSKY, GENE                                  | 06/23/05   |

|                    |  |                 |  |
|--------------------|--|-----------------|--|
| Examiner Signature |  | Date Considered |  |
|--------------------|--|-----------------|--|

\*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

<sup>1</sup> Unique citation designation number.  
<sup>2</sup> See attached Kinds of U.S. Patent Documents.

Please type a plus sign (+) inside this box →

+

|   |                  |                          |                   |
|---|------------------|--------------------------|-------------------|
| Substitute for form 1449A/PTO<br><br><b>INFORMATION DISCLOSURE<br/>STATEMENT BY APPLICANT</b><br><br><i>(use as many sheets as necessary)</i> |                  | <i>Complete if Known</i> |                   |
|   |                  | Application Number       | 11/104,202        |
|   |                  | Filing Date              | 04/12/05          |
|   |                  | First Named Inventor     | Michael Burtscher |
|   |                  | Group Art Unit           | 2161              |
| Examiner Name   | Not Yet Assigned | Attorney Docket No.      | WEBR-011/00US     |
| Sheet   | 2 of 2           |                          |                   |

| FOREIGN PATENT DOCUMENTS |                       |                         |                     |                                      |   |  |                |
|--------------------------|-----------------------|-------------------------|---------------------|--------------------------------------|---|--|----------------|
| Examiner Initials*       | Cite No. <sup>1</sup> | Foreign Patent Document |                     |                                      | Name of Patentee or Applicant of Cited Document | Date of Publication of Cited Document MM-DD-YYYY | T <sup>4</sup> |
|                          |                       | Office <sup>1</sup>     | Number <sup>2</sup> | Kind Code <sup>3</sup><br>(if known) |   |  |                |
|                          |                       |                         |                     |                                      |   |  |                |
|                          |                       |                         |                     |                                      |   |  |                |
|                          |                       |                         |                     |                                      |   |  |                |
|                          |                       |                         |                     |                                      |   |  |                |
|                          |                       |                         |                     |                                      |   |  |                |

| OTHER – NON PATENT LITERATURE DOCUMENTS |                       |   |                |
|---|-----------------------|---|----------------|
| Examiner Initials*                      | Cite No. <sup>1</sup> | Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published. | T <sup>2</sup> |
|   | I.                    | Codeguru, Three Ways to Inject Your Code Into Another Process, by Robert Kuster, August 4, 2003, 22 pgs.  |                |
|   | II.                   | Codeguru, Managing Low-Level Keyboard Hooks With The Windows API for VB .Net, by Paul Kimmel, April 18, 2004, 10 pgs.   |                |
|   | III.                  | Codeguru, Hooking The Keyboard, by Anoop Thomas, December 13, 2001, 6 pgs.  |                |
|   | IV.                   | Illusive Security, Wolves In Sheep's Clothing: malicious DLLs Injected Into trusted Host Applications, Author Unknown, <a href="http://home.arcor.de/scheinsicherheit/dll.htm">http://home.arcor.de/scheinsicherheit/dll.htm</a> 13 pgs.                        |                |
|   | V.                    | DevX.com, Intercepting Systems API Calls, by Seung-Woo Kim, May 13, 2004, 6 pgs.  |                |
|   | VI.                   | Microsoft.com, How To Subclass A Window in Windows 95, Article ID 125680, July 11, 2005, 2 pgs.   |                |
|   | VII.                  | MSDN, by Kyle Marsh, July 29, 1993, 15 pgs.   |                |
|   | VII.                  | PCT Search Report, PCT/US05/34874, 07/05/06, 7 Pages  |                |

|                    |  |                 |  |
|--------------------|--|-----------------|--|
| Examiner Signature |  | Date Considered |  |
|--------------------|--|-----------------|--|

\*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

<sup>1</sup> Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3).  
<sup>2</sup> For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document.  
<sup>3</sup> Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible.  
<sup>4</sup> Applicant is to place a check mark here if English language Translation is attached.

<sup>1</sup> Unique citation designation number.  
<sup>2</sup> Applicant is to place a check mark here if English language Translation attached.

Required Reading for IT Professionals: Delivering Intelligent Network Access Through Identity Driven Manager

[Trigent: Software Development](#)   
 [Close more deals by knowing who's most interested!](#)   
 [Numara Software: Network Management Software](#)   
 [eWork Markets: IT](#)

[ydesigns.com: Web Site Development](#)   
 [Web Store Builders: AmeriCommerce](#)   
 [ydesigns.com: Web Store Design](#)   
 [Web Design Price](#)

IT MANAGEMENT    NETWORKING    WEB DEVELOPMENT    HARDWARE & SYSTEMS    SOFTWARE DEVELOPMENT    IT NEWS



SEARCH: CodeGuru.com



Developer • Gamelan • Jars • Wireless • Discussion

- CodeGuru Navigation:**
- [Visual C++ / C++](#)
- [.NET / C#](#)
- [Visual Basic](#)
- [Videos](#)
- [Submit an Article](#)
- [Discussion Forums](#)
- [Resource Directory](#)
- [Announcements](#)
- [Book List](#)
- [Book Reviews](#)
- [List of Gurus](#)
- [Guest Book](#)
- [About Us](#)
- [FAQs](#)
- [Site Map](#)

Home >> [Visual C++ / C++](#) >> [Windows Programming](#) >> [System](#) >> [Processes / Modules](#)

**Whitepaper: 4 Steps to Developing a Service Management Strategy for Midsized Business.** [Learn how to manage IT processes & assets while improving service & security, reducing costs, & achieving compliance.](#)

## Three Ways To Inject Your Code Into Another Process

Rating: ★★★★★

**Robert Kuster** ([view profile](#))  
August 4, 2003

Environment: VC6 SP4, Win 2000 SP2

Key Words: Code Injection, Windows Hooks, Remote Threads

### Contents

- [Introduction](#)
- [Windows Hooks](#)
- [The CreateRemoteThread & LoadLibrary Technique](#)
  - [Interprocess Communications](#)
- [The CreateRemoteThread & WriteProcessMemory Technique](#)
  - [How to Subclass a Remote Control With this Technique](#)
  - [When to Use this Technique](#)
- [Some Final Words](#)
- [Appendixes](#)
- [References](#)
- [Downloads](#)
- [Article History](#)
- [Comments](#)

#### Member Sign In:

User ID: \_\_\_\_\_

Password: \_\_\_\_\_

Remember Me:



[Forgot Password?](#)

Not a member?  
[Click here for more](#)

### Introduction

(continued)

**BEST AVAILABLE COPY**

information and to register.

**HardwareCentral**  
**Compare Prices:**  
 go





- PDA's
- PC Notebooks
- Printers
- Monitors

**internet jobs** ▶


**internet.commerce**

- [Partners & Affiliates](#)
- [Email Marketing](#)
- [Memory](#)
- [Desktop Computers](#)
- [Cheap Plane Tickets](#)
- [Graphics Cards](#)
- [Promote Your Website](#)
- [IT Discount Club](#)
- [Compare Prices](#)
- [Televisions](#)
- [Web Hosting](#)
- [Inbound Calls](#)
- [Cheap Digital Camera](#)
- [Promotional Products](#)
- [IT Degrees](#)

**RSS Feeds**

-  All
-  VC++/C++
-  .NET/C#
-  VB


See more EarthWeb Network feeds




Get More Out of Your Datacenter

**AMD In the Enterprise**  
 An Online Series | Event #6  
**Happening NOW**

Get Started NOW :-

**AMD**   
 Smarter Choice

**AMD64 devSource** 

Embracing the full spectrum of developer needs including content supporting 64 bit, Multi-Core, Tools, and Optimization.

➤ **I/O Virtualization and AMD's IOMMU**

AMD64's virtualization extensions provide hardware support for VMM CPU virtualization, but that's only half the picture. I/O virtualization is the other half, and it's critical, because without hardware, I/O virtualization requires the high overhead of device emulation. [Read more.](#)

➤ **DB2 9 on AMD: A Perfect Match**

What happens when you pair IBM's latest and greatest data server, DB2 9, with AMD's leading-edge Opteron architecture? You get a blisteringly fast data server platform that makes the most of advances on both fronts. Learn how DB2 9 has been optimized for NUMA and x86-64 architecture, and how it works with AMD 64-bit multi-core. [Read more.](#)

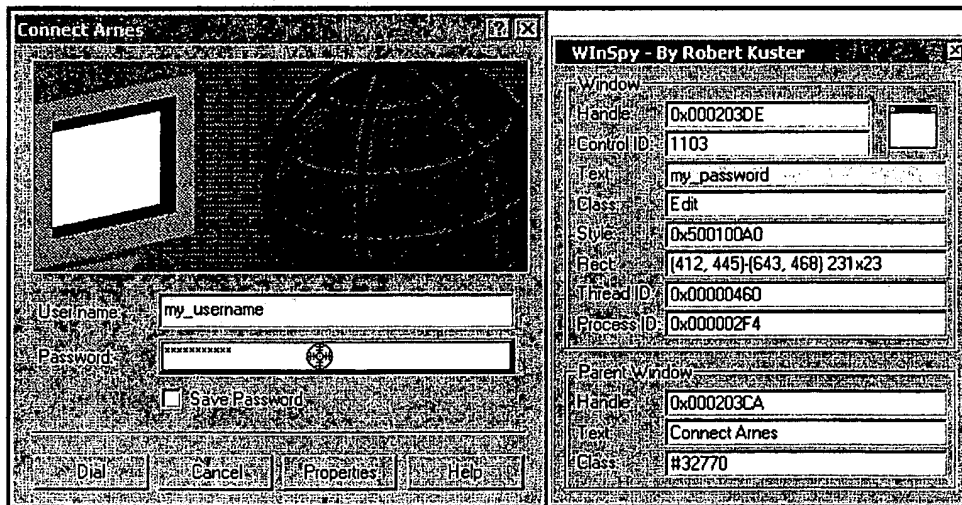
➤ **Virtualization Using AMD Servers and libVirt**

Virtualization as a tool for development and deployment has come of age. Hardware advancements from manufacturers like AMD, and software tools such as libVirt, make creating and managing virtual machines a breeze. Let's look at how AMD, Red Hat, and others are helping push the virtualization envelope. [Read more.](#)

➤ **Widen Your Opportunities with 64-Bit Compilers: Microsoft Visual Studio 2005**

Explore the capabilities and feature set of AMD's 64-bit compiler solution contained in Microsoft's Visual Studio. [Read more.](#)

➤ **For more relevant code samples, tutorials and editorials click here.**



[Click here for a larger image.](#)

Several password spy tutorials have been posted to [CodeGuru](#), but all of them rely on Windows any other way to make such a utility? Yes, there is. But first, let me review the problem briefly, we're all on the same page.

To "read" the contents of any control—either belonging to your application or not—you generally WM\_GETTEXT message to it. This also applies to edit controls, except in one special case. If the

to another process and the `ES_PASSWORD` style is set, this approach fails. Only the process that " password control can get its contents via `WM_GETTEXT`. So, our problem reduces to the following:

```

::SendMessage( hPwEdit, WM_GETTEXT, nMaxChars, psBuffer );

```

executed in the address space of another process.

In general, there are three possibilities to solve this problem:

- I. Put your code into a DLL; then, map the DLL to the remote process via [windows hooks](#).
- II. Put your code into a DLL and map the DLL to the remote process using the [CreateRemoteLoadLibrary](#) technique.
- III. Instead of writing a separate DLL, copy your code to the remote process directly—via `WriteProcessMemory`—and start its execution with `CreateRemoteThread`. A detailed description technique can be found [here](#).

## I. Windows Hooks

Demo applications: **HookSpy** and **HookInjEx**

The primary role of Windows hooks is to monitor the message traffic of some thread. In general

1. **Local hooks**, where you monitor the message traffic of any thread belonging to your process.
2. **Remote hooks**, which can be:
  - a. **thread-specific**, to monitor the message traffic of a thread belonging to another process.
  - b. **system-wide**, to monitor the message traffic for all threads currently running or

If the hooked thread belongs to another process (cases 2a & 2b), your hook procedure must res link library (DLL). The system then maps the DLL containing the hook procedure into the address hooked thread. Windows will map the entire DLL, not just the hook procedure. That is why `Wind used to inject code into another process's address space.`

While I won't discuss hooks in this article further (take a look at the `SetWindowsHookEx` API in MS details), let me give you two more hints that you won't find in the documentation, but might stil

1. After a successful call to `SetWindowsHookEx`, the system maps the DLL into the address : hooked thread automatically, but not necessary immediately. Because Windows hooks at messages, the DLL isn't really mapped until an adequate event happens. For example:

If you install a hook that monitors all nonqueued messages of some thread (`WH_CALL` won't be mapped into the remote process until a message is actually sent to (some w hooked thread. In other words, if `UnhookWindowsHook` is called before a message was hooked thread, the DLL will never be mapped into the remote process (although the `SetWindowsHookEx` itself succeeded). To force an immediate mapping, send an approp concerned thread right after the call to `SetWindowsHookEx`.

The same is true for unmapping the DLL after calling `UnhookWindowsHook`. The DLL isn't until an adequate event happens.

2. When you install hooks, they can affect the overall system performance (especially syste However, you can easily overcome this shortcoming if you use [thread-specific](#) hooks sole mapping mechanism, and not to trap messages. Consider the following code snippet:

```

BOOL WINAPI DllMain( HANDLE hModule,
                    DWORD ul_reason_for_call,

```



```

        LPVOID lpReserved )
    {
        if( ul_reason_for_call == DLL_PROCESS_ATTACH )
        {
            // Increase reference count via LoadLibrary
            char lib_name[MAX_PATH];
            ::GetModuleFileName( hDll, lib_name, MAX_PATH );
            ::LoadLibrary( lib_name );

            // Safely remove hook
            ::UnhookWindowsHookEx( g_hHook );
        }
        return TRUE;
    }
}

```

So, what happens?

First, we map the DLL to the remote process via Windows hooks. Then, right after the DLL been mapped, we unhook it. Normally, the DLL would be unmapped now, too, as soon as to the hooked thread would arrive. The dodgy thing is we prevent this unmapping by inc reference count via `LoadLibrary`.

The question that remains is: How to unload the DLL now, once we are finished? `UnhookWindowsHookEx` won't do it because we unhooked the thread already. You could do it this way:

- Install another hook, just before you want to unmap the DLL;
- Send a "special" message to the remote thread;
- Catch this message in your hook procedure; in response, call `FreeLibrary & UnhookWindowsHookEx`.

Now, hooks are used only while mapping/unmapping the DLL to/from the remote process; influence on the performance of the "hooked" thread in the meantime. Put another way: mapping mechanism that doesn't interfere the target process more than the `LoadLibrary` discussed below does (see [Section II.](#)). However, opposed to the `LoadLibrary` technique works on both WinNT and Win9x.

But, when should one use this trick?

Always when the DLL has to be present in the remote process for a longer period of time (subclass a control belonging to another process) and you want to interfere the target process as little as possible. I didn't use it in `HookSpy` because the DLL there is injected just for a moment—to get the password. I rather provided another example—`HookInjEx`—to demonstrate it. `HookInjEx` maps/unmaps a DLL into "explorer.exe", where it subclasses the Start button. More precisely, it intercepts left and right mouse clicks for the Start button.

You will find `HookSpy` and `HookInjEx` as well as their sources in the download package at [the end of the article](#).

## II. The CreateRemoteThread & LoadLibrary Technique

Demo application: `LibSpy`

In general, any process can load a DLL dynamically by using the `LoadLibrary` API. But, how do we call this function in an external process? The answer is `CreateRemoteThread`.

Let's take a look at the declaration of the `LoadLibrary` and `FreeLibrary` APIs first:

```

HINSTANCE LoadLibrary(
    LPCTSTR lpLibFileName // address of filename of library module
);

```

```

BOOL FreeLibrary(
    HMODULE hLibModule // handle to loaded library module
);

```

Now, compare them with the declaration of `ThreadProc`—the thread routine—passed to `CreateRemoteThread`.

```

DWORD WINAPI ThreadProc(
    LPCVOID lpParameter // thread data
);

```

As you can see, all functions use the same calling convention and all accept a 32-bit parameter. The returned value is the same. In other words: We may pass a pointer to `LoadLibrary/FreeLibrary` thread routine to `CreateRemoteThread`.

However, there are two problems (see the description for `CreateRemoteThread` [below](#)):

1. The `lpStartAddress` parameter in `CreateRemoteThread` must represent the starting address of the routine in the remote process.
2. If `lpParameter`—the parameter passed to `ThreadFunc`—is interpreted as an ordinary 32-bit pointer (`FreeLibrary` interprets it as an `HMODULE`), everything is fine. However, if `lpParameter` is a `char` pointer (`LoadLibraryA` interprets it as a pointer to a `char` string), it must point to some valid process.

The first problem is actually solved by itself. Both `LoadLibrary` and `FreeLibrary` are functions re `kernel32.dll`. Because `kernel32.dll` is guaranteed to be present and at the same load address in every process (see [Appendix A](#)), the address of `LoadLibrary/FreeLibrary` is the same in every process. Thus, that a valid pointer is passed to the remote process.

The second problem is also easy to solve: Simply copy the DLL module name (needed by `LoadLibrary`) to the remote process via `WriteProcessMemory`.

So, to use the [CreateRemoteThread & LoadLibrary technique](#), follow these steps:

1. Retrieve a `HANDLE` to the remote process (`OpenProcess`).
2. Allocate memory for the DLL name in the remote process (`VirtualAllocEx`).
3. Write the DLL name, including full path, to the allocated memory (`WriteProcessMemory`).
4. Map your DLL into the remote process via `CreateRemoteThread & LoadLibrary`.
5. Wait until the remote thread terminates (`WaitForSingleObject`); this is until the call to `LoadLibrary` returns. Put another way, the thread will terminate as soon as our `DllMain` (called with `DLL_PROCESS_ATTACH`) returns.
6. Retrieve the exit code of the remote thread (`GetExitCodeThread`). Note that this is the `DWORD` returned by `LoadLibrary`, thus the base address (`HMODULE`) of our mapped DLL.
7. Free the memory allocated in Step #2 (`VirtualFreeEx`).
8. Unload the DLL from the remote process via `CreateRemoteThread & FreeLibrary`. Pass the handle retrieved in Step #6 to `FreeLibrary` (via `lpParameter` in `CreateRemoteThread`).  
Note: If your injected DLL spawns any new threads, be sure they are all terminated before Step #8.
9. Wait until the thread terminates (`WaitForSingleObject`).

Also, don't forget to close all the handles once you are finished: To both threads, created in Step #4, and to the handle to the remote process, retrieved in Step #1.

Let's examine some parts of `LibSpy`'s sources now, to see how the above steps are implemented. For the sake of simplicity, error handling and unicode support are removed.

```

HANDLE hThread;
char szLibPath[_MAX_PATH]; // The name of our "LibSpy.dll"
                               // module (including full path!);

```

```

void* pLibRemote; // The address (in the remote process)
// where szLibPath will be copied to;
DWORD hLibModule; // Base address of loaded module (==HMODULE);

// initialize szLibPath
//...

// 1. Allocate memory in the remote process for szLibPath
// 2. Write szLibPath to the allocated memory
pLibRemote = ::VirtualAllocEx( hProcess, NULL, sizeof(szLibPath),
                               MEM_COMMIT, PAGE_READWRITE );
::WriteProcessMemory( hProcess, pLibRemote, (void*)szLibPath,
                      sizeof(szLibPath),NULL );

// Load "LibSpy.dll" into the remote process
// (via CreateRemoteThread & LoadLibrary)
hThread = ::CreateRemoteThread( hProcess, NULL, 0,
                               (LPTHREAD_START_ROUTINE)::GetProcAddress(
                                   ::GetModuleHandle("Kernel32"), "LoadLibraryA"),
                               pLibRemote, 0, NULL );
::WaitForSingleObject( hThread, INFINITE );

// Get handle of the loaded module
::GetExitCodeThread( hThread, &hLibModule );

// Clean up
::CloseHandle( hThread );
::VirtualFreeEx( hProcess, pLibRemote,
                 sizeof(szLibPath),MEM_RELEASE );

```

Assume our `SendMessage`—the code that we actually wanted to inject—was placed in `DllMain (DLL_PROCESS_ATTACH)`, so it has already been executed by now. Then, it is time to unload the C process:

```

// Unload "LibSpy.dll" from the target process
// (via CreateRemoteThread & FreeLibrary)
hThread = ::CreateRemoteThread( hProcess, NULL, 0,
                               (LPTHREAD_START_ROUTINE)::GetProcAddress(
                                   ::GetModuleHandle("Kernel32"), "FreeLibrary"),
                               (void*)hLibModule,
                               0, NULL );
::WaitForSingleObject( hThread, INFINITE );

// Clean up
::CloseHandle( hThread );

```

## Interprocess Communications

Until now, we only talked about how to inject the DLL into the remote process. However, in most injected DLL will need to communicate with your original application in some way (recall that the DLL is injected into some remote process now, not to our local application!). Take our Password Spy: The DLL has a handle to the control that actually contains the password. Obviously, this value can't be hard-coded at compile time. Similarly, once the DLL gets the password, it has to send it back to our application appropriately.

Fortunately, there are many ways to deal with this situation: File Mapping, `WM_COPYDATA`, the CLI sometimes very handy `#pragma data_seg`, to name just a few. I won't describe these techniques they are all well documented either in MSDN (see Interprocess Communications) or in other tutorials. I used solely the `#pragma data_seg` in the LibSpy example.

You will find LibSpy and its sources in the download package [at the end](#) of the article.

### III. The CreateRemoteThread & WriteProcessMemory Technique

#### Demo application: WinSpy

Another way to copy some code to another process's address space and then execute it in the process involves the use of remote threads and the WriteProcessMemory API. Instead of writing you copy the code to the remote process directly now—via WriteProcessMemory—and start its execution with CreateRemoteThread.

Let's take a look at the declaration of CreateRemoteThread first:

```
HANDLE CreateRemoteThread(
    HANDLE hProcess,          // handle to process to create thread in
    LPSECURITY_ATTRIBUTES lpThreadAttributes, // pointer to security
                                                // attributes
    DWORD dwStackSize,      // initial thread stack size, in bytes
    LPTHREAD_START_ROUTINE lpStartAddress,    // pointer to thread
                                                // function
    LPVOID lpParameter,     // argument for new thread
    DWORD dwCreationFlags,  // creation flags
    LPDWORD lpThreadId      // pointer to returned thread identifier
);
```

If you compare it to the declaration of CreateThread (MSDN), you will notice the following differences:

- The *hProcess* parameter is additional in CreateRemoteThread. It is the handle to the process in which the thread is to be created.
- The *lpStartAddress* parameter in CreateRemoteThread represents the starting address in the remote process's address space. **The function must exist in the remote process**, so we have to pass a pointer to the local ThreadFunc. We have to copy the code to the remote process.
- Similarly, the data pointed to by *lpParameter* must exist in the remote process, so we have to copy it there, too.

Now, we can summarize this technique in the following steps:

1. Retrieve a HANDLE to the remote process (OpenProcess).
2. Allocate memory in the remote process's address space for injected data (VirtualAlloc).
3. Write a copy of the initialised INJDATA structure to the allocated memory (WriteProcessMemory).
4. Allocate memory in the remote process's address space for injected code.
5. Write a copy of ThreadFunc to the allocated memory.
6. Start the remote copy of ThreadFunc via CreateRemoteThread.
7. Wait until the remote thread terminates (WaitForSingleObject).
8. Retrieve the result from the remote process (ReadProcessMemory or GetExitCodeThread).
9. Free the memory allocated in Steps #2 and #4 (VirtualFreeEx).
10. Close the handles retrieved in Steps #6 and #1 (CloseHandle).

Additional caveats that ThreadFunc has to obey:

1. ThreadFunc should not call any functions besides those in **kernel32.dll** and **user32.dll**; **user32** are, if present (note that *user32* isn't mapped into every Win32 process!), guaranteed to have the same load address in both the local and the target process (see [Appendix A](#)). If you need to load other libraries, pass the addresses of LoadLibrary and GetProcAddress to the injected code and get the rest itself. You could also use GetModuleHandle instead of LoadLibrary, if fi

reason the debatable DLL is already mapped into the target process.

Similarly, if you want to call your own subroutines from within `ThreadFunc`, copy each rc remote process individually and supply their addresses to `ThreadFunc` via `INJDATA`.

2. Don't use any static strings. Rather pass all strings to `ThreadFunc` via `INJDATA`. Why? The compiler puts all static strings into the ".data" section of an executable and on (=pointers) remain in the code. Then, the copy of `ThreadFunc` in the remote process won't have something that doesn't exist (at least not in its address space).
3. Remove the `/GZ` compiler switch; it is set by default in debug builds (see [Appendix B](#)).
4. Either declare `ThreadFunc` and `AfterThreadFunc` as `static` or disable incremental linking.
5. There must be less than a page-worth (4 Kb) of local variables in `ThreadFunc` (see [Appendix C](#)). In debug builds some 10 bytes of the available 4 Kb are used for internal variables.
6. If you have a `switch` block with more than three case statements, either split it up like t

```
switch( expression ) {
    case constant1: statement1; goto END;
    case constant2: statement2; goto END;
    case constant3: statement2; goto END;
}
switch( expression ) {
    case constant4: statement4; goto END;
    case constant5: statement5; goto END;
    case constant6: statement6; goto END;
}
END:
```

or modify it into an `if-else if` sequence (see [Appendix E](#)).

7. ...

You will almost certainly crash the target process if you don't play by those rules. Just remember anything in the target process is at the same address as it is in your process (see [Appendix F](#)).

## GetWindowTextRemote(A/W)

All the functionality you need to get the password from a "remote" edit control is encapsulated in `GetWindowTextRemot(A/W)`:

```
int GetWindowTextRemoteA( HANDLE hProcess, HWND hWnd, LPSTR
lpString );
int GetWindowTextRemoteW( HANDLE hProcess, HWND hWnd, LPWSTR
lpString );
```

## Parameters

*hProcess*

Handle to the process the edit control belongs to.

*hWnd*

Handle to the edit control containing the password.

*lpString*

Pointer to the buffer that is to receive the text.

## Return Value

The return value is the number of characters copied.

Let's examine some parts of its sources now—especially the injected data and code—to see how `GetWindowTextRemote` works. Again, unicode support is removed for the sake of simplicity.

## INJDATA

```
typedef LRESULT      (WINAPI *SENDMESSAGE) (HWND, UINT, WPARAM, LPARAM) ;

typedef struct {
    HWND hwnd;           // handle to edit control
    SENDMESSAGE fnSendMessage; // pointer to user32!SendMessageA

    char psText[128];    // buffer that is to receive the password
} INJDATA;
```

`INJDATA` is the data structure being injected into the remote process. However, before doing so pointer to `SendMessageA` is initialised in our application. The dodgy thing here is that `user32.dll` always mapped to the same address in every process; thus, the address of `SendMessageA` is always the same. This ensures that a valid pointer is passed to the remote process.

## ThreadFunc

```
static DWORD WINAPI ThreadFunc (INJDATA *pData)
{
    pData->fnSendMessage( pData->hwnd, WM_GETTEXT, // Get password
                          sizeof(pData->psText),
                          (LPARAM)pData->psText );

    return 0;
}

// This function marks the memory address after ThreadFunc.
// int cbCodeSize = (PBYTE) AfterThreadFunc - (PBYTE) ThreadFunc.
static void AfterThreadFunc (void)
{
}
}
```

`ThreadFunc` is the code executed by the remote thread. Point of interest:

- Note how `AfterThreadFunc` is used to calculate the code size of `ThreadFunc`. In general idea, because the linker is free to change the order of your functions (i.e. it could place `AfterThreadFunc` before `ThreadFunc`). However, you can be pretty sure that in small projects, like our Win32 applications, your functions will be preserved. If necessary, you also could use the `/ORDER` linker option or yet better: Determine the size of `ThreadFunc` with a disassembler.

## How to Subclass a Remote Control with This Techn

Demo application: `InjectEx`

Let's explain something more complicated now: how to subclass a control belonging to another process using this technique.

First of all, note that you have to copy two functions to the remote process to accomplish this task:

1. `ThreadFunc`, which actually subclasses the control in the remote process via `SetWindowLong`.
2. `NewProc`, the new window procedure of the subclassed control.

However, the main problem is how to pass data to the remote `NewProc`. Because `NewProc` is a callback function, it cannot pass data back to the caller.

and thus has to conform to specific guidelines, we can't simply pass a pointer to INJDATA to it as: Fortunately, there are other ways to solve this problem (I found two), but all rely on the assembly when I tried to preserve the assembly for the appendixes until now, it won't go without it this ti

## Solution 1

Observe the following picture:

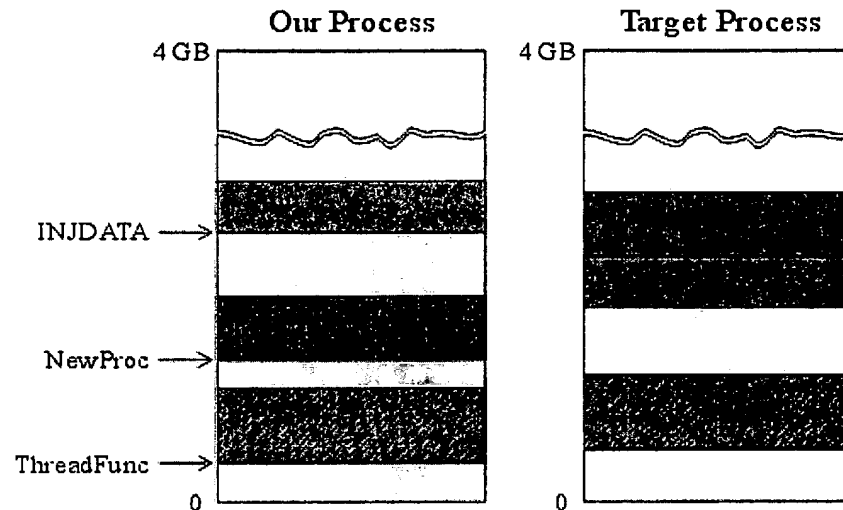


Figure 2: The virtual address space

Note that INJDATA is placed immediately before NewProc in the remote process? This way NewProc memory location of INJDATA in the remote processes address space at compile time. More precise address of INJDATA relative to its own location, but that's actually all we need. Now NewProc mi

```
static LRESULT CALLBACK NewProc(
    HWND hwnd,        // handle to window
    UINT uMsg,        // message identifier
    WPARAM wParam,    // first message parameter
    LPARAM lParam )   // second message parameter
{
    INJDATA* pData = (INJDATA*) NewProc; // pData points to
                                        // NewProc;
    pData--; // now pData points to INJDATA;
            // recall that INJDATA in the remote
            // process is immediately before NewProc;

    //-----
    // subclassing code goes here
    // .....
    //-----

    // call original window procedure;
    // fnOldProc (returned by SetWindowLong) was initialised by
    // (the remote) ThreadFunc and stored in (the remote) INJDATA;
    return pData->fnCallWindowProc( pData->fnOldProc,
                                    hwnd, uMsg, wParam, lParam );
}
```

However, there is still a problem. Observe the first line:

```
INJDATA* pData = (INJDATA*) NewProc;
```

This way, a hard-coded value (the memory location of the original `NewProc` in our process) will be stored in `pData`. That is not quite what we want: The memory location of the "current" copy of `NewProc` in the remote process, regardless of to what location it is (`NewProc`) actually moved. In other words, we would have a "this pointer."

While there is no way to solve this in C/C++, it can be done with inline assembly. Consider the following:

```
static LRESULT CALLBACK NewProc(
    HWND hwnd,          // handle to window
    UINT uMsg,          // message identifier
    WPARAM wParam,      // first message parameter
    LPARAM lParam )     // second message parameter
{
    // calculate location of the INJDATA struct
    // (remember that INJDATA in the remote process
    // was placed immediately before NewProc)
    INJDATA* pData;
    _asm {
        call    dummy
dummy:
        pop    ecx    // <- ECX contains the current EIP
        sub    ecx, 9  // <- ECX contains the address of NewProc
        mov    pData, ecx
    }
    pData--;

    //-----
    // subclassing code goes here
    // .....
    //-----

    // call original window procedure
    return pData->fnCallWindowProc( pData->fnOldProc,
                                    hwnd, uMsg, wParam, lParam );
}
```

So, what's going on?

Virtually every processor has a special register that points to the memory location of the next instruction to be executed. That's the so-called instruction pointer, denoted EIP on 32-bit Intel and AMD processors. As a special-purpose register, you can't access it programmatically as you can a general purpose register. Put another way: There is no OpCode, with which you could address EIP and read or change its value explicitly. However, EIP can still be changed (and is changed all the time) implicitly, by instructions like `CALL` and `RET`. Let's, for example, explain how the subroutine `CALL/RET` mechanism works on 32-bit processors:

When you call a subroutine (via `CALL`), the address of the subroutine is loaded into EIP. But, before EIP is modified, its old value is automatically pushed onto the stack (for use later as a return instruction). At the end of a subroutine, the `RET` instruction automatically pops the top of the stack into EIP.

Now you know how EIP is modified via `CALL` and `RET`, but how to get its current value?

Well, remember that `CALL` pushes EIP onto the stack? So, in order to get its current value call `CALL` and pop the stack right thereafter. Let's explain the whole trick at our compiled `NewProc`:

| Address   | OpCodes | Params | Decoded instruction               |
|-----------|---------|--------|-----------------------------------|
| :00401000 | 55      |        | push ebp ; entry point of NewProc |



```

:00401001 8BEC          mov ebp, esp
:00401003 51             push ecx
:00401004 E800000000    call 00401009      ; *a*   call dummy
:00401009 59             pop ecx           ; *b*
:0040100A 83E909       sub ecx, 00000009 ; *c*
:0040100D 894DFC       mov [ebp-04], ecx ; mov pData, ECX
:00401010 8B45FC       mov eax, [ebp-04]
:00401013 83E814       sub eax, 00000014 ; pData--;
.....
.....
:0040102D 8BE5          mov esp, ebp
:0040102F 5D             pop ebp
:00401030 C21000       ret 0010

```

- A dummy function call; it just jumps to the next instruction and pushes EIP onto the stack.
- Pop the stack into ECX. ECX then holds EIP; this is exactly the address of the "pop ECX" instruction.
- Note that the "distance" between the entry point of `NewProc` and the "pop ECX" instruction to calculate the address of `NewProc`, subtract 9 from ECX.

This way, `NewProc` can always calculate its own address, regardless of to what location it is actually located. However, be aware that the distance between the entry point of `NewProc` and the "pop ECX" instruction can change as you change your compiler/linker options, and is thus different in release and debug builds. The point is that you still know the exact value at compile time:

- First, compile your function.
- Determine the correct distance with a disassembler.
- Finally, recompile with the correct distance.

That's the solution used in `InjectEx`. `InjectEx`, similarly as `HookInjEx`, swaps the left and right mouse buttons.

## Solution 2

Placing `INJDATA` right before `NewProc` in the remote process's address space isn't the only way to solve this problem. Consider the following variant of `NewProc`:

```

static LRESULT CALLBACK NewProc(
    HWND hwnd,          // handle to window
    UINT uMsg,          // message identifier
    WPARAM wParam,      // first message parameter
    LPARAM lParam )     // second message parameter
{
    INJDATA* pData = 0xA0B0C0D0; // a dummy value

    //-----
    // subclassing code goes here
    // .....
    //-----

    // call original window procedure
    return pData->fnCallWindowProc( pData->fnOldProc,
                                     hwnd, uMsg, wParam, lParam );
}

```

Here, `0xA0B0C0D0` is just a placeholder for the real (absolute!) address of `INJDATA` in the remote process. Recall that you can't know this address at compile time. However, you do know the location of the remote process right after the call to `VirtualAllocEx` (for `INJDATA`) is made.

Our `NewProc` could compile into something like this:

| Address   | OpCode&Params | Decoded instruction    |
|-----------|---------------|------------------------|
| :00401000 | 55            | push ebp               |
| :00401001 | 8BEC          | mov ebp, esp           |
| :00401003 | C745FC0C0B0A0 | mov [ebp-04], A0B0C0D0 |
| :0040100A | ...           |                        |
| ....      |               |                        |
| :0040102D | 8BE5          | mov esp, ebp           |
| :0040102F | 5D            | pop ebp                |
| :00401030 | C21000        | ret 0010               |

...thus, its compiled code (in hexadecimal) would be: 558BECC745FC0C0B0A0.....8BE55DC21000

Now, you would proceed as follows:

1. Copy INJDATA, ThreadFunc and NewProc to the target process.
2. Change the code of NewProc, so that pData holds the real address of INJDATA. For example, let's say the address of INJDATA (the value returned by VirtualAllocEx) in the process is 0x008a0000. Then you modify the code of NewProc as follows:
 

```
558BECC745FC0C0B0A0.....8BE55DC21000      ← original NewProc 1
558BECC745FC0008A00.....8BE55DC21000      ← modified NewProc with real
                                                INJDATA
```

Put another way: You replace the dummy value A0B0C0D0 with the real address of INJDATA.
3. Start execution of the remote ThreadFunc, which in turn subclasses the control in the remote process.

<sup>1</sup> One might wonder why the addresses A0B0C0D0 and 008a0000 in the compiled code appear in because Intel and AMD processors use the little-endian notation for to represent their (multi-byte words): The low-order byte of a number is stored in memory at the lowest address, and the high highest address.

Imagine the word UNIX stored in four bytes. In big-endian systems, it would be stored as UNIX. In little-endian systems, it would be stored as XINU.

<sup>2</sup> Some (bad) cracks modify the code of an executable in a similar way. However, once loaded in the target process, the program can't change its own code (the code resides in the ".text" section of an executable, which is protected). Still we could modify our remote NewProc, because it was previously copied to a page with PAGE\_EXECUTE\_READWRITE permission.

## When to use the CreateRemoteThread & WriteProcessMemory technique

The CreateRemoteThread & WriteProcessMemory technique of code injection is, when compared to other methods, more flexible in that you don't need an additional DLL. Unfortunately, it is also more risky than the other methods. You can (and most probably will) easily crash the remote process if something is wrong with your ThreadFunc (see [Appendix F](#)). Because debugging a remote thread is a nightmare, you should use this technique only when injecting at most a few instructions. To inject a large amount of code, use one of the methods discussed in Sections II and I.

Again, WinSpy and InjectEx, as well as their sources, can be found in the download package at [this](#) article.

## Some Final Words

At the end, let's summarize some facts we didn't mention so far:

|  | OS              | Processes                      |
|--|-----------------|--------------------------------|
| I. Hooks                                     | Win9x and WinNT | only processes that link with  |
| II. CreateRemoteThread & LoadLibrary         | WinNT only 2*   | all processes 3*, including 4* |
| III. CreateRemoteThread & WriteProcessMemory | WinNT only      | all processes, including 5     |

1. Obviously you can't hook a thread that has no message queue. Also, `SetWindowsHookEx` system services, even if they link against `USER32.DLL`.
2. There is no `CreateRemoteThread` nor `VirtualAllocEx` on Win9x. (Actually, they can be Win9x, too; but that's a story for yet another day.)
3. **All processes = All Win32 processes + `csrss.exe`**  
Native applications (`smss.exe`, `os2ss.exe`, `autochk.exe`, etc) don't use Win32 APIs, and they link against `kernel32.dll` either. The only exception is `csrss.exe`, the Win32 subsystem itself. It's a native application but some of its libraries (`~winsrv.dll`) require Win32 DLLs, including `kernel32.dll`.
4. If you want to inject code into system services (`lsass.exe`, `services.exe`, `winlogon.exe`, or `csrss.exe`, set the privileges of your process to "SeDebugPrivilege" (`AdjustTokenPrivileges`), then `OpenProcess` to get a handle to the remote process (`OpenProcess`).

That's almost it. There is just one more thing that you should bear in mind: Your injected code could do something wrong with it, easily pull the target process down to oblivion with it. Just remember to be responsible with responsibility!

Because many examples in this article were about passwords, you might find it interesting to read [Super Password Spy++](#), written by Zhefu Zhang, too. There he explains how to get the password from the Internet Explorer password field. More. He even shows you how to protect your password from password attacks.

Last note: The only reward someone gets for writing and publishing an article is the feedback he found it useful, simply drop in a comment. But even more importantly: Let me know if something is buggy, if you think something could be done better, or that something is still left unclear.

## Acknowledgments

First, thanks to all my readers here at CodeGuru. It is mainly because of your questions, that that was its initial 1200 words to what it is today: An 6000 word "animal." However, if there is someone I deserve to be singled out, then it is Rado Picha. Parts of the article greatly benefited from his explanations to me. Last, but not least, thanks to Susan Moore for helping me through that minor English language, and making my article more readable.

## Appendixes

A) Why are `KERNEL32.DLL` and `USER32.DLL` always mapped to the same address?

My presumption: Because Microsoft programmers thought that it could be a useful speed optimization. Let's explain why.

In general, an executable is composed of several sections, including a ".reloc" section.

When the linker creates an EXE or DLL file, it makes an assumption about where the file will be loaded into memory. That's the so-called assumed/preferred load/base address. All the absolute addresses in the image are based on this linker assumed load address. If for whatever reason the image is loaded at a different address, the PE—portable executable—loader has to fix all the absolute addresses in the image. This is where the ".reloc" section comes in: It contains a list of all the places in the image, where the linker assumed load address and the actual load address needs to be factored in. (Note that most of the instructions produced by the compiler use some kind of relative addressing, so there are not as many relocations as you might think). If, on the other side, the image is loaded at the linker's preferred base address, the ".reloc" section is completely ignored.

But, how do *kernel32.dll*, *user32.dll* and their load addresses fit into the story? Because every Win32 application needs *kernel32.dll*, and most of them need *user32.dll*, improve the load time of all executables by always mapping them (*kernel32* and *user32*) bases. Then the loader must never fix any (absolute) addresses in *kernel32.dll* and *user32.dll*.

Let's close out this discussion with the following example:

```
Set the image base of some App.exe to KERNEL32's (/base:"0x77e80000") or to USER32 (/base:"0x77e10000") preferred base. If App.exe doesn't import from USER32, just :
Then compile App.exe and try to run it. An error box pops up ("Illegal System DLL Re
App.exe fails to load.
```

Why? When creating a process, the loader on Win 2000, Win XP and Win 2003 checks if *user32.dll* (their names are hardcoded into the loader) are mapped at their preferred base. If not, an error is raised. In WinNT 4 *ole32.dll* was also checked. In WinNT 3.51 and lower such checks are not present, so *kernel32.dll* and *user32.dll* could be anywhere. Anyway, the only module that the loader checks is *ntdll.dll*. The loader doesn't check it, but if *ntdll.dll* is not at its base, the process creation fails.

To summarize, on WinNT 4 and higher:

- DLLs, that are always mapped to their bases: *kernel32.dll*, *user32.dll* and *ntdll.dll*
- DLLs that are present in every Win32 application (+ *csrss.exe*): *kernel32.dll* and *user32.dll*
- The only DLL that is present in every process, even in native applications: *ntdll.dll*

#### B) The /GZ compiler switch

In Debug builds, the /GZ compiler feature is turned on by default. You can use it to catch errors (see the documentation for details). But what does it mean to our executable?

When /GZ is turned on, the compiler will add some additional code to every function in every executable, including a function call (added at the very end of every function) that verifies if the pointer hasn't changed through our function. But wait, a function call is added to *ThreadFunc* and *AfterThreadFunc*. Now the remote copy of *ThreadFunc* will call a function that doesn't exist in the process (at least not at the same address).

#### C) Static functions Vs. Incremental linking

Incremental linking is used to shorten the linking time when building your applications. The difference between normally and incrementally linked executables is that in incrementally linked executables, a call goes through an extra *JMP* instruction emitted by the linker (an exception to this rule is functions declared as static!). These *JMPS* allow the linker to move the functions around in memory and update all the *CALL* instructions that reference the function. But it's exactly this *JMP* that causes *ThreadFunc* and *AfterThreadFunc* will point to the *JMP* instructions instead to the real code. Calculating the size of *ThreadFunc* this way:

```
const int cbCodeSize = ((LPBYTE) AfterThreadFunc
                        - (LPBYTE) ThreadFunc);
```

you will actually calculate the "distance" between the *JMPS* that point to *ThreadFunc* and *AfterThreadFunc* respectively (usually they will appear one right after the other; but don't count on this). *ThreadFunc* is at address 004014C0 and the accompanying *JMP* instruction at 00401020.

```
:00401020  jmp  004014C0
...
:004014C0  push EBP          ; real address of ThreadFunc
:004014C1  mov  EBP, ESP
...
```

Then

```
WriteProcessMemory( .., &ThreadFunc, cbCodeSize, ..);
```

will copy the "JMP 004014C0" instruction (and all instructions in the range of `cbCodeSize` in the remote process—not the real `ThreadFunc`. The first thing the remote thread will execute is "JMP 004014C0". Well, it will also be among its last instructions—not only to the remote thread but to the remote process.

However, there is an exception to this JMP instruction "rule." If a function is declared as `__stdcall` and called directly, even if linked incrementally. That's why [Rule #4](#) says to declare `ThreadFunc` and `AfterThreadFunc` as `static` or disable incremental linking. (Some other aspects of incremental linking can be found in the article "Remove Fatty Deposits from Your Applications Using Our 32-bit Linker" by Matt Pietrek.)

#### D) Why can my `ThreadFunc` have only 4k of local variables?

Local variables are always stored on the stack. If a function has, say, 256 bytes of local variables, the stack pointer is decreased by 256 when entering the function (more precisely, in the function's prologue). The following function:

```
void Dummy(void) {
    BYTE var[256];
    var[0] = 0;
    var[1] = 1;
    var[255] = 255;
}
```

could, for instance, compile into something like this:

```
:00401000  push ebp
:00401001  mov  ebp, esp
:00401003  sub  esp, 00000100    ; change ESP as storage for
                        ; local variables is needed
:00401006  mov  byte ptr [esp], 00    ; var[0] = 0;
:0040100A  mov  byte ptr [esp+01], 01    ; var[1] = 1;
:0040100F  mov  byte ptr [esp+FF], FF    ; var[255] = 255;
:00401017  mov  esp, ebp            ; restore stack pointer
:00401019  pop  ebp
:0040101A  ret
```

Note how the stack pointer (ESP) was changed in the above example? But what if a function needs more than 4 Kb for its local variables? Well, then the stack pointer isn't changed and if another function (a stack probe) is called, which in turn changes it appropriately. But it's an additional function call that makes our `ThreadFunc` "corrupt," because its remote copy won't have something that's not there.

Let's see what the documentation says about stack probes and the `/Gs` compiler option:

**"The `/Gssize` option is an advanced feature with which you can control stack probes. A sequence of code that the compiler inserts into every function call. When activated, it reaches benignly into memory by the amount of space required to store the associated variables.**

**If a function requires more than `size` stack space for local variables, its stack probe is triggered. The default value of `size` is the size of one page (4 Kb for 80x86 processors). This value is tuned to the interaction between an application for Win32 and the Windows NT virtual-memory manager. You can increase the amount of memory committed to the program stack at run time."**

I'm sure one or another wondered about the above statement: "...a stack probe reaches

memory...". Those compiler options (their descriptions!) are sometimes really irritating, look under the hood and see what's going on. If, for instance, a function needs 12 Kb stack variables, the memory on the stack would be "allocated" (more precisely: committed) th

```

sub    esp, 0x1000    ; "allocate" first 4 Kb
test   [esp], eax     ; touches memory in order to commit a
                       ; new page (if not already committed)
sub    esp, 0x1000    ; "allocate" second 4 Kb
test   [esp], eax     ; ...
sub    esp, 0x1000
test   [esp], eax

```

Note how the stack pointer is changed in 4 Kb steps now and, more importantly, how the stack is "touched" (via `test`) after each step. This ensures the page containing the bottom being committed, before "allocating" (committing) another page.

After reading ..

"Each new thread receives its own stack space, consisting of both committed and reserved. By default, each thread uses 1 Mb of reserved memory, and one page of committed system will commit one page block from the reserved stack memory as needed." (see `CreateThread > dwStackSize > "Thread Stack Size"`).

... it should also be clear why the documentation about `/Gs` says that you get with stack tuned interaction between your application and the Windows NT virtual-memory manager.

Now back to our `ThreadFunc` and 4 Kb limit:

Although you could prevent calls to the stack probe routine with `/Gs`, the documentation does so. Further, the documentation says you can turn stack probes on or off by using the `check_stack` directive. However, it seems this pragma doesn't affect stack probes at all (documentation is buggy, or I am missing some other facts?). Anyway, recall that the `CreateProcessMemory` technique should be used only when injecting small pieces of code; variables should rarely \*consume\* more than a few bytes and thus not get even close to

E) Why should I split up my `switch` block with more than three `case` statements? Again, it is easiest to explain it with an example. Consider the following function:

```

int Dummy( int arg1 )
{
    int ret = 0;

    switch( arg1 ) {
        case 1: ret = 1; break;
        case 2: ret = 2; break;
        case 3: ret = 3; break;
        case 4: ret = 0xA0B0; break;
    }
    return ret;
}

```

It would compile into something like this:

| Address   | OpCode&Params | Decoded instruction                       |
|-----------|---------------|---|
| :00401000 | 8B4C2404      | mov ecx, dword ptr [esp+04] ; arg1 -> ECX |
| :00401004 | 33C0          | xor eax, eax ; EAX = 0                    |
| :00401006 | 49            | dec ecx ; ECX --                          |

```

:00401007 83F903          cmp ecx, 00000003
:0040100A 771E                ja 0040102A

; JMP to one of the addresses in table ***
; note that ECX contains the offset
:0040100C FF248D2C104000     jmp dword ptr [4*ecx+0040102C]

; case 1: eax = 1;
:00401013 B801000000         mov eax, 00000001
:00401018 C3                 ret

; case 2: eax = 2;
:00401019 B802000000         mov eax, 00000002
:0040101E C3                 ret

; case 3: eax = 3;
:0040101F B803000000         mov eax, 00000003
:00401024 C3                 ret

; case 4: eax = 0xA0B0;
:00401025 B8B0A00000         mov eax, 0000A0B0

:0040102A C3                 ret
:0040102B 90                 nop

; Address table ***
:0040102C 13104000          DWORD 00401013 ; jump to case 1
:00401030 19104000          DWORD 00401019 ; jump to case 2
:00401034 1F104000          DWORD 0040101F ; jump to case 3
:00401038 25104000          DWORD 00401025 ; jump to case 4

```

Note how the switch-case was implemented?

Rather than examining every single case statement separately, an address table is created to the right case by simply calculating the offset into the address table. If you think for a really is an improvement. Imagine you had a switch with 50 case statements. Without it had to execute 50 CMP and JMP instructions to get to the last case. With the address table you can jump to any case by a single table look-up. In terms of computer algorithms and We replace an  $O(2n)$  algorithm by an  $O(5)$  one, where:

1.  $O$  denotes the worst-case time complexity.
2. We assume five instructions are necessary to calculate the offset, do the table look-up, and jump to the appropriate address.

Now, one might think the above was possible only because the case constants were consecutive (1,2,3,4). Fortunately, it turns out the same solution can be applied to most examples, only the offset calculation becomes somewhat more complicated. But there are a few things to consider:

- if there are three or fewer case statements or
- if the case constants are completely unrelated to each other (i.e. "case 1", "case 1000")

then the resulting code does it the long way by examining every single case constant sequentially with CMP and JMP instructions. In other words, then the resulting code is essentially the same ordinary if-else if sequence.

Point of interest: If you ever wondered for what reason only a constant-expression can be used in a switch statement, then you know why by now. In order to create the address table, this value is known at compile time.

Now back to the problem!

Notice the JMP instruction at address 0040100C? Let's see what Intel's documentation says about the opcode FF:

| Opcode | Instruction | Description  |
|--------|-------------|--|
| FF /4  | JMP r/m32   | Jump near, <u>absolute indirect</u> , address given in r/m32 |

Oops, the debatable `JMP` uses some kind of absolute addressing? In other words, one of (0040102C in our case) represents an absolute address. Need I say more? Now, the remote process would blindly think the address table for its switch is at 0040102C, `JMP` to a wrong place effectively crash the remote process.

#### F) Why does the remote process crash, anyway?

When your remote process crashes, it will always be for one of the following reasons:

1. You referenced a string inside of `ThreadFunc` that doesn't exist.
2. One or more instructions in `ThreadFunc` use absolute addressing (see [Appendix E](#))
3. `ThreadFunc` calls a function that doesn't exist (the call could be added by the compiler). When you will look at `ThreadFunc` in disassembler in this case you will see something like:

```

:004014C0    push EBP           ; entry point of ThreadFunc
:004014C1    mov EBP, ESP
...
:004014C5    call 0041550       ; this will crash the
                        ; remote process
...
:00401502    ret

```

If the debatable `CALL` was added by the compiler (because some "forbidden" switch was turned on), it will be located either somewhere at the beginning or near the end of `ThreadFunc`. In any case, you can't be careful enough with the `CreateRemoteThread` & `WriteProcessMemory`. Especially watch for your compiler/linker options. They could easily add something to your code.

## References:

1. [Load Your 32-bit DLL into Another Process's Address Space Using INJLIB](#) by Jeffrey Richter
2. [HOWTO: Subclass a Window in Windows 95](#); Microsoft Knowledge Base Article - 125680
3. [Tutorial 24: Windows Hooks](#) by Iczelion
4. [CreateRemoteThread](#) by Felix Kasza
5. [API hooking revealed](#) by Ivo Ivanov
6. [Peering Inside the PE: A Tour of the Win32 Portable Executable File Format](#) by Matt Pietri
7. [Intel Architecture Software Developer's Manual, Volume 2: Instruction Set Reference](#)

## Downloads

[Download entire package - 174 Kb](#)

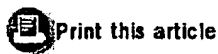
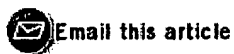
[Download WinSpy - 20 Kb](#) (demo application)

## Article History

### DEVELOPER SOLUTIONS

- ▶ Get the most out of Visual Studio. Visit the Microsoft Visual Studio Extensibility Portal on DevX.
- ▶ Webcast: Linux on Multi-Core--WAS CE and the Open Stack Appliance
- ▶ Developer.com Webcast: Defining Your Own Software Development Methodology.
- ▶ Get DB2 Express-C 9. Free to Develop, Deploy, Distribute. No limits--just data. Download Now!
- ▶ Generate Complete .NET Web Apps in Minutes . Download Iron Speed Designer today.





**RATE THIS ARTICLE:**  Excellent  Very Good  Average  Below Average  Poor

(You must be signed in to rank an article. Not a member? [Click here to register](#))

**Latest Comments:**

- [Bug fix](#) - tkho (08/04/2006)
- [memory edit](#) - wh1sp3r (01/05/2006)
- [Oops. Error in your article.](#) There is some inaccuracy in your explanation which bothers a little (08/31/2004)
- [@Robert Kuster > More precious](#) - Legacy CodeGuru (02/19/2004)
- [question](#) - Legacy CodeGuru (01/02/2004)

[View All Comments](#)

**Add a Comment:**

Title:

Comment:

**Pre-Formatted:**  Check this if you want the text to display with the formatting as typed (go code)



(You must be signed in to comment on an article. Not a member? [Click here to register](#))



Compare prices and save on:

| Laptops  | PDA's   | Digital Cameras   | Desktop Computers  |
|--|---|---|--|
| <ul style="list-style-type: none"> <li>▪ <a href="#">Toshiba Satellite</a></li> <li>▪ <a href="#">Powerbook G4</a></li> <li>▪ <a href="#">Sony Vaio VGN</a></li> <li>▪ <a href="#">Dell Inspiron 6000</a></li> <li>▪ <a href="#">IBM ThinkPad</a></li> </ul> | <ul style="list-style-type: none"> <li>▪ <a href="#">Palm One</a></li> <li>▪ <a href="#">Bluetooth</a></li> <li>▪ <a href="#">HP Ipaq</a></li> <li>▪ <a href="#">Dell Axim</a></li> <li>▪ <a href="#">I-Mate</a></li> </ul> | <ul style="list-style-type: none"> <li>▪ <a href="#">Olympus 740</a></li> <li>▪ <a href="#">Sony Cyber Shot</a></li> <li>▪ <a href="#">Nikon Coolpix</a></li> <li>▪ <a href="#">Canon S80</a></li> <li>▪ <a href="#">Panasonic DMC</a></li> </ul> | <ul style="list-style-type: none"> <li>▪ <a href="#">Graphics Cards</a></li> <li>▪ <a href="#">Sound Cards</a></li> <li>▪ <a href="#">Memory Cards</a></li> <li>▪ <a href="#">Motherboards</a></li> <li>▪ <a href="#">Gaming Software</a></li> </ul> |

Con

**JupiterWeb networks:**



Search JupiterWeb:

Search input field



Jupitermedia Corporation has two divisions: [Jupiterimages](#) and [JupiterWeb](#)

[Jupitermedia Corporate Info](#)

Copyright 2006 Jupitermedia Corporation All Rights Reserved.  
[Legal Notices](#), [Licensing](#), [Reprints](#), & [Permissions](#), [Privacy Policy](#).

[Web Hosting](#) | [Newsletters](#) | [Tech Jobs](#) | [Shopping](#) | [E-mail Offers](#)

**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

**BEST AVAILABLE IMAGES**


Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- BLACK BORDERS
- IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT OR DRAWING
- BLURRED OR ILLEGIBLE TEXT OR DRAWING
- SKEWED/SLANTED IMAGES
- COLOR OR BLACK AND WHITE PHOTOGRAPHS
- GRAY SCALE DOCUMENTS
- LINES OR MARKS ON ORIGINAL DOCUMENT
- REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- OTHER: \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**

 **Bee Information Technology: Improve the performance, reliability, and interoperability of your network. Read this case :**

- [Numara Software: Information Technology Services](#)
- [Numara Software: Network Management Software](#)
- [AMD Enterprise Event](#)
- [Numara Software: Management Softw](#)
- [Network Liquidators: Network Security Hardware](#)
- [At Battery Company: Original Dell Parts](#)
- [No one knows wireless like TESCO.](#)
- [Citrix Access Gate](#)

IT MANAGEMENT   NETWORKING   WEB DEVELOPMENT   HARDWARE & SYSTEMS   SOFTWARE DEVELOPMENT   IT NEWS



SEARCH: CodeGuru.com 



[Developer](#) • [Gamelan](#) • [Jars](#) • [Wireless](#) • [Discussion](#)

- CodeGuru Navigation:
- [Visual C++ / C++](#)
- [.NET / C#](#)
- [Visual Basic](#)
- [Videos](#)
- [Submit an Article](#)
- [Discussion Forums](#)
- [Resource Directory](#)
- [Announcements](#)
- [Book List](#)
- [Book Reviews](#)
- [List of Gurus](#)
- [Guest Book](#)
- [About Us](#)
- [FAQs](#)
- [Site Map](#)

[Home](#) >> [Visual Basic](#) >> [General](#) >> [System](#) >> [Keyboard](#)

[Whitepaper: Delivering Intelligent Network Access Through Identity Driven Management. For IT professionals who need to take network security to the next level.](#)

## Managing Low-Level Keyboard Hooks with the Windows API for VB .NET

Rating: ★★★★★

[Paul Kimmel](#) ([view profile](#))  
April 18, 2003

I am amazed at the overwhelming and disproportionately high number of email responses I get regarding keyboard hooks. Many people in a diverse group of industries have legitimate reasons for wanting to be able to capture key combinations. Last November, I wrote about low-level keyboard hooks for VB6 (see [Managing Low-Level Keyboard Hooks with the Windows API](#), November 18, 2002 in codeguru.com's VB Today.) In response to your request, I have revised the keyboard hooks example for VB .NET.

The inimitable Robbie Powell read my earlier article on keyboard trapping and wanted to use the code for a testing application. The basic idea is that the application should not be distracted during a test. By eliminating the ability to open an application other than the test application, the candidate's attention was more ably focused. Considering the nature and importance of the candidate's test, a bit of tunnel vision during testing was warranted. Unfortunately, the code from the November port directly from VB6 to VB.NET. Mr. Powell did a superlative job porting the code but something quite right. Together we figured out the differences, which are provided here.

(continued)

BEST AVAILABLE COPY

**Member Sign In:**

User ID:

Password:

Remember Me:

**SIGN IN**

[Forgot Password?](#)

Not a member?  
[Click here for more](#)

information and to register.



internet.commerce

- [Partners & Affiliates](#)
- [Cheap Airline Tickets](#)
- [Domain registration](#)
- [Graphics Cards](#)
- [Email Marketing](#)
- [Cheap Plane Tickets](#)
- [GPS](#)
- [2nd Mortgage](#)
- [CRM Software](#)
- [Marketing Products](#)
- [Online Education](#)
- [Car Insurance Quotes](#)
- [Cheap Digital Camera](#)
- [T-Shirts](#)
- [Register Domain Name](#)

RSS Feeds

- All
- VC++/C++
- .NET/C#
- VB

See more EarthWeb Network feeds

**\_DAY 27**  
 \_Managing and controlling software development is a hassle. We don't have a complete view.

►► Roll over bar graphs to keep Gil on his toes.

**Rational**

- ▶▶ **Watch:** *Webcast: Manage Change across the Software Lifecycle*
- ▶ **Download:** *Forrester white paper: Software Configuration Management*
- ▶ **Download:** *Rational ClearCase product datasheet*
- ▶▶ **Attend:** *Events and business briefings in your area*

AMD64 devSource
AMD

---

**Embracing the full spectrum of developer needs including content supporting 64 bit, Multi-Core, Tools, and Optimization.**

---

➤ **I/O Virtualization and AMD's IOMMU**  
 AMD64's virtualization extensions provide hardware support for VMM CPU virtualization, but that's only half the picture. I/O virtualization is the other half, and it's critical, because without hardware, I/O virtualization requires the high overhead of device emulation. [Read more.](#)

.....

➤ **DB2 9 on AMD: A Perfect Match**  
 What happens when you pair IBM's latest and greatest data server, DB2 9, with AMD's leading-edge Opteron architecture? You get a blisteringly fast data server platform that makes the most of advances on both fronts. Learn how DB2 9 has been optimized for NUMA and x86-64 architecture, and how it works with AMD 64-bit multi-core. [Read more.](#)

.....

➤ **Virtualization Using AMD Servers and libVirt**  
 Virtualization as a tool for development and deployment has come of age. Hardware advancements from manufacturers like AMD, and software tools such as libVirt, make creating and managing virtual machines a breeze. Let's look at how AMD, Red Hat, and others are helping push the virtualization envelope. [Read more.](#)

.....

➤ **Widen Your Opportunities with 64-Bit Compilers: Microsoft Visual Studio 2005**  
 Explore the capabilities and feature set of AMDs 64-bit compiler solution contained in Microsofts Visual Studio. [Read more.](#)

.....

➤ **For more relevant code samples, tutorials and editorials click here.**

Permit me to rehash some of the material in the November article for those who did not have a read that article. If you have read the November article and just need to fill in the blanks, I encourage you to read ahead to the *Implementing the Keyboard Delegate* section and *The Complete Code Listing* section presentation, continue.

## Writing API Declarations

The .NET Framework has tidily wrapped up much of the Windows API in methods that are significant. However, occasionally you may need to turn to the Windows API. Trapping keystrokes from user input for all applications is a pretty low-level operation, and in such an instance you need to turn to the Windows API. Consequently, you will need to declare API methods.

For VB.NET developers, we can use the old-style Declare syntax to import DLL library methods. However, the ability to use new .NET attributes for declaring API methods, specifically the `DllImportAttribute`, is a significant improvement. The `DllImportAttribute` keyword is shorthand notation that causes the compiler to add and use the `DllImportAttribute`. So, keep in mind that you will need to use the `DllImportAttribute` if you are programming in some other .NET language. For our purposes, we will use the convenience notation.

To trap and examine keys before other applications get them, we need to hook the keyboard (using the hook), call the old keyboard handler, and interpret key combinations. To accomplish this feat, we will import the `SetWindowsHookEx`, `UnhookWindowsHookEx`, `CallNextHookEx`, and `GetAsyncState`. To help you understand the rationale a bit better with some background information. So, before we look at the mechanics of a declaration statement, let's take a quick historical journey.

## Understanding Low-Level Hooks

It seems like just a few brief years ago that you couldn't write anything interesting without writing handlers. In very low memory, Basic Input and Output (BIOS) code is loaded. This code provides capabilities that your PC needs. (Assuming you are using a DOS-based PC. I imagine a MAC has analogous to the BIOS for PCs...) These basic services are called interrupt handlers, and they are numbered. For example, interrupt 5 is the print screen interrupt. Interrupt 0x10 (hexadecimal) provides input and output, interrupt 0x19 will reboot your computer, and interrupts 0x9 and 0x16 manage pretty powerful stuff, these interrupt handlers.

Just a few years ago, one would have to write a custom interrupt handler and redirect the BIOS handler to replace the basic services. For example, prior to Windows, if code attempted to read a diskette and no diskette were in the drive, an application would hang. However, if the code provided an interrupt handler, the error could be caught and new behavior provided. Supplanting basic BIOS behavior is exactly what popup programs and TSR (Terminate and Stay Resident) utilities did all the time working at this level is an all or nothing proposition. Make a mistake and the whole PC crashed. Low-level capabilities can still be accessed—for example, write *asm int 3 end* in Delphi and the debug because interrupt 3 is a low-level breakpoint. However, because replacing basic system services with unreliable PC behavior, operating system engineers were motivated to shield programmers from

To aid in productivity, we work at a higher level of abstraction. Instead of writing an interrupt handler for 0x9 and 0x16 to handle keyboard input directly, we simply write an event handler for the KeyDown (related) event handler. However, you can still interact with the operating system at a much lower abstraction than the VB KeyDown event. Simply keep in mind that the lower you go, the more you have. Back to the present.

To trap keystrokes before other applications get them, we have to interact with the operating system between the BIOS' interrupt handler and the high-level KeyDown event. To trap all keys, we are using the BIOS, perhaps, rather than the KeyDown event. Consequently, care must be exercised.

## Declaring API Methods

The convenience syntax for declaring an API method is very similar to the notation used in VB6. Using the `Declare` keyword, match the signature of the API method, indicate the library that contains it and optionally, indicate the visibility. For example, to import the `SetWindowsHookEx` API method:

```
Public Declare Function SetWindowsHookEx Lib "user32" _
    Alias "SetWindowsHookExA" (ByVal idHook As Integer, _
    ByVal lpfn As KeyboardHookDelegate, ByVal hmod As Integer, _
    ByVal dwThreadId As Integer) As Integer
```

Here is the breakdown of the declaration statement:

- **Public**—Defines the visibility as Public. (Any code can call this method.)
- **Declare**—The keyword that indicates that we are implicitly importing a library method
- **Function**—The library method returns a value
- **SetWindowsHookEx**—The name we'll use in our code
- **Lib "user32"**—Specifies the library that contains the method. (You can find the physical *user32.dll* on your PC.)
- **Alias "SetWindowsHookExA"**—Indicates the real name of the method in the DLL

The rest of the declaration defines the signature of the DLL method. If you look closely at the declaration, you will notice something suspicious—`KeyboardHookDelegate`. Delegates didn't exist prior to .NET, yet this clearly uses something that calls `KeyboardHookDelegate`.

The API method does not use a delegate. The API method actually defines the `lpfn` argument as a pointer to a function. The CLR does an excellent job matching the needs of the API—a pointer to a function—with an entity called a delegate. Delegates are classes that contain function pointers; however, a delegate is more than just the address of a function. A function pointer can be represented as a 32-bit integer, but some fudging is done for us to permit a delegate to be passed where only an integer is needed. The benefit is that we can use more convenient .NET types where previously less convenient raw data

have been used. Additional declarations are shown in *The Complete Code Listing*.

## Implementing the Keyboard Delegate

To hook the keyboard, we are inserting our method into the address space for the existing low-level abstraction. As is true with interrupt handlers, we still perform the same basic operation at a model of abstraction. As is true with interrupt handlers, we need to hang onto the old handler, and ensure we don't call the old handler, we prevent someone else's code from running. This would be rude; the intention is to prevent someone else's keyboard code from running.

The delegate signature has to play by the same rules as a plain vanilla function pointer. The delegate must match an expected signature. Delegates will be invoked with the anticipated and necessary specific arguments and a return value if one is expected. In our example, the operating system expects two integers and a structure that contains key state information. The caller will be expecting a return value. We can name the delegate anything, but as mentioned, the signature must match. The signature method is defined next.

```
Public Delegate Function KeyboardHookDelegate( _
    ByVal Code As Integer, _
    ByVal wParam As Integer, ByVal lParam As KBDLLHOOKSTRUCT) _
    As Integer
```

Decomposed into chunks, we have:

- **Public**—The Delegate type is public
- **Delegate**—Defines this method signature as a subclass of the System.Delegate type
- **Function**—Indicates that the caller will expect a return value
- **KeyboardHookDelegate**—Is the name of the delegate
- **Code**—Is the name of the first argument, an Integer, that is passed by value
- **wParam**—Is a by-value Integer that we don't need in the example but is commonly found in other methods
- **lParam**—Very important to keyboard hooking; we need a pointer to the keyboard state information. The structure will tell us everything we need to know about the keys being pressed, released, and held down. It is important to define this argument ByRef.
- **As Integer**—Indicates that the caller will be expecting an Integer.

We will actually need a method that very closely matches the signature of the delegate. The only thing that can deviate is the name of the actual arguments. The callback method can use different names, but the order and type of the arguments and the method type—function or subroutine—must match.

## Hooking the Keyboard

To hook the keyboard, we need to call the SetWindowsHookEx method. We will need a constant to identify what we want to hook, the idHook argument. We need a method that can be called back, the lpfn argument, the application doing the hooking, which is our application and the hmod argument, and the thread ID of the thread we want to hook.

When hooking the keyboard in .NET, this part of the revision—from VB6–7 to VB.NET—is the most difficult. I have taken an important excerpt from the complete listing, listing 2. That excerpt is as follows:

### **Listing 1: Critical revisions to hooking the keyboard in .NET.**

```
<MarshalAs(UnmanagedType.FunctionPtr)> _
Private callback As KeyboardHookDelegate

Public Sub HookKeyboard()
    callback = New KeyboardHookDelegate(AddressOf KeyboardCallback)
```



```

KeyboardHandle = SetWindowsHookEx( _
    WH_KEYBOARD_LL, callback, _
    Marshal.GetHINSTANCE( _
        [Assembly].GetExecutingAssembly.GetModules() (0)).ToInt32, 0)

Call CheckHooked()
End Sub

```

Delegates are managed objects in .NET. This means that they are garbage collected. A problem pass a delegate to the unmanaged code of the user32.dll API. Apparently, the garbage collector the delegate object is in use and after a short interval—roughly 47 seconds in experiments—the garbage collected. Consequently, when the API method attempts to call the method represented back, a null reference exception occurs. To prevent the delegate from getting GC'd, we need to 1 variable with the System.Runtime.InteropServices.MarshalAsAttribute, passing the enumerated UnmanagedType.FunctionPtr. This tags the delegate argument, preventing it from being GC'd in fashion.

The first argument to SetWindowsHookEx is WH\_KEYBOARD\_LL. The second argument is the tag contains the address of our local callback method. The third argument is the handle (hWnd) of ti doing the hooking, and passing 0 for the thread id means that we want to hook the keyboard for

For all of our efforts, if we forget the MarshalAsAttribute, the code fails miserably. You can read COMInterop in my new book *Visual Basic .NET Power Coding* from Addison-Wesley, available Jul

## Trapping Key Combinations

Determining if specific key combinations are being pressed requires some tricky gyrations. (Keep are working at a pretty low level here.) This code remains pretty much unchanged from the Nov basic idea is to read the current key press in the KBDLLHOOKSTRUCT.vkCode. If you need to loc multi-key combinations, you may need to call GetAsyncKeyState to determine whether addition: held. For example, we call GetAsyncKeyState(VK\_CONTROL) in listing 2 to see whether the Ctrl I down.

## Unhooking the Keyboard

The return value from SetWindowsHookEx is stored. This is the address of the hook we replaced this value because if we want to let some key combinations slip past our hook, we need to use t SetWindwosHookEx to call the old hook. We also use this value to unhook the keyboard, returni state, when we are finished holding onto the keyboard handler. Call UnhookWindowsHookEx pas value from SetWindowsHookEx to restore the original keyboard hook.

## The Complete Code Listing

Listing 2 presents the complete revised listing for VB.NET. Most of this code is more of the same we have discussed already, including some additional methods, declare statements, the KDDLH some useful constants. You can copy and paste the code in listing 2 directly into a module to exj Call HookKeyboard to begin intercepting the three defined key combinations and UnhookKeyboa old keyboard state.

**Listing 2: The complete revised listing for implementing low-level keyboard hooks.**

```

Imports System.Runtime.InteropServices
Imports System.Reflection
Imports System.Drawing
Imports System.Threading

Module Keyboard
    Public Declare Function UnhookWindowsHookEx Lib "user32" _
        (ByVal hHook As Integer) As Integer

```

```

Public Declare Function SetWindowsHookEx Lib "user32" _
    Alias "SetWindowsHookExA" (ByVal idHook As Integer, _
    ByVal lpfn As KeyboardHookDelegate, ByVal hmod As Integer, _
    ByVal dwThreadId As Integer) As Integer

Private Declare Function GetAsyncKeyState Lib "user32" _
    (ByVal vKey As Integer) As Integer

Private Declare Function CallNextHookEx Lib "user32" _
    (ByVal hHook As Integer, _
    ByVal nCode As Integer, _
    ByVal wParam As Integer, _
    ByVal lParam As KBDLLHOOKSTRUCT) As Integer

Public Structure KBDLLHOOKSTRUCT
    Public vkCode As Integer
    Public scanCode As Integer
    Public flags As Integer
    Public time As Integer
    Public dwExtraInfo As Integer
End Structure

' Low-Level Keyboard Constants
Private Const HC_ACTION As Integer = 0
Private Const LLKHF_EXTENDED As Integer = &H1
Private Const LLKHF_INJECTED As Integer = &H10
Private Const LLKHF_ALTDOWN As Integer = &H20
Private Const LLKHF_UP As Integer = &H80

' Virtual Keys
Public Const VK_TAB = &H9
Public Const VK_CONTROL = &H11
Public Const VK_ESCAPE = &H1B
Public Const VK_DELETE = &H2E

Private Const WH_KEYBOARD_LL As Integer = 13&
Public KeyboardHandle As Integer

' Implement this function to block as many
' key combinations as you'd like
Public Function IsHooked( _
    ByRef Hookstruct As KBDLLHOOKSTRUCT) As Boolean

    Debug.WriteLine("Hookstruct.vkCode: " & Hookstruct.vkCode)
    Debug.WriteLine(Hookstruct.vkCode = VK_ESCAPE)
    Debug.WriteLine(Hookstruct.vkCode = VK_TAB)

    If (Hookstruct.vkCode = VK_ESCAPE) And _
        CBool(GetAsyncKeyState(VK_CONTROL) _
            And &H8000) Then

        Call HookedState("Ctrl + Esc blocked")
        Return True
    End If

    If (Hookstruct.vkCode = VK_TAB) And _
        CBool(Hookstruct.flags And _
            LLKHF_ALTDOWN) Then

        Call HookedState("Alt + Tab blockd")
        Return True
    End If

    If (Hookstruct.vkCode = VK_ESCAPE) And _

```

```

        CBool(Hookstruct.flags And _
            LLKHF_ALTDOWN) Then

            Call HookedState("Alt + Escape blocked")
            Return True
        End If

        Return False
    End Function

    Private Sub HookedState(ByVal Text As String)
        Debug.WriteLine(Text)
    End Sub

    Public Function KeyboardCallback(ByVal Code As Integer, _
        ByVal wParam As Integer, _
        ByVal lParam As KBDLLHOOKSTRUCT) As Integer

        If (Code = HC_ACTION) Then
            Debug.WriteLine("Calling IsHooked")

            If (IsHooked(lParam)) Then
                Return 1
            End If

        End If

        Return CallNextHookEx(KeyboardHandle, _
            Code, wParam, lParam)

    End Function

    Public Delegate Function KeyboardHookDelegate( _
        ByVal Code As Integer, _
        ByVal wParam As Integer, ByVal lParam As KBDLLHOOKSTRUCT) _
        As Integer

    <MarshalAs(UnmanagedType.FunctionPtr)> _
    Private callback As KeyboardHookDelegate

    Public Sub HookKeyboard()
        callback = New KeyboardHookDelegate(AddressOf KeyboardCallback)

        KeyboardHandle = SetWindowsHookEx( _
            WH_KEYBOARD_LL, callback, _
            Marshal.GetHINSTANCE( _
                [Assembly].GetExecutingAssembly.GetModules()(0)).ToInt32, 0)

        Call CheckHooked()
    End Sub

    Public Sub CheckHooked()
        If (Hooked()) Then
            Debug.WriteLine("Keyboard hooked")
        Else
            Debug.WriteLine("Keyboard hook failed: " & Err.LastDllError)
        End If
    End Sub

    Private Function Hooked()
        Hooked = KeyboardHandle <> 0
    End Function

    Public Sub UnhookKeyboard()
        If (Hooked()) Then

```

```

        Call UnhookWindowsHookEx(KeyboardHandle)
    End If
End Sub

End Module

```

Be aware that mistakes may completely lock up your keyboard and you may need to reboot. To solve this problem, I use the Thread Pool and a separate thread to release the keyboard after 10 or 15 seconds. This strategy has been invaluable while developing low-level code. You can learn more about multithreading in my past and future articles or by picking up a copy of my book, *Visual Basic .NET Unleashed*, from Sams.

## Summary

Run the sample code and you will see that the Windows API is alive and well in .NET. Thankfully, .NET does not have very special needs indeed to resort to calling into the Windows API. This is a far cry from VBA where anything useful required interaction with the Windows API.

One of the most important differences between VB6 and VB.NET is the notion of managed code. In .NET, managed objects can be moved around in memory and garbage collected. Old Windows API code does not represent managed code. As a result, you may get some quirky behavior when interacting with the Windows API. If you plan on writing a lot of code that interoperates with the Windows API, I encourage you to pick up a good book on COM Interop and a good advanced book such as my *Power Coding* from Addison-Wesley that explores these intricate nooks and crannies for you.

## About the Author

Paul Kimmel is a freelance writer for Developer.com and CodeGuru.com. Look for his recent book *Visual Basic .NET Power Coding*, from Addison-Wesley on Amazon.com. Paul Kimmel is available to help with your .NET solutions and can be contacted at [pkimmel@softconcepts.com](mailto:pkimmel@softconcepts.com).

# # #

## DEVELOPER SOLUTIONS

- ▶ Developer.com Webcast: Defining Your Own Software Development Methodology.
- ▶ Get the most out of Visual Studio. Visit the Microsoft Visual Studio Extensibility Portal on DevX.
- ▶ Get DB2 Express-C 9. Free to Develop, Deploy, Distribute. No limits--just data. Download Now!
- ▶ Webcast: Linux on Multi-Core--WAS CE and the Open Stack Appliance
- ▶ Generate Complete .NET Web Apps in Minutes . Download Iron Speed Designer today.



Email this article



Print this article

RATE THIS ARTICLE:  Excellent  Very Good  Average  Below Average  Poor

(You must be signed in to rank an article. Not a member? [Click here to register](#))

### Latest Comments:

- [How to disable windows keys or startup key on keyboard using vb.net](#) - shivraj jadhav (10/24)
- [This Code Should be in a DLL](#) - RoyK (03/11/2005)
- [keys are being processed twiced](#) - bigmutter (10/12/2004)
- [Wow what a great post!!](#) - IcyCode (10/10/2004)
- [How do I process the keys otherwise using your VB6 keyboard handler?](#) - DSanborn3 (09/26/2004)

[View All Comments](#)

**Add a Comment:**

**Title:**

**Comment:**

**Pre-Formatted:**  Check this if you want the text to display with the formatting as typed (go code)



(You must be signed in to comment on an article. Not a member? [Click here](#) to register)

Next-Generation Technology. Featuring Phil Hester SVP & CTO, AMD. AM

**JupiterWeb networks:**



**Search JupiterWeb:**



Jupitermedia Corporation has two divisions: Jupiterimages and JupiterWeb

Jupitermedia Corporate Info

Copyright 2006 Jupitermedia Corporation All Rights Reserved.  
Legal Notices, Licensing, Reprints, & Permissions, Privacy Policy.

Web Hosting | Newsletters | Tech Jobs | Shopping | E-mail Offers

**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

**BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- BLACK BORDERS
- IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT OR DRAWING
- BLURRED OR ILLEGIBLE TEXT OR DRAWING
- SKEWED/SLANTED IMAGES
- COLOR OR BLACK AND WHITE PHOTOGRAPHS
- GRAY SCALE DOCUMENTS
- LINES OR MARKS ON ORIGINAL DOCUMENT
- REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- OTHER: \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**

[Pushing Security to the Perimeter: Trusted Computing Technology Adapts to Changing Enterprise Needs](#) Register to d

[Symantec Server Management](#) [Endpoint Compliance](#)

[Close more deals by knowing who's most interested!](#)

[Best Buy For Business Software Applications](#) [more.](#)

[Perpetuating Technologies: Web Database Development](#)

[Pillar Data Systems: Data Backup Services](#)

[Belzabar Software Design: Custom Software Programming](#)

[SQL Management](#)

[IT MANAGEMENT](#) [NETWORKING](#) [WEB DEVELOPMENT](#) [HARDWARE & SYSTEMS](#) [SOFTWARE DEVELOPMENT](#) [IT NEWS](#)



SEARCH:



[Developer](#) • [Gamelan](#) • [Jars](#) • [Wireless](#) • [Discussion](#)

**CodeGuru Navigation:**

- [Visual C++ / C++](#)
- [.NET / C#](#)
- [Visual Basic](#)
- [Videos](#)
- [Submit an Article](#)
- [Discussion Forums](#)
- [Resource Directory](#)
- [Announcements](#)
- [Book List](#)
- [Book Reviews](#)
- [List of Gurus](#)
- [Guest Book](#)
- [About Us](#)
- [FAQs](#)
- [Site Map](#)

[Home](#) >> [Visual C++ / C++](#) >> [Windows Programming](#) >> [System](#) >> [Keyboard](#)

[Is Your Accounting Software Limiting Your Growth and Productivity? Get Your FREE Financial Evaluation Kit.](#) Identify problems with your software, data management, reporting, and more.

## Hooking the Keyboard

Rating: ★★★★★

**Anoop Thomas** ([view profile](#))  
December 13, 2001

**Environment:** VC6 , Windows 2000/NT/ME/9x

This article describes how to install a Keyboard hook in Microsoft Windows.  
(continued)

**Member Sign In:**

User ID:

Password:


Remember Me:

[Forgot Password?](#)

[Not a member? Click here for more](#)

### Technical Brief: Identity Driven Management

Enable your network to adapt to each user individually, on the basis of business needs






BEST AVAILABLE COPY

information and to register.



Compare Prices:



Televisions (TVs)  
Laptop Computers  
Digital Cameras

internet jobs ▶

internet.commerce

[Partners & Affiliates](#)  
[Car Donations](#)  
[Tech Jobs](#)  
[Promotional Hats](#)  
[Prepaid Phone Card](#)  
[Mortgage Refinance](#)  
[Web Design](#)  
[Register Domain Name](#)  
[Dental Insurance](#)  
[Phone Systems](#)  
[Online Booking Hotels](#)  
[Prepaid Calling Cards](#)  
[Cheap Digital Camera](#)  
[PDA Phones & Cases](#)  
[Cell Phone Plans](#)

RSS Feeds

All  
 VC++/C++  
 .NET/C#  
 VB

See more EarthWeb  
Network feeds

Embracing the full spectrum of developer needs including content supporting 64 bit, Multi-Core, Tools, and Optimization.

► **[I/O Virtualization and AMD's IOMMU](#)**

AMD64's virtualization extensions provide hardware support for VMM CPU virtualization, but that's only half the picture. I/O virtualization is the other half, and it's critical, because without hardware, I/O virtualization requires the high overhead of device emulation. [Read more.](#)

► **[DB2 9 on AMD: A Perfect Match](#)**

What happens when you pair IBM's latest and greatest data server, DB2 9, with AMD's leading-edge Opteron architecture? You get a blisteringly fast data server platform that makes the most of advances on both fronts. Learn how DB2 9 has been optimized for NUMA and x86-64 architecture, and how it works with AMD 64-bit multi-core. [Read more.](#)

► **[Virtualization Using AMD Servers and libVirt](#)**

Virtualization as a tool for development and deployment has come of age. Hardware advancements from manufacturers like AMD, and software tools such as libVirt, make creating and managing virtual machines a breeze. Let's look at how AMD, Red Hat, and others are helping push the virtualization envelope. [Read more.](#)

► **[Widen Your Opportunities with 64-Bit Compilers: Microsoft Visual Studio 2005](#)**

Explore the capabilities and feature set of AMD's 64-bit compiler solution contained in Microsoft's Visual Studio. [Read more.](#)

► **[For more relevant code samples, tutorials and editorials click here.](#)**

There are two types of Hooks - Thread specific hooks and Systemwide hooks. A thread specific hook with particular thread only (Any thread owned by the calling process.). If you want to associate other processes and threads, you will have to use a systemwide hook. There is a hook procedure hook. This procedure is always called when the particular event occurs. For eg. the mouse. When associated with the mouse, this hook procedure is called. The hook is set by calling the function `SetWindowsHookEx()`. The hook is removed by calling `UnhookWindowsHookEx()`.

For thread hooks, the hook procedure may be in an EXE file or a DLL. But for Global or System hook procedure must reside in a DLL. For this, we need to create a DLL.

To do this, create a Win32 DLL project with only the starter files in it and modify it to suit your requirements to put the code for installing and removing the hook in the DLL itself.

Now, define the functions in the DLL's header file as follows.

```
#ifdef KEYDLL3_EXPORTS
#define KEYDLL3_API __declspec(dllexport)
#else
#define KEYDLL3_API __declspec(dllimport)
#endif

//This function installs the Keyboard hook:
KEYDLL3_API void installhook(HWND h);

//This function removes the previously installed hook.
KEYDLL3_API void removehook();

//hook procedure:
```

BEST AVAILABLE COPY



```
KEYDLL3_API LRESULT CALLBACK hookproc( int ncode,
                                       WPARAM wparam,
                                       LPARAM lparam);
```

For exporting the functions in the DLL, it is a good idea to use the `__declspec` and `dllexport` keywords than using a separate .DEF file. The `SetWindowsHookEx( )` function returns a handle to a hook for later uninstall of the hook from the hook chain. We also have a window handle, which we will use to send messages to the main Application Window. We first find the application window by using the `FindWindow` function, and then send the keystroke message parameters to the Application's main window using `PostMessage( )` call. This is as in the code fragment below:

```
//Find application window handle
hwnd = FindWindow("#32770", "Keylogger Exe");

//Send info to app Window.
PostMessage(hwnd, WM_USER+755, wparam, lparam);
```

At the end of the hook procedure, we must call the `CallNextHookEx( )` function to pass on the next hook installed in the hook chain. This is highly recommended because not doing so can cause system behaviour and lockouts. The procedures for installing, removing the hooks, and the hook chain are shown below:

```
KEYDLL3_API void installhook(HWND h)
{
    hook = NULL;
    hwnd = h;
    hook = SetWindowsHookEx( WH_KEYBOARD,
                             hookproc,
                             hinstance,
                             NULL);

    if(hook==NULL)
        MessageBox( NULL,
                    "Unable to install hook",
                    "Error!",
                    MB_OK);
}

KEYDLL3_API void removehook()
{
    UnhookWindowsHookEx(hook);
}

KEYDLL3_API LRESULT CALLBACK hookproc( int ncode,
                                       WPARAM wparam,
                                       LPARAM lparam)
{
    if(ncode>=0)
    {
        //Find application window handle
        hwnd = FindWindow("#32770", "Keylogger Exe");
        //Send info to app Window.
        PostMessage(hwnd, WM_USER+755, wparam, lparam);
    }
    //pass control to next hook.
    return ( CallNextHookEx(hook, ncode, wparam, lparam) );
}
```

If there are multiple instances of the DLL in memory, they all have different values for each data member. But, certain data, such as the hook handle, the window handle should be shared between all instances. This is because all instances send info to the same Application window. For this, we need to share data as shared in the DLL's .CPP file. This is done as follows:

```
#pragma data_seg(".HOOKDATA")//Shared data among all instances.
HHOOK hook = NULL;
HWND hwnd = NULL;
#pragma data_seg()
```

Now, the linker must be given instructions so as to place the shared data in separate space in th we use the following code, soon after the abovementioned code.

```
//linker directive
#pragma comment(linker, "/SECTION:.HOOKDATA,RWS")
```

So much for the DLL. Now, we will take a look at the Main application(EXE). Create an MFC appl or dialog based). I created a Dialog based EXE for simplicity. After creating the project, Go to Pr dialog box by selecting Project>Settings from the Main Menubar. Select the 'Link' tab and type 'Object/library modules' box. Click OK. Now, Insert the DLL's header file into the workspace by s Project>Add to project> files from the main menubar. Select the .h file of the DLL that we built it in your project as follows:

```
//Include this for functions in the DLL:
#include "..\Keydll3\Keydll3.h"
```

This should be in the .CPP file for the Main dialog class. Now, in the main dialog class, add a put function to process the keystroke messages sent by the DLL. This function is as shown below:

```
afx_msg LRESULT processkey(WPARAM w,LPARAM l);//declaration
LRESULT CKeyexeDlg::processkey(WPARAM w, LPARAM l)//definition
{
    //This block processes the keystroke info.
    .
    .
    return 0L;
}
```

(This member can be easily added using the wizardbar). Now, define the Message we shall recei the .CPP file as follows:

```
//This message is recieved when key is down/up
#define WM_KEYSTROKE (WM_USER + 755)
```

Now add the newly created member function as the message handler for the **WM\_KEYSTROKE** the **ON\_MESSAGE( )** macro in the Message maps section(in the CPP file) as below: \

```
BEGIN_MESSAGE_MAP(CKeyexeDlg, CDialog)
    //{AFX_MSG_MAP(CKeyexeDlg)
    .
    .
    ON_MESSAGE(WM_KEYSTROKE, processkey)
    //}AFX_MSG_MAP
END_MESSAGE_MAP()
```

We are almost finished. But, before compiling and building the EXE, add the path to the .LIB file the Visual studio Library paths. To do this, select Tools>Options from the main menubar and sel 'Directories' tab. Select 'Library files' from the 2<sup>nd</sup> dropdown list, and add the path to the DLL's . below. Click OK, Save all files and workspace, and then build your project.



For more information on Hooks, see the following sections in the MSDN library:

- SetWindowsHookEx( ),
- Hook functions,
- Virtual-key codes,
- Keystroke message flags.

The example I have used here is provided for download (See below).

**Note:** For Windows NT/2000, your windows password might be logged by the hook procedure if enabled the 'Ctrl-Alt-Del' logon sequence(Only while unlocking the PC).

## Downloads

- [Download demo project - 69 Kb](#)
- [Download source - 25 Kb](#)

## DEVELOPER SOLUTIONS

- ▶ Webcast: Linux on Multi-Core--WAS CE and the Open Stack Appliance
- ▶ Get DB2 Express-C 9. Free to Develop, Deploy, Distribute. No limits--just data. Download Now!
- ▶ Developer.com Webcast: Defining Your Own Software Development Methodology.
- ▶ Generate Complete .NET Web Apps in Minutes . Download Iron Speed Designer today.
- ▶ Generate Complete .NET Web Apps in Minutes . Download Iron Speed Designer today.



Email this article



Print this article

RATE THIS ARTICLE:  Excellent  Very Good  Average  Below Average  Poor

(You must be signed in to rank an article. Not a member? [Click here to register](#))

### Latest Comments:

- [two key on the same time jams the application](#) - o.k. (04/03/2006)
- [VB - lordnephilim](#) (03/03/2005)
- [Anyone Know THIS?](#) - Legacy CodeGuru (02/26/2004)
- [Easy to understand](#) - Legacy CodeGuru (02/23/2004)
- [hooking remote keyboard ?](#) - Legacy CodeGuru (02/05/2004)

[View All Comments](#)

Add a Comment:

BEST AVAILABLE COPY

Title: \_\_\_\_\_

Comment: \_\_\_\_\_

**Pre-Formatted:**  Check this if you want the text to display with the formatting as typed (go code)



(You must be signed in to comment on an article. Not a member? [Click here to register](#))

| Featured Resources for Developing Intelligent Connections from the Avaya DeveloperConnection (  |   |   |
|---|---|---|
| <b>ARTICLE</b><br><a href="#">Avaya's New Release of Interaction Center 7.1 Offers Cutting-edge Functionality to Contact Management</a> | <b>DOWNLOAD</b><br><a href="#">Application Enablement Services IP Communications SDK</a><br>Client API libraries, XSDs, WSDL, Java/XML programmer guides, sample apps & more. | <b>WHITEPAPER</b><br><a href="#">Guide to VoIP for the Small Business</a><br>Is VoIP reliable? Can it address business needs? Read this article |

JupiterWeb networks:



Search JupiterWeb:



[Jupitermedia Corporation](#) has two divisions: [Jupiterimages](#) and [JupiterWeb](#)

[Jupitermedia Corporate Info](#)

Copyright 2006 Jupitermedia Corporation All Rights Reserved.  
[Legal Notices](#), [Licensing](#), [Reprints](#), & [Permissions](#), [Privacy Policy](#).

[Web Hosting](#) | [Newsletters](#) | [Tech Jobs](#) | [Shopping](#) | [E-mail Offers](#)

BEST AVAILABLE COPY



Introduction

Background

Example

AV Reviews

Scanners

Forum

## ***Wolves In Sheep's Clothing: Malicious DLLs Injected Into Trusted Host Applications***

The injection of malicious dynamic link libraries ("DLLs") into trusted host applications can be considered one of the trojan scene's most recent hypes. This article provides you with the background knowledge to understand several common injection techniques and helps you to assess the potential dangers arising from DLL injections.

### **1. Dynamic Link Libraries are ... ?**

Just in case you don't know what we are talking about. Dynamic link libraries are a feature of the Windows OS. They can be described as code libraries (containing executable routines) that are separately saved as files with the extension .dll. Because DLLs do not constitute stand-alone programs they cannot be independently executed but have to be loaded by another application before they become active. Usually, a DLL is loaded into the memory by an application that wants to use it. By contrast, trojan DLLs are "injected" into other applications ("hosts") and try to abuse them. After the injection has been finished a trojan DLL can be considered a part ("module") of the host application ("process"). Although the trojan DLL is a mere module of the host process it can perform the same actions like a nasty stand-alone trojan executable.

### **2. Are there really DLL trojans "in the wild"?**

Definitely. It started about two years ago with firewall leaktests like "Firehole". The aforementioned leaktest injected a harmless DLL into a trusted application with internet access in order to demonstrate the limitations of personal firewalls'

### 3. What's so special about DLL trojans?

From a trojan coder's perspective, DLL trojans offer many advantages:

#### (a) Stealth

DLL trojans are relatively stealth. This is because they do not show up in the Windows Task-Manager which merely lists processes but not modules (DLLs).

Fortunately, there are several advanced process monitors like "TaskInfo", "System Analyzer", "Process Explorer" (a freeware tool from Sysinternals) and "APM - Advanced Process Manipulation" (a freeware tool from DiamondCS) which allow a computer user to inspect the modules loaded by a process. It is still difficult to detect a DLL trojan though because (i) there are dozens if not hundreds of modules to inspect (unless you already know the infected process) and (ii) there is no easy way to determine whether a DLL is malicious or not (e.g., the DLL trojan may look like a harmless Microsoft DLL).

Moreover, DLL trojans cannot be easily exposed by a firewall (see below). In case that a DLL trojan fails to bypass a firewall and triggers an alert the ordinary user may not expect to have found a trojan but to have experienced a relatively harmless "phone home" originating from a trusted application.

A DLL trojan's filename may be invisible. For instance, the DLL trojan Nuclear Uploader offers basic root kit functionality: it injects itself into the Windows Explorer and hides certain filenames (e.g., the trojan files) from the user.

#### (b) Hard To Kill

It can be quite difficult to get rid of a DLL trojan if it is injected into a critical system process which cannot be terminated. For instance, the DLL trojan Beast 2 injects itself into the winlogon.exe process. (It is still possible to remove this trojan if you reboot the computer in "Safe Mode" or unload the DLL from the winlogon.exe process with the help of a tool like Trojan Hunter.) Other DLL trojans infect almost every process they can find in order to complicate their removal.

and passively listen for incoming connections. Server DLLs are usually injected into trusted server applications which are expressly allowed to listen. For instance, a server DLL may be injected into a web server, ftp server or any other application for which a firewall rule has been created that allows incoming connections. A tight firewall rule set may help to prevent server DLLs from abusing trusted server applications. For example, a web server which is only permitted to listen on a single port cannot be easily infected by a DLL trojan because generally the DLL trojan will be unable to share the permitted port with the infected application. However, there are numerous server applications (like filesharing tools) for which it is not possible to create such a tight firewall rule set.

Client DLLs (so-called reverse trojans) are not listening for incoming connections but actively establish outgoing connections. Usually, client DLLs are injected into trusted client applications (like web browsers, email programs or FTP clients) which are allowed to connect to the web. For example, a client DLL may abuse the iexplore.exe process in order to connect to "www.remote-control.heaven.org". This means that an outgoing connection is established from local port 1024-5000 to remote port 80. It is not possible to create a tight firewall rule set in order to avoid outgoing connections via local port 1024-5000 since outgoing connections cannot be restricted to a single local port: the Windows OS dynamically assigns local ports to applications which want to establish outgoing connections. (It is also not feasible to disallow any connections to remote port 80 because this would make it impossible to surf the web.)

In principle, modern personal firewalls like Outpost 2 or Sygate Pro 5 have the ability to warn a user if a DLL is injected into a trusted application like Internet Explorer. However, the alert messages are usually inexpressive (and annoying because in most cases not DLL trojans but completely harmless DLLs are loaded into the trusted application). See also <http://www.securityfocus.com/bid/9312/discussion/>

#### **4. Common Injection Techniques**

Basically, there are two ways to inject a DLL trojan into a trusted host application. These ways are called dynamic & static DLL injection.

and forces the host process to load the trojan DLL. The key functions used to perform the injection are VirtualAllocEx, WriteProcessMemory and CreateRemoteThread. Trojan coders Aphex and Rezmond made the VX community happy by publishing the respective source codes. Moreover, there are several injection tools (Aphex Inject, Nuclear Inject etc.) which allow even script kiddies to inject DLL trojans into trusted host applications. Fortunately, these tools are detected as malware by many AV scanners.

We have called the dynamic injection technique "shady" because we believe that there is generally no legit reason to hijack other applications and perform functions like CreateRemoteThread. In other words, standard applications should not use this technique at all. If they do, they are highly suspicious. (This does not apply to certain system level applications.) In the last part of this article, we will make you familiar with two security tools that can prevent applications from (ab)using the function CreateRemoteThread.

(Please note that it is also possible to use the function SetWindowsHookEx for injecting DLLs. However, we do not know any trojans using this technique.)

#### (b) Static DLL Injection

Static DLL injection is a less frequently used but highly effective and dangerous technique to inject DLL trojans into trusted host applications. Broadly speaking, static DLL injection means that the code required to load the trojan DLL is patched directly into the host application. In other words, the host application is permanently infected and will load the trojan DLL (in addition to other harmless DLLs) each time it is started.

Static DLL injection has the "advantage" that a primitive loader application (and a conspicuous autostart entry in the registry) are not required. In addition, it is not necessary to use shady functions like CreateRemoteThread in order to have the DLL loaded (i.e., the standard LoadLibrary function can be used).

Consequently, it can be very hard to determine whether an application has been infected by means of static DLL injection. Primary targets for static DLL injection are applications which are traded via filesharing networks etc. In particular, internet



because most static DLL injections will remain undetected. We know for sure, however, that trojan coders are trying to perfect this injection technique: the source code for an automatic static injection tool has already been revealed. Fortunately, this particular source code is buggy and uses viral code so that the patched target application will be detected by AV scanners.

#### (c) Final Note

This article is not meant to be a tutorial for trojan coders. Therefore, we do not publish the source codes for dynamic DLL injection. Moreover, we do not discuss the particulars of static DLL injection (like entry point redirection and redirection from jumps). However, we would like to clarify that neither dynamic nor static DLL injection require any sophisticated programming skills. It takes virtually no time to compile the source code for a dynamic DLL injector and also static DLL injection can be done within less than a minute. Therefore, we believe that these injection techniques are not merely a theoretical threat.

We have collected/prepared a modest selection of trojan samples which demonstrate both injection techniques. The samples can be sent to AV/AT software producers upon request. Anybody else is invited to try the above-mentioned APM tool from DiamondCS which allows you to dynamically inject DLLs into running processes.

### **5. How do AV/AT scanners detect DLL trojans?**

Well ... they rarely do! Please note that users of DLL trojans are not stupid. It is common practice not to use a DLL trojan right "out of the box" since the standard distribution package (i.e., a bundle of files containing the loader application, the DLL trojan, etc.) is detected by almost every AV/AT scanner. Consequently, DLL trojans are frequently hexedited and protected with an executable compressor or crypter. An undetectable custom loader takes care for the injection.

For this reason, we believe that a good AV/AT scanner must be able to detect not only the standard distribution package or the loader application but the DLL trojan itself. We therefore compiled a sample test with a few DLL trojans stemming from our new test archive. (The new test archive which covers a reasonable selection of DLL trojans will be used for any future comparisons.)

|   |        |
|---|--------|
| ADDBYTE.10034.Coldfusion108.NotPacked.dll | 45 KB  |
| Armadillo301.Coldfusion108.Hexedited.dll  | 232 KB |
| ASPack212.Coldfusion108.dll               | 25 KB  |
| ASProtect11.Coldfusion108.dll             | 64 KB  |
| HEX.AphexFTP.UNPACKED.dll                 | 595 KB |
| HEX.Coldfusion108.NotPacked.dll           | 35 KB  |
| HEX.SimpleRename.Beast201.notpacked.dll   | 125 KB |
| JDPack101.Coldfusion108.hexedited.dll     | 25 KB  |
| Netwalker.Coldfusion108.Win98.dll         | 36 KB  |
| ORG.AphexFTP.UPX.dll                      | 248 KB |
| ORG.Beast201.notpacked.dll                | 125 KB |
| ORG.Coldfusion108.NotPacked.dll           | 35 KB  |
| PECompact150.Coldfusion108.dll            | 22 KB  |
| Petite22.AphexFTP.dll                     | 278 KB |
| Petite22.RESCCOMPR7.Beast201.dll          | 56 KB  |
| Petite22.Weak8.Beast201.dll               | 57 KB  |
| PKLite3211.AphexFTP.dll                   | 329 KB |
| RESOURCE.ICONREPL.Assasin20.NotPacked.dll | 131 KB |
| RESOURCE.RESCCOMPR.Beast201.Petite22.dll  | 56 KB  |
| tELock098.Coldfusion108.dll               | 31 KB  |
| UNPACKED.AphexFTP.dll                     | 595 KB |
| UPX190b.Coldfusion108.dll                 | 19 KB  |

The above mini archive contains a number of compressed/rypted DLLs. Moreover, there are DLL trojans which have been hexedited or increased in size. Finally, we modified or compressed the resource section of several trojans.

#### (a) AV Scanners /w Unpacking Support

Kaspersky Anti-Virus and McAfee VirusScan were chosen as representatives of a class of AV scanners with unpacking support.

Kaspersky did a relatively good job and detected 20 out of 22 DLL trojans. However, it failed to detect the malware samples packed with PKLite and Armadillo. This suffices to make any DLL trojan a gatecrasher. In addition, there are already many trojan users who employ advanced camouflage techniques (like patching and entry point obfuscation) which make an AV scanner like Kaspersky almost useless.

McAfee performed significantly worse than Kaspersky. It missed

Scanning for 77927 viruses, trojans and variants.

Options:

TESTDIR\\*. \* /ALL /SECURE /L /PANALYZE /PROGRAM /REPORT  
ZZZ\_ERGEBNIS.TXT

ORG.AphexFTP.UPX.dll ... Found the BackDoor-AHZ trojan !!!  
ORG.Beast201.notpacked.dll ... Found the BackDoor-AMQ  
trojan !!!  
ORG.Coldfusion108.NotPacked.dll ... Found the BackDoor-AOP.svr  
trojan !!!  
PECompact150.Coldfusion108.dll ... is OK.  
Petite22.AphexFTP.dll ... Found trojan or variant BackDoor-  
AHZ !!!  
Petite22.RESCCOMPR7.Beast201.dll ... is OK.  
Petite22.Weak8.Beast201.dll ... is OK.  
PKLite3211.AphexFTP.dll ... is OK.  
RESOURCE.ICONREPL.Assasin20.NotPacked.dll ... is OK.  
RESOURCE.RESCCOMPR.Beast201.Petite22.dll ... is OK.  
tELock098.Coldfusion108.dll ... is OK.  
UNPACKED.AphexFTP.dll ... Found trojan or variant BackDoor-  
AHZ !!!  
UPX190b.Coldfusion108.dll ... is OK.  
ADDBYTE.10034.Coldfusion108.NotPacked.dll ... Found trojan or  
variant BackDoor-AOP.svr !!!  
Armadillo301.Coldfusion108.Hexedited.dll ... is OK.  
ASPack212.Coldfusion108.dll ... is OK.  
ASProtect11.Coldfusion108.dll ... is OK.  
HEX.AphexFTP.UNPACKED.dll ... Found trojan or variant  
BackDoor-AHZ !!!  
HEX.Coldfusion108.NotPacked.dll ... Found trojan or variant  
BackDoor-AOP.svr !!!  
HEX.SimpleRename.Beast201.notpacked.dll ... Found trojan or  
variant BackDoor-AMQ !!!  
JDPack101.Coldfusion108.hexedited.dll ... is OK.  
Netwalker.Coldfusion108.Win98.dll ... is OK.

Summary report

File(s)

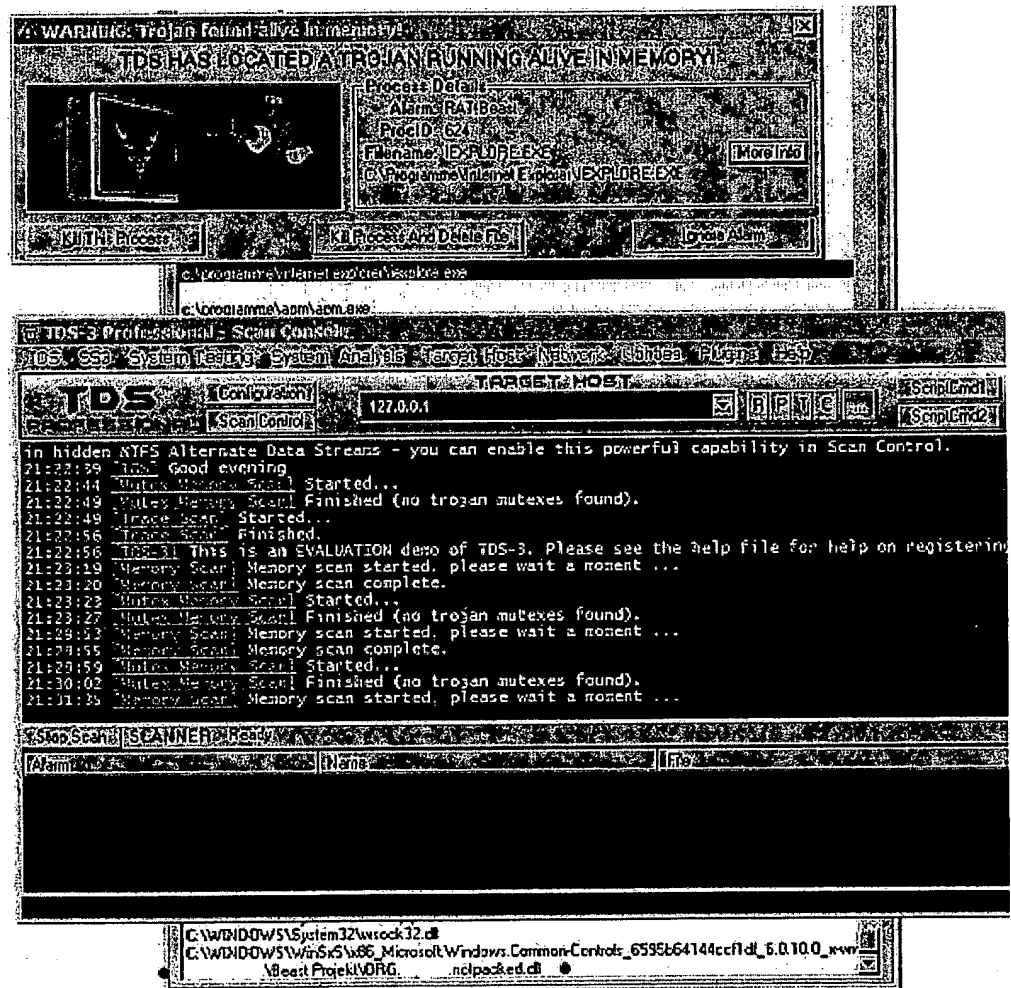
Total files: ..... 22

Clean: ..... 13

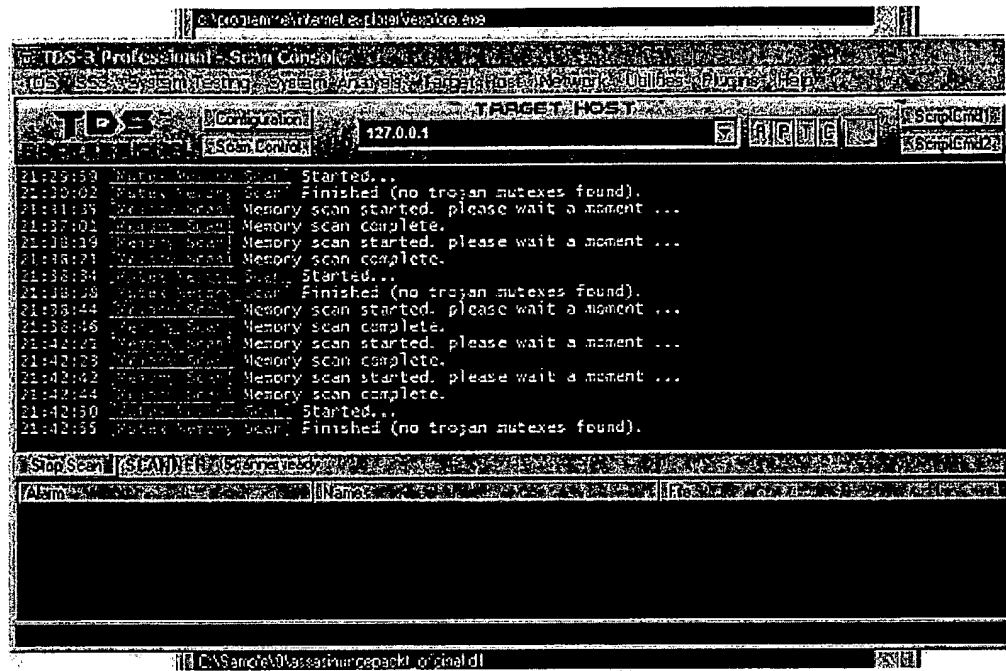
Possibly Infected: ..... 9

---

(b) Memory scanners

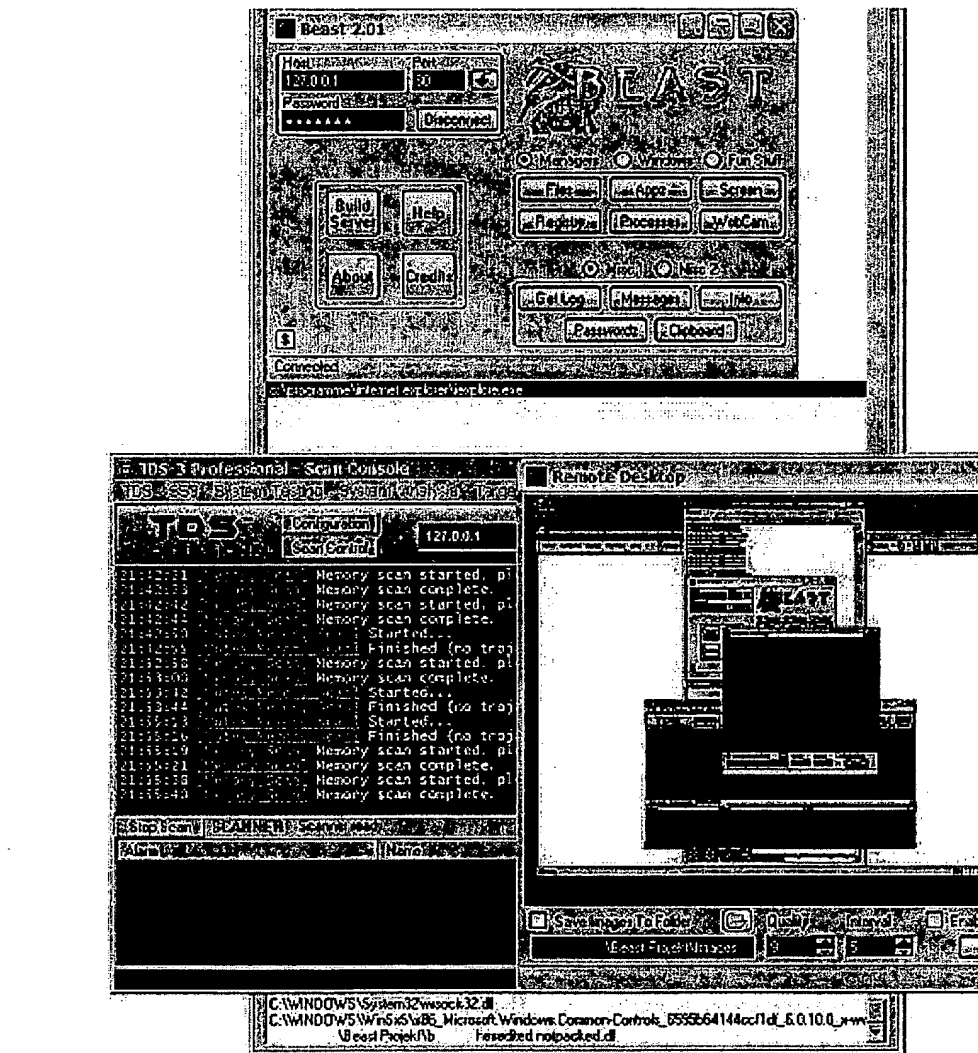


The bad thing is that TDS-3 did not automatically detect any other DLL trojans in memory, not even the widely-spread Assassin 2.0. It is necessary to open the TDS-3 process viewer and manually scan the modules of every active process in order to detect trojan DLLs. This procedure is quite uncomfortable and time consuming.



In addition, TDS-3 failed to detect a hexedited Beast 2.01 trojan because it uses a string containing the trojan's name as a signature (i.e., TDS-3 uses the most insecure signature you can possibly imagine).

| Offset  | 0  | 1  | 2  | 3  | 4  | 5  | 6  | 7  | 8  | 9  | A  | B  | C  | D  | E  | F  | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 1A | 1B | 1C | 1D | 1E | 1F |                     |
|---------|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|---------------------|
| 0013FE0 | 61 | 6E | 64 | 00 | FF | FF | FF | FF | 0C | 00 | 00 | 00 | 45 | 78 | 7D | 6C | 6F | 72 | 65 | 72 | 2E | 65 | 78 | 65 | 00 | 00 | 00 | 00 | FF | FF | FF | FF | end.yyyy...Explorer |
| 0014000 | 02 | 00 | 00 | 00 | 00 | 0A | 00 | 00 | FF | FF | FF | FF | 06 | 00 | 00 | 00 | 23 | 31 | 2E | 74 | 74 | 69 | 00 | 00 | 49 | 43 | 4F | 00 | 57 | 61 | 79 | 6E | .....yyyy...#1.v    |
| 0014020 | 65 | 6E | 00 | 00 | 53 | 59 | 53 | 00 | FF | FF | FF | FF | 04 | 00 | 00 | 00 | 2E | 62 | 6C | 66 | 00 | 00 | 00 | 00 | FF | FF | FF | FF | 13 | 00 | 00 | 00 | ty::SYS.yyyy...blf  |

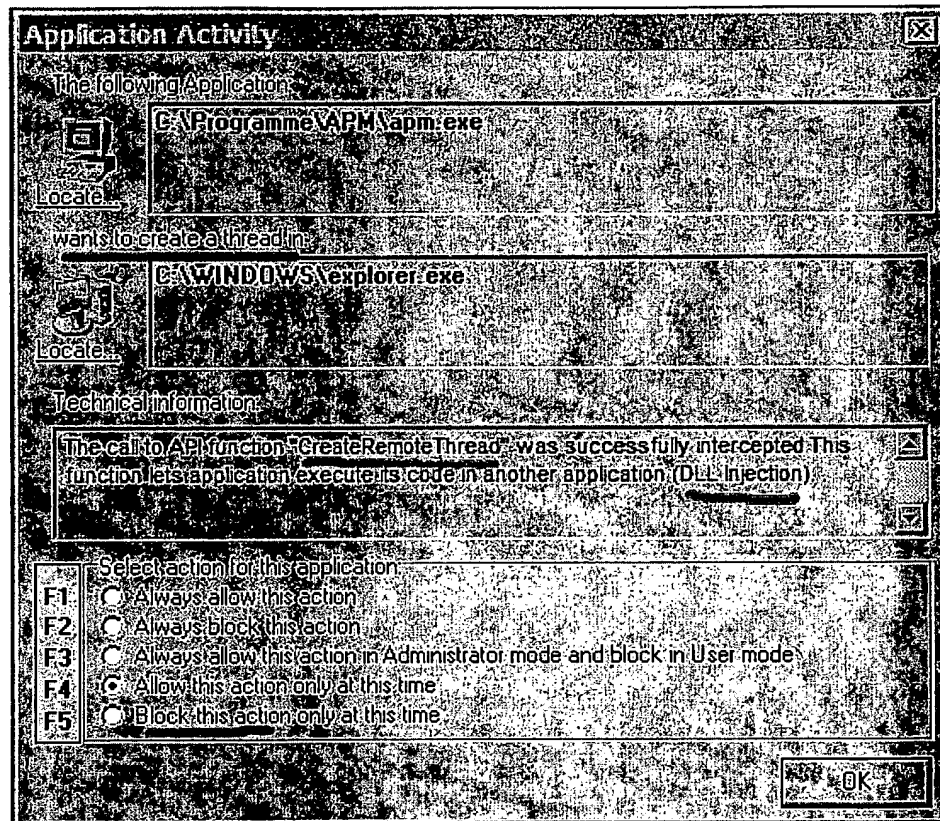


Note: According to our experience, other memory scanners like BoClean or TrojanHunter do not use "stronger" signatures than TDS-3. We believe that any of these AT products could significantly improve its performance if their makers kept an eye on signature quality. (N.B.: TDS-3 uses different signatures for file scanning. Unfortunately, it does not have an unpacking engine and, therefore, its file scanner detected only 6 out of 22 DLL trojans. )

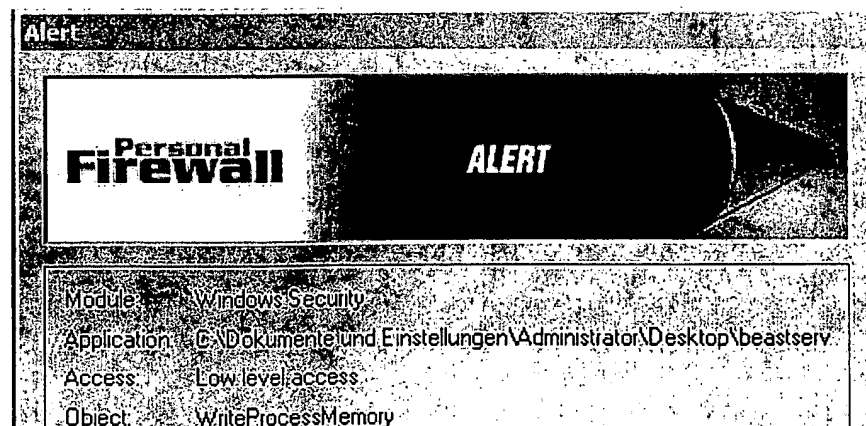
(c) Conclusion

stemming from trustworthy sources (not including filesharing networks, IRC channels, Newsgroups, and e-mail attachments) will significantly reduce the risk of being infected by any trojan. In addition (or alternatively) you may consider some of the following options:

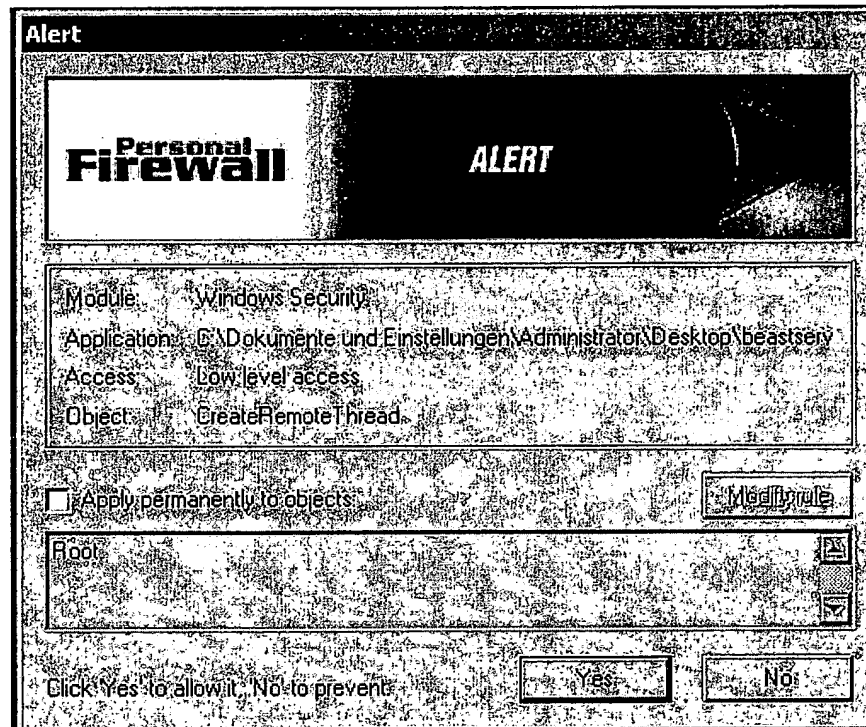
- (a) Be extra careful when using filesharing networks. Reconsider twice whether it is wise to grant internet access to an application which you have downloaded from a non-trustworthy source.
- (b) Surf a little bit. Thereafter, close the Internet Explorer (but do not close the internet connection). Open a process monitor like Process Explorer or APM. If you can still see a task called "iexplore.exe" (i.e., a hidden Internet Explorer window is still open) you may be infected. In such case you can inspect the modules loaded by iexplore.exe (or any other suspicious process) in order to determine the name of the malicious DLL. If you are in doubt you may ask for expert help in a computer security forum.
- (c) Use a freeware tool like TCPView (from Sysinternals) and check any open ports on your computer system. Make sure that you exactly know why a port is open.
- (d) Use a personal firewall and create a tight firewall rule set. Stop any applications from phoning home.
- (e) Create a firewall rule set which blocks your standard browser. Use alternative browsers like Opera, Mozilla or Firebird instead.
- (f) Check out a security tool called "System Safety Monitor". It will help you to block dynamic DLL injection by means of "CreateRemoteThread" and "SetWindowsHookEx".



(g) Alternatively check out "Tiny Personal Firewall". This firewall uses sandbox technology and will inform you if dynamic DLL injection takes place. (Please note that Tiny Personal Firewall is quite difficult to configure.)







(h) Use a freeware tool like Autostart Explorer (from Mischel Internet Security) and check your autostart entries. Use several AV/AT scanners. Be careful and good luck ...

ntl, 10 August 2003

**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

**BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- BLACK BORDERS
- IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT OR DRAWING
- BLURRED OR ILLEGIBLE TEXT OR DRAWING
- SKEWED/SLANTED IMAGES
- COLOR OR BLACK AND WHITE PHOTOGRAPHS
- GRAY SCALE DOCUMENTS
- LINES OR MARKS ON ORIGINAL DOCUMENT
- REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- OTHER: \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**

## Intercepting System API Calls

Various ways of function interception and a generic method to intercept system **API calls** without relying on commercial software packages or being bound to GNU licensing.

by **Seung-Woo Kim**

May 13, 2004

There are many cases where it is necessary for software developers or testers to intercept system function **calls** in order to instrument code or to extend operating-system functionality. There are a few packages available that provide this functionality, such as the Detours library from Microsoft or Syringe from OK Thinking Software. On the other hand, developers may wish to implement this functionality themselves, without implementing third-party software.

This article describes various ways of function interception and presents a generic method to achieve this task without relying on commercial software packages or being bound to GNU licensing. All materials in this paper were either developed by Intel or modified from MSDN sample code.

### Two Basic Techniques for Intercepting System Function Calls

Most methods of **intercepting** arbitrary function **calls** work by preparing a DLL that replaces the target function to be intercepted and then injecting the DLL to the target process; upon attaching to the target process, the DLL hooks itself to the target function. This technique is suitable, because the source code for the target application is not available most of the time, and it is relatively simple to write a DLL that contains the replacement function, separating it from the rest of the software.

Two **intercepting** methods have been studied and analyzed. Syringe works by modifying the function import entries (*thunking table*). On the other hand, the Detours library directly modifies the target function (in the target process space) to make an unconditional jump to the replacement function. Optionally, it provides a trampoline function that can call the original function.

The Detours technique follows this latter method because Syringe has trouble finding the thunks in many cases, and it does not provide trampoline capability to call the original function. Injecting the DLL works the same way in both cases.

The overall workflow to intercept system function **calls** is as follows:

1. **DLL Injection:** First, the main software opens the target process and forces it to load the DLL that contains the replacement functions.
2. **Target Function Modification:** When the DLL attaches to the process, it modifies the target function in the target process space so that it directly jumps to the replacement function in the DLL. Optionally, a trampoline function can call the original function.
3. **Target Function Intercepted:** When the target function is called, it directly jumps to the replacement function in the DLL. If the developer wishes to invoke the original functionality, he or she **calls** the trampoline function.

## DLL Injection

This section is entirely based on the MSDN article, "[Escape from DLL Hell with Custom Debugging and Instrumentation Tools and Utilities](#)," which includes downloadable source code. [Inject.cpp](#) and [Inject.h](#) are available in this article. They are customized for easy integration—just include them in a project and call [InjectLib](#). The algorithm to force the target process to load the DLL works as follows:

- Open the target process by calling [OpenProcess](#).
- Allocate memory in the target process by calling [VirtualAllocEx](#). Write to the allocated memory the name of the DLL to be injected using [WriteProcessMemory](#).
- Get the address of [LoadLibrary](#) by calling [GetProcAddress\(GetModuleHandle\(TEXT\("Kernel32"\)\), "LoadLibraryW"\)](#);
- Call [CreateRemoteThread](#), specifying the entry point of [LoadLibrary](#) and the name of the DLL (in step 2) as its argument. The target process will load the DLL.
- Free the allocated memory using [VirtualFreeEx](#). It is not needed anymore.

[Inject.cpp](#) incorporates a great deal more functionality, including substantial security features, but the preceding steps are sufficient to illustrate core concepts.

## Target-Function Modification

Target-function modification is self-modifying code that is well documented on [MSDN](#), although there are a few pitfalls in injecting [jmp](#) into the process memory. This section shows almost complete sample code to avoid confusion. The two aspects of target-function modification are replacement and trampoline functions.

The following code snippet is an example DLL to intercept the [GetSystemPowerStatus](#) API:

```

BOOL WINAPI GetSystemPowerStatusReplaced(LPSYSTEM_POWER_STATUS lpSystemPowerStatus)
{
    // Your replacement code goes here.
    return TRUE;
}

BOOL InterceptAPI(HMODULE hLocalModule, const char* c_szDllName,
                 const char* c_szApiName, DWORD dwReplaced)
{
    DWORD dwOldProtect;
    DWORD dwAddressToIntercept = (DWORD)GetProcAddress(
        GetModuleHandle((char*)c_szDllName), (char*)c_szApiName);
    BYTE *pbTargetCode = (BYTE *) dwAddressToIntercept;
    BYTE *pbReplaced = (BYTE *) dwReplaced;

    VirtualProtect((void *) dwAddressToIntercept, 5, PAGE_WRITECOPY, &dwOldProtect);

```

```

*pbTargetCode++ = 0xE9; // jump rel32
*((signed int *) (pbTargetCode)) = pbReplaced - (pbTargetCode +4);
VirtualProtect((void *) dwAddressToIntercept, 5, PAGE_EXECUTE, &dwOldProtect);

FlushInstructionCache(GetCurrentProcess(), NULL, NULL);
return TRUE;
}

BOOL WINAPI DllMain(HINSTANCE hinst, DWORD dwReason, LPVOID reserved)
{
    if (dwReason == DLL_PROCESS_ATTACH) {
        InterceptAPI(hinst, "kernel32.dll", "GetSystemPowerStatus",
        (DWORD) GetSystemPowerStatusReplaced);
    }
    else if (dwReason == DLL_PROCESS_DETACH) {
        // Cleanup
    }
    return TRUE;
}

```

The first thing this code does upon attaching is to call **InterceptAPI**. It requires the name of the module containing the target function, the name of the target function, and the address of the replacement function. **GetSystemPowerStatus** is in **kernel32.dll**. Other basic Win32 APIs, such as **MessageBox** and **PeekMessage**, are available in **user32.dll**. MSDN specifies the module to which each **API** belongs; a future enhancement could automatically find the correct module for a given **API**.

**InterceptAPI** overwrites the first five bytes of the target function to an unconditional jump (**opcode 0xE9**), followed by the displacement to the replacement function as a signed integer (four bytes). The displacement starts at the next instruction; hence, **pbReplaced - (pbTargetCode +4)** is required. Two cautions are necessary to make this code work:

- Change the protection mode of the region overwritten by **VirtualProtect**. Otherwise, an access-violation error occurs.
- **FlushInstructionCache** is necessary to support those cases where the instructions are already in cache. Otherwise, old code will run from cache, even though the instructions have been changed in memory.

Now, when the **GetSystemPowerStatus** function is called, all it does is to jump to our replacement function, and it returns directly to the caller, successfully **intercepting** the call.

### Trampoline Function

In many cases, the replacement function needs to call the original target function in addition to its own code, in order to extend the capability of the **API**, rather than replacing the whole thing. A trampoline function provides this functionality. The theory behind trampoline functions is as follows:

- Prepare a dummy function that has the same declaration that will be used as the trampoline. Make sure the dummy function is more than 10 bytes long.
- Before overwriting the first five bytes of the target function, copy them to the beginning of the trampoline function.
- Overwrite from the sixth byte of the trampoline with an unconditional jump to the sixth byte of the target function.
- Overwrite the target function as before.
- When a trampoline function is called (from the replacement function or anywhere else), it executes the first five bytes of the copied original code, and then jumps to the sixth byte of the real original code. The control returns to the caller of the trampoline. After optionally completing additional tasks, control returns to the caller of the **API**.

One additional complication exists, in that the sixth byte of the original code may be part of the previous instruction. In that case, the function overwrites part of the previous instruction and then crashes. In the case of **GetSystemPowerStatus**, the beginning of a new instruction after the first five bytes is the seventh byte. Thus, for this scheme to work, six bytes need to be copied to the trampoline, and the code must adjust this offset accordingly.

The number of bytes that the code needs to copy depends upon the **API**. It is necessary to look at the original target code (using a debugger or a disassembler) and to count the number of bytes to copy. A future enhancement could automatically detect the correct offset. Assuming that we know the correct offset, the following code shows the extended **InterceptAPI** function that sets up the trampoline function as well:

```

BOOL InterceptAPI(HMODULE hLocalModule, const char* c_szDllName, const char* c_szApiName,
                 DWORD dwReplaced, DWORD dwTrampoline, int offset)
{
    int i;
    DWORD dwOldProtect;
    DWORD dwAddressToIntercept = (DWORD)GetProcAddress(
        GetModuleHandle((char*)c_szDllName), (char*)c_szApiName);

    BYTE *pbTargetCode = (BYTE *) dwAddressToIntercept;
    BYTE *pbReplaced = (BYTE *) dwReplaced;
    BYTE *pbTrampoline = (BYTE *) dwTrampoline;

    // Change the protection of the trampoline region
    // so that we can overwrite the first 5 + offset bytes.
    VirtualProtect((void *) dwTrampoline, 5+offset, PAGE_WRITECOPY, &dwOldProtect);
    for (i=0;i<offset;i++)
        *pbTrampoline++ = *pbTargetCode++;
    pbTargetCode = (BYTE *) dwAddressToIntercept;

    // Insert unconditional jump in the trampoline.
    *pbTrampoline++ = 0xEB; // jump rel32
    *((signed int *) (pbTrampoline)) = (pbTargetCode+offset) - (pbTrampoline + 4);
}

```

```
VirtualProtect((void *) dwTrampoline, 5+offset, PAGE_EXECUTE, &dwOldProtect);

// Overwrite the first 5 bytes of the target function
VirtualProtect((void *) dwAddressToIntercept, 5, PAGE_WRITECOPY, &dwOldProtect);
*pbTargetCode++ = 0xE9; // jump rel32
*((signed int *) (pbTargetCode)) = pbReplaced - (pbTargetCode +4);
VirtualProtect((void *) dwAddressToIntercept, 5, PAGE_EXECUTE, &dwOldProtect);

// Flush the instruction cache to make sure
// the modified code is executed.
FlushInstructionCache(GetCurrentProcess(), NULL, NULL);
return TRUE;
}
```

### Conclusion

This article describes a generic method to intercept system function calls, as well as providing trampoline functions to retain the original functionality. Because this paper is a summary of methods, rather than a complete package, some details are not implemented:

- Automatic detection of the module containing the target API.
- Automatic detection of the offset for the trampoline function.
- Removing replacement functions and ejecting the DLL. (For now, the only way to clean up is to close the application.)

Nevertheless, the techniques, explanations, and source code in this article should be sufficient for developers to implement software that can intercept any system function calls without relying on third-party software packages.

### Additional Resources

#### Articles

- [Writing Portable, Adaptable Code Using Compl.lib](#)
- [Introduction to Intrinsics](#)
- [Intel@ Extreme Graphics 2: Developer's Guide](#)
- [Branch and Loop Reorganization to Prevent Mispredicts](#)

### Intel Software Forums

- <http://softwareforums.intel.com/ids>

*Page 1 of 1*

Seung-Woo Kim received his Ph.D in computer science at University of Minnesota and is currently working as a senior application engineer

at Intel. He specializes in the performance optimization for technical and commercial software.



## How To Subclass a Window in Windows 95

This article was previously published under Q125680

|             |                 |
|-------------|-----------------|
| Article ID  | : 125680        |
| Last Review | : July 11, 2005 |
| Revision    | : 1.3           |

### On This Page

↓ [SUMMARY](#)

↓ [MORE INFORMATION](#)

↓ [Method 1: Windows 95 and Windows NT](#)

↓ [Method 2: Windows NT Only](#)

↓ [Method 3: Windows 95 and Windows NT](#)

↓ [REFERENCES](#)

### SUMMARY

While sub-classing windows within the same application in Windows 95 is unchanged from Windows version 3.1, sub-classing windows belonging to other applications is somewhat more complicated in Windows 95. This article explains the process.

### MORE INFORMATION

For a 16-bit application, sub-classing methods are the same as they were in Windows version 3.1. However, Windows 95 performs some behind-the-scenes magic to make it possible for a 16-bit window to subclass a 32-bit window.

Usually, a subclass consists of saving one window procedure and substituting another in its place. However, this could present a problem when a 16-bit application tries to call a 32-bit window procedure. Windows 95 works around this potential problem by providing 32-bit windows with a 16-bit window procedure. All 32-bit windows will have the same selector for their wndProcs that references code in KRNL386.EXE where the 16-bit wndProcs for all 32-bit windows are stored. Eventually, each of these 16-bit wndProcs will jump to the real 32-bit window procedure.

Sub-classing windows belonging to another process, either 16-bit or 32-bit, from a 32-bit process or application works as it does in Windows NT. The difficulty is that each 32-bit process has its own private address space. Hence, a window procedure's address in one process is not valid in another. To get a window procedure from one process into another, you need to inject the subclass procedure code into the other process's address space. There are a number of ways to do this.

#### Method 1: Windows 95 and Windows NT

You can use the registry, hooks, or remote threads and the WriteProcessMemory() API to inject code into another process's address space.

#### Method 2: Windows NT Only

If you use the registry, the code that needs to be injected should reside in a DLL. By either running REGEDIT.EXE or using the registry APIs, add the \HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\AppInit\_DLLs key to the registry if it does not exist. Set its value to a string containing the DLL's pathname. This key may contain more than one DLL pathname separated by single spaces. This has the effect, once the machine is restarted, of loading the library with DLL\_PROCESS\_ATTACH into every process at its creation time. While this method is very easy, it also has several disadvantages. For example, the computer must be restarted before it takes effect, and the DLL will last the lifetime of the process.

#### Method 3: Windows 95 and Windows NT

You can also use hooks to inject code into another process's address space. When a window hooks another thread belonging to a different process, the system maps the DLL containing the hook procedure into the address space of the hooked thread. Windows will map the entire DLL, not just the hook procedure.

Because of this mapping, the target process will get a fresh copy of all the DLL[ASCII 146]s variables. Any changes to variables that are created by one process will not be available to another. One way to share DLL data among processes is to create a shared section:

```
#pragma data_seg(".MyData")
HWND hMyWin = NULL
HHOOK ghMyHookProc = MyProcedureName
...other data
#pragma data_seg()
```

These items should be initialized when the share is created. Please review the documentation on Win95[ASCII 146]s memory management to make sure that your data is sharable.

Be aware that shared sections are a violation of Level B security on WinNT systems, so be careful about what kind of data gets placed in these sections.

To subclass a window in another process, install a WH\_GETMESSAGE hook or another such hook on the thread that owns the window to be sub-classed. In the DLL that contains the hook procedure, include the subclass window procedure. In the hook procedure, call SetWindowLong() to enact the subclass. It is important to leave the hook in place until the subclass is no longer needed, so the DLL remains in the target window's address space. When the subclass is removed, the hook would be unhooked, thus un-mapping the DLL.

A third way to inject a DLL into another address space involves the use of remote threads and the WriteProcessMemory() API. It is more flexible and significantly more complicated than the previously mentioned methods, and is described in the following reference.

## REFERENCES

"Load Your 32-bit DLL into Another Process's Address Space Using INJLIB" by Jeffrey Richter, MSJ May 1994.

---

## APPLIES TO

- Microsoft Platform Software Development Kit-January 2000 Edition, when used with:  
Microsoft Windows 95

**Keywords:** kbhowto kbhook kbwndw kbwndwproc KB125680

---

© 2006 Microsoft Corporation. All rights reserved.

## Win32 Hooks

Kyle Marsh

Microsoft Developer Network Technology Group

Created: July 29, 1993

Revised: February 1994

Added exception for journal hooks in "Filter functions in DLLs" section.

Added .EXE file to where filters can reside in "WH\_JOURNALRECORD" and "WH\_JOURNALPLAYBACK" sections.

Changed HIWORD and LOWORD to HIBYTE and LOBYTE in "HC\_ACTION" section.



### Page Options

Average rating:  
7 out of 9



Rate this page



Print this page



E-mail this page



Add to Favorites

### Abstract

This article describes hooks and their use in the Microsoft® Win32® application programming interface (API). It discusses hook functions, filter functions, and the following types of hooks:

- WH\_CALLWNDPROC
- WH\_CBT
- WH\_DEBUG
- WH\_FOREGROUNDIDLE
- WH\_GETMESSAGE
- WH\_JOURNALPLAYBACK
- WH\_JOURNALRECORD
- WH\_KEYBOARD
- WH\_MOUSE
- WH\_MSGFILTER
- WH\_SHELL
- WH\_SYSMSGFILTER

**Terminology** In this article, the term *Windows* refers to the Windows family of operating systems, that is, 16-bit Windows, Windows NT®, and Windows for Workgroups. Likewise, *Windows 3.1* refers to the 3.1 version of these operating systems.

### Introduction

In the Microsoft® Windows® operating system, a hook is a mechanism by which a function can intercept events (messages, mouse actions, keystrokes) before they reach an application. The function can act on events and, in some cases, modify or discard them. Functions that receive events are called *filter functions* and are classified according to the type of event they intercept. For example, a filter function might want to receive all keyboard or mouse events. For Windows to call a filter function, the filter function must be installed—that is, attached—to a Windows hook (for example, to a keyboard hook). Attaching one or more filter functions to a hook is known as *setting* a hook. If a hook has more than one filter function attached, Windows maintains a chain of filter functions. The most recently installed function is at the beginning of the chain, and the least recently installed function is at the end.

When a hook has one or more filter functions attached and an event occurs that triggers the hook, Windows calls the first filter function in the filter function chain. This action is known as *calling* the hook. For example, if a filter function is attached to the CBT hook and an event that triggers the hook occurs (for example, a window is about to be created), Windows calls the CBT hook by calling the first function in the filter function chain.

To maintain and access filter functions, applications use the **SetWindowsHookEx** and the **UnhookWindowsHookEx** functions.

Hooks provide powerful capabilities for Windows-based applications. These applications can use hooks to:

- Process or modify all messages meant for all the dialog boxes, message boxes, scroll bars, or menus for an application (WH\_MSGFILTER).
- Process or modify all messages meant for all the dialog boxes, message boxes, scroll bars, or menus for the system (WH\_SYSMSGFILTER).
- Process or modify all messages (of any type) for the system whenever a **GetMessage** or a **PeekMessage** function is called (WH\_GETMESSAGE).
- Process or modify all messages (of any type) whenever a **SendMessage** function is called (WH\_CALLWNDPROC).
- Record or play back keyboard and mouse events (WH\_JOURNALRECORD, WH\_JOURNALPLAYBACK).
- Process, modify, or remove keyboard events (WH\_KEYBOARD).
- Process, modify, or discard mouse events (WH\_MOUSE).
- Respond to certain system actions, making it possible to develop computer-based training (CBT) for applications (WH\_CBT).
- Prevent another filter from being called (WH\_DEBUG).

Applications have used hooks to:

- Provide F1 help key support to menus, dialog boxes, and message boxes (WH\_MSGFILTER).
- Provide mouse and keystroke record and playback features, often referred to as *macros*. For example, the Windows Recorder accessory program uses hooks to supply record and playback functionality (WH\_JOURNALRECORD, WH\_JOURNALPLAYBACK).
- Monitor messages to determine which messages are being sent to a particular window or which actions a message generates (WH\_GETMESSAGE, WH\_CALLWNDPROC). The Spy utility program in the Platform SDK uses hooks to perform these tasks. The source for Spy is available in the SDK.
- Simulate mouse and keyboard input (WH\_JOURNALPLAYBACK). Hooks provide the only reliable way to simulate these activities. If you try to simulate these events by sending or posting messages, Windows internals do not update the keyboard or mouse state, which can lead to unexpected behavior. If hooks are used to play back keyboard or mouse events, these events are processed exactly like real keyboard or mouse events. Microsoft Excel uses hooks to implement its SEND.KEYS macro function.
- Provide CBT for applications that run in the Windows environment (WH\_CBT). The WH\_CBT hook makes developing CBT applications much easier.

## How to Use Hooks

To use hooks, you need to know:

- How to use the Windows hook functions to add and remove filter functions to and from a hook's filter function chain.
- What action the filter function you are installing will be required to perform.
- What kinds of hooks are available, what they can do, and what information (parameters) they pass to your filter function.

## Windows Hook Functions

Windows-based applications use the **SetWindowsHookEx**, **UnhookWindowsHookEx**, and **CallNextHookEx** functions to manage the hooks filter function chain. Before version 3.1, Windows implemented hook management with the **SetWindowsHook**, **UnhookWindowsHook**, and **DefHookProc** functions. Although these functions are implemented in Win32, they have fewer capabilities than the new (**Ex**) versions. Please convert your existing code

to the new versions of these functions, and always use the new functions for new code.

**SetWindowsHookEx** and **UnhookWindowsHookEx** are described below. See "Calling the next function in the filter function chain" for a discussion of **CallNextHookEx**.

### SetWindowsHookEx

The **SetWindowsHookEx** function adds a filter function to a hook. This function takes four arguments:

- An integer code describing the hook to which to attach the filter function, and the address of the filter function. These codes are defined in WINUSER.H and are described later.
- The address of the filter function. The filter function must be exported by including it in the **EXPORTS** statement in the module definition file for the application or dynamic-link library (DLL), or by using the appropriate compiler flags.
- The instance handle of the module containing the filter function. In Win32 (unlike Win16), this value should be NULL when installing a thread-specific hook (see below), but does not have to be NULL as the documentation states. When you install a systemwide hook or a thread-specific hook for a thread in another process, you must use the instance handle of the DLL where the filter function resides.
- The thread ID for which the hook is to be installed. If the thread ID is not zero, the installed filter function will be called only in the context of the specified thread. If the thread ID is zero, the installed filter function has system scope and may be called in the context of any thread in the system. An application or library can use the **GetCurrentThreadId** function to obtain the thread handle for hooking the current thread.

Some hooks may be set with system scope only; some may be set only for a specific thread; and others may have either system or thread scope, as shown in the following table.

| Hook               | Scope            |
|--------------------|------------------|
| WH_CALLWNDPROC     | Thread or System |
| WH_CBT             | Thread or System |
| WH_DEBUG           | Thread or System |
| WH_GETMESSAGE      | Thread or System |
| WH_JOURNALRECORD   | System Only      |
| WH_JOURNALPLAYBACK | System Only      |
| WH_FOREGROUNDIDLE  | Thread or System |
| WH_SHELL           | Thread or System |
| WH_KEYBOARD        | Thread or System |
| WH_MOUSE           | Thread or System |
| WH_MSGFILTER       | Thread or System |
| WH_SYSMSGFILTER    | System Only      |

For a given hook type, thread hooks are called first, followed by system hooks.

It is a good idea to use thread hooks instead of system hooks for several reasons. Thread hooks:

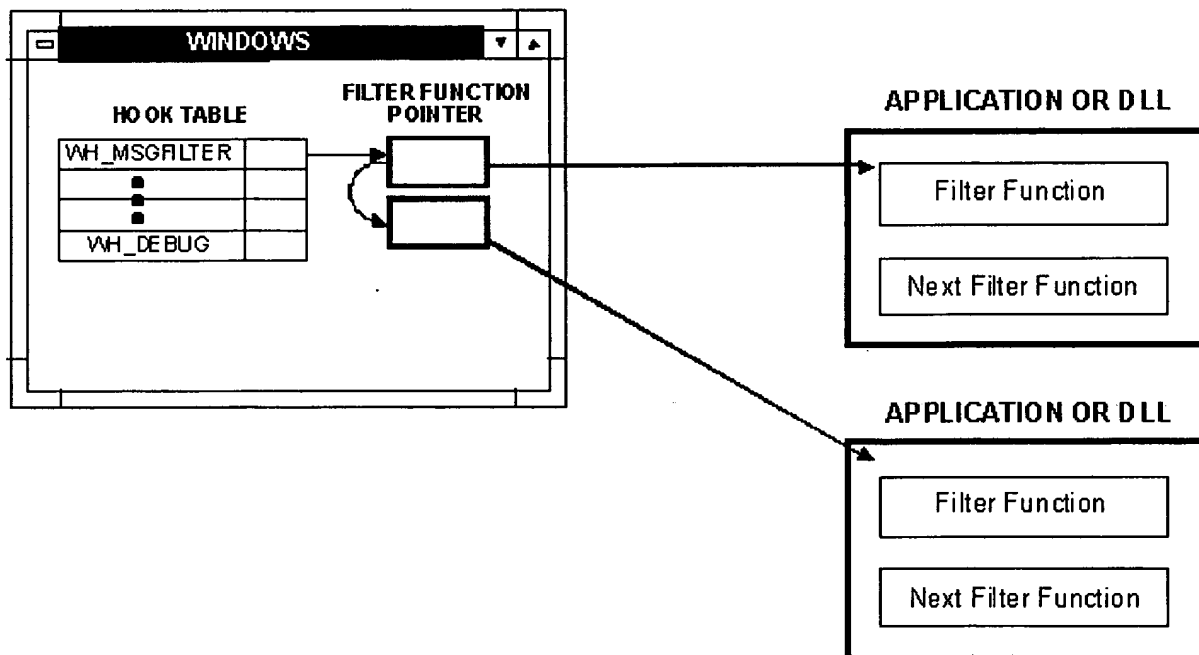
- Do not incur a systemwide overhead in applications that are not interested in the call.
- Do not cause all events for a hook to be serialized. For example, if an application installs a systemwide keyboard hook, all keyboard messages for all applications will be funneled through that application's keyboard filter function, effectively wasting the system's multiple input queue functionality. If that filter function stops processing keyboard events, the system will appear stopped to the user, but it will not really be stopped. The user can always use the CTRL+ALT+DEL key combination to log out and solve the problem, but he or she will probably not be happy with all this hassle. Also, users may not realize that they can reset the system with the logout/logon sequence.
- Do not require packaging the filter function implementation in a separate DLL. All systemwide hooks and hooks for threads in different applications must reside in DLLs.
- Do not need to share data within a DLL that is attached to different processes. A systemwide filter function, which must reside in a DLL, must also share any data that it needs with other processes. Since this is not

default DLL behavior, you must be careful when implementing systemwide filter functions. If a filter function is not correctly developed to share data and uses data in a process in which the data is invalid, the process may crash.

**SetWindowsHookEx** returns a handle to the installed hook (an HHOOK). The application or library must use this handle to identify this hook later when it calls the **UnhookWindowsHookEx** function. **SetWindowsHookEx** returns NULL if it is unable to add the filter function to the hook. **SetWindowsHookEx** also sets the last error to one of the values listed below to indicate why the function failed.

- **ERROR\_INVALID\_HOOK\_FILTER**: The hook code is invalid.
- **ERROR\_INVALID\_FILTER\_PROC**: The filter function is invalid.
- **ERROR\_HOOK\_NEEDS\_HMOD**: A global hook is being set with a NULL *hInstance* parameter or a thread-specific hook is being set for a thread that is not in the setting application.
- **ERROR\_GLOBAL\_ONLY\_HOOK**: A hook that can only be a system hook is being installed to a specific thread.
- **ERROR\_INVALID\_PARAMETER**: The thread ID is invalid.
- **ERROR\_JOURNAL\_HOOK\_SET**: There is already a hook set for a journal hook type. Only one journal record or journal playback hook can be installed at one time. This code can also be set if an application tries to set a journal hook while a screen saver is running.
- **ERROR\_MOD\_NOT\_FOUND**: The *hInstance* parameter for a global hook was not a library. (Actually, this value simply means that User was unable to locate the module handle in its list of modules.)
- Any other value: Security does not allow this hook to be set, or the system is out of memory.

Windows keeps the filter function chain internally (see the figure below) and does not rely on the filter functions to store the address of the next filter function in the chain correctly (as versions of Windows before 3.1 did). Thus, hooks are much more robust in Windows version 3.1 than they were in previous versions. In addition, performance is enhanced significantly because the filter function chain is kept internally.



**The filter function chain in Windows 3.1**

### **UnhookWindowsHookEx**

To remove a filter function from a hook's chain, call the **UnhookWindowsHookEx** function. This function takes the hook handle returned from **SetWindowsHookEx** and returns a value indicating whether the hook was removed.

**UnhookWindowsHookEx** always returns TRUE at this time.

## Filter Functions

Filter (*hook*) functions are functions that are attached to a hook. Because filter functions are called by Windows and not by an application, they are sometimes referred to as *callback functions*. For consistency, this article uses the term *filter functions*.

All filter functions must have the following form:

```
LRESULT CALLBACK FilterFunc( nCode, wParam, lParam )int nCode;
WORD wParam;
DWORD lParam;
```

All filter functions should return a **LONG**. *FilterFunc* is a placeholder for the actual filter function name.

## Parameters

Filter functions receive three parameters: *nCode* (the hook code), *wParam*, and *lParam*. The hook code is an integer code that informs the filter function of any additional data it should know. For example, the hook code might indicate what action is causing the hook to be called.

In previous versions of Windows (before 3.1), the hook code indicated whether the filter function should process the event or call **DefHookProc**. If the hook code is less than zero, the filter function should not process the event; it should call **DefHookProc**, passing the three parameters it was passed without any modification. Windows used these negative codes to maintain the filter function chain, with help from the applications.

Windows 3.1 still requires that if Windows sends a filter function a negative hook code, the filter function must call **CallNextHookEx** with the parameters Windows passed to the filter function. The filter function must also return the value returned by **CallNextHookEx**. Windows 3.1 never sends negative hook codes to filter functions.

The second parameter passed to the filter function, *wParam*, is a **WPARAM**, and the third parameter, *lParam*, is an **LPARAM**. These parameters pass information needed by the filter function. Each hook attaches different meanings to *wParam* and *lParam*. For example, filter functions attached to the WH\_KEYBOARD hook receive a virtual-key code in *wParam*, and *lParam* contains bit fields that describe the state of the keyboard at the time of the key event. Filter functions attached to the WH\_MSGFILTER hook receive a NULL value in *wParam* and a pointer to a message structure in *lParam*. Some hooks attach different meanings for *wParam* and *lParam* depending on the event that causes the hook to be called. For a complete list of arguments and their meanings for each hook type, see the filter functions listed below in Platform SDK.

| Hook               | Filter function documentation |
|--------------------|-------------------------------|
| WH_CALLWNDPROC     | <b>CallWndProc</b>            |
| WH_CBT             | <b>CBTProc</b>                |
| WH_DEBUG           | <b>DebugProc</b>              |
| WH_GETMESSAGE      | <b>GetMsgProc</b>             |
| WH_JOURNALRECORD   | <b>JournalRecordProc</b>      |
| WH_JOURNALPLAYBACK | <b>JournalPlaybackProc</b>    |
| WH_SHELL           | <b>ShellProc</b>              |
| WH_KEYBOARD        | <b>KeyboardProc</b>           |
| WH_MOUSE           | <b>MouseProc</b>              |
| WH_MSGFILTER       | <b>MessageProc</b>            |
| WH_SYSMSGFILTER    | <b>SysMsgProc</b>             |

## Calling the next function in the filter function chain

When a hook is set, Windows calls the first function in the hook's filter function chain, and the responsibility of Windows ends. The filter function is responsible for ensuring that the next filter function in the chain is called. Windows supplies **CallNextHookEx** to enable a filter function to call the next filter in the filter function chain.

**CallNextHookEx** takes four parameters.

The first parameter is the value returned from the **SetWindowsHookEx** call. This value is currently ignored by Windows, but this behavior may change in the future.

The next three parameters—*nCode*, *wParam*, and *lParam*—are the parameters that Windows passed to the filter function.

Windows stores the filter function chain internally and keeps track of which filter function it is calling. When **CallNextHookEx** is called, Windows determines the next filter function in the chain and calls that function.

At times, a filter function may not want to pass an event to the other hook functions on the same chain. In particular, when a hook allows a filter function to discard an event and the filter function decides to do so, the function must not call **CallNextHookEx**. When a filter function modifies a message, it may decide not to pass the message to the rest of the filter function chain.

Because filter functions are not installed in any particular order, you cannot be sure where your function is in the filter function chain at any moment except at the moment of installation, when it is the first function in the chain. As a result, you are never absolutely certain that you will get every event that occurs. A filter function installed ahead of your filter function in the chain—a function that was installed after your function timewise—might not pass the event to your filter function.

### Filter functions in DLLs

Systemwide filter functions must reside in a DLL. In Win16 it was possible (although not recommended) to install a systemwide hook to a filter function in an application. This does not work in Win32. Do not install systemwide filter functions that are not in DLLs, even if it does seem to work on a particular system. The journal hooks, **WH\_JOURNALRECORD** and **WH\_JOURNALPLAYBACK**, are exceptions to this rule. Because of the way Windows calls these hooks, their filter functions do not have to be in a DLL.

Filter functions for systemwide hooks must be prepared to share any data they need across the different processes they are running from. A DLL is mapped into the address space of each of its client processes. Global variables within the DLL will be instance specific unless they are placed in a shared data section. For example, the **HOOKSDLL.DLL** library in the Hooks sample application needs to share two data items:

- The window handle to display messages.
- The height of the text lines in that window.

To share this data, **HOOKSDLL** puts these data items in a shared data section. Here are the steps **HOOKSDLL** takes to share the data:

- Use pragmas to place the data in a named data segment. Note that the data must be initialized for this to work.

```
// Shared DATA
#pragma data_seg(".SHARDATA")
static HWND  hwndMain = NULL; // Main hwnd. We will get this from the app.
static int   nLineHeight = 0; // Height of lines in window.
#pragma data_seg()
```

- Add a **SECTIONS** statement to the DLL's .DEF file:

```
SECTIONS
    .SHARDATA    Read Write Shared
```

- Create an .EXP file from the .DEF file:

```
hooksdll.exp: hooksdll.obj hooksdll.def
```



```

$(implib) -machine:$(CPU) \
-def:hooks.def \
hooksdll.obj \
-out:hooksdll.lib

```

- Link with the HOOKSDLL.EXP file:

```

hooksdll.dll: hooksdll.obj hooksdll.def hooksdll.lib hooksdll.exp
$(link) $(linkdebug) \
-base:0x1C000000 \
-dll \
-entry:LibMain$(DLENTY) \
-out:hooksdll.dll \
hooksdll.exp hooksdll.obj hooksdll.rbj \
$(guilibsdll)

```

## Types of Hooks

### WH\_CALLWNDPROC

Windows calls this hook whenever the Windows **SendMessage** function is called. The filter functions receive a hook code from Windows indicating whether the message was sent from the current thread and receive a pointer to a structure containing the actual message.

The CWPSTRUCT structure has the following form:

```

typedef struct tagCWPSTRUCT {
    LPARAM lParam;
    WPARAM wParam;
    DWORD message;
    HWND hwnd;
} CWPSTRUCT, *PCWPSTRUCT, NEAR *NPCWPSTRUCT, FAR *LPCWPSTRUCT;

```

Filters can process the message, but cannot modify the message (this was possible in 16-bit Windows). The message is sent to the Windows function for which it was intended. This hook is a significant drain on system performance, especially when it is installed as a systemwide hook, so use it only as a development or debugging tool.

### WH\_CBT

To write a CBT application, the developer must coordinate the CBT application with the application for which it is written. Windows supplies the WH\_CBT hook to make this possible. Windows passes a hook code to the filter function, indicating which event has occurred and the appropriate data for the event.

A filter function attached to the WH\_CBT hook needs to be aware of ten hook codes:

- HCBT\_ACTIVATE
- HCBT\_CREATEWND
- HCBT\_DESTROYWND
- HCBT\_MINMAX
- HCBT\_MOVESIZE
- HCBT\_SYSCOMMAND
- HCBT\_CLICKSKIPPED
- HCBT\_KEYSKIPPED
- HCBT\_SETFOCUS

- HCBT\_QS

### HCBT\_ACTIVATE

Windows calls the `WH_CBT` hook with this hook code when any window is about to be activated. In the case of thread-specific hooks, the window must be owned by the thread. If the filter function returns `TRUE`, the window is not activated.

The *wParam* parameter contains the handle to the window being activated. The *lParam* parameter contains a far pointer to **CBTACTIVATESTRUCT**, which has the following structure:

```
typedef struct tagCBTACTIVATESTRUCT
{
    BOOL    fMouse;           // TRUE if activation results from a
                             // mouse click; otherwise FALSE.
    HWND    hWndActive;      // Contains the handle to the
                             // currently active window.
} CBTACTIVATESTRUCT, *LPCBTACTIVATESTRUCT;
```

### HCBT\_CREATEWND

Windows calls the `WH_CBT` hook with this hook code when a window is about to be created. In the case of thread-specific hooks, the thread must be creating the window. The `WH_CBT` hook is called before Windows sends the `WM_GETMINMAXINFO`, `WM_NCCREATE`, or `WM_CREATE` messages to the window. Thus, the filter function can return `TRUE` and not allow the window to be created.

The *wParam* parameter contains the handle to the window being created. The *lParam* parameter contains a pointer to the following structure.

```
/*
 * HCBT_CREATEWND parameters pointed to by lParam
 */
struct CBT_CREATEWND
{
    struct tagCREATESTRUCT *lpcs;    // The create parameters for the
                                     // new window.
    HWND    hWndInsertAfter;        // The window this window will
                                     // be added after, in Z-order.
} CBT_CREATEWND, *LPCBT_CREATEWND;
```

A filter function can alter the *hWndInsertAfter* value or the values in *lpcs*.

### HCBT\_DESTROYWND

Windows calls the `WH_CBT` hook with this hook code when Windows is about to destroy any window. In the case of thread-specific hooks, the thread must own the window. Windows calls the `WH_CBT` hook before the `WM_DESTROY` message is sent. If the filter function returns `TRUE`, the window is not destroyed.

The *wParam* parameter contains the handle to the window being destroyed. The *lParam* parameter contains `0L`.

### HCBT\_MINMAX

Windows calls the `WH_CBT` hook with this hook code when Windows is about to minimize or maximize a window. In the case of thread-specific hooks, the thread must own the window. If the filter function returns `TRUE`, the action does not occur.

The *wParam* parameter contains the handle to the window being minimized or maximized. The *lParam* is any one of the `SW_*` values defined in `WINUSER.H` specifying the operation that is taking place.

### HCBT\_MOVESIZE

Windows calls the `WH_CBT` hook with this hook code when Windows is about to move or size a window, and the

user has just finished selecting the new window position or size. In the case of thread-specific hooks, the thread must own the window. If the filter function returns TRUE, the action does not occur.

The *wParam* parameter contains the handle to the window being moved or sized. The *lParam* parameter contains an **LPRECT** that points to the drag rectangle.

### HCBT\_SYSCOMMAND

Windows calls the WH\_CBT hook with this hook code when Windows processes a system command. In the case of a thread-specific hook, the thread must own the window whose System menu is being used. The WH\_CBT hook is called from within **DefWindowsProc**. If an application does not send the WH\_SYSCOMMAND message to **DefWindowsProc**, this hook is not called. If the filter function returns TRUE, the system command is not processed.

The *wParam* parameter contains the system command (SC\_TASKLIST, SC\_HOTKEY, and so on) that is about to be performed. If *wParam* is SC\_HOTKEY, the LOWORD of *lParam* contains the handle to the window for which the hot key applies. If *wParam* contains any value other than SC\_HOTKEY and if the System menu command is selected with the mouse, the LOWORD of *lParam* contains the horizontal position of the cursor and the HIWORD of *lParam* contains the vertical position of the cursor.

The following system commands trigger this hook from within **DefWindowProc**:

|               |  |
|---------------|--|
| SC_CLOSE      | Close the window.  |
| SC_HOTKEY     | Activate the window associated with the application-specified hot key. |
| SC_HSCROLL    | Scroll horizontally.   |
| SC_KEYMENU    | Retrieve a menu through a keystroke.                                   |
| SC_MAXIMIZE   | Maximize the window.   |
| SC_MINIMIZE   | Minimize the window.   |
| SC_MOUSEMENU  | Retrieve a menu through a mouse click.                                 |
| SC_MOVE       | Move the window.   |
| SC_NEXTWINDOW | Move to the next window.   |
| SC_PREVWINDOW | Move to the previous window.   |
| SC_RESTORE    | Save the previous coordinates (checkpoint).                            |
| SC_SCREENSAVE | Execute the screen-save application.                                   |
| SC_SIZE       | Size the window.   |
| SC_TASKLIST   | Execute or activate the Windows Task Manager application.              |
| SC_VSCROLL    | Scroll vertically.   |

### HCBT\_CLICKSKIPPED

Windows calls the WH\_CBT hook with this hook code when a mouse event is removed from a thread's input queue and the mouse hook is set. Windows will call a systemwide hook when a mouse event is removed from any input queue and either a systemwide mouse hook or a thread-specific hook for the current thread is installed. This hook code is not generated unless a filter function is attached to the WH\_MOUSE hook. Despite its name, HCBT\_CLICKSKIPPED is called not only for skipped mouse events but also whenever a mouse event is removed from the system queue. Its main use is to install a WH\_JOURNALPLAYBACK hook in response to a mouse event. (See the "WM\_QUEUESYNC" section below for more information.)

The *wParam* parameter contains the message identifier for the mouse message—for example, the WM\_LBUTTONDOWN or any WM\_?BUTTON\* messages. The *lParam* parameter contains a far pointer to **MOUSEHOOKSTRUCT**, which has the following structure:

```
typedef struct tagMOUSEHOOKSTRUCT {
    POINT    pt;           // Location of mouse in screen coordinates
    HWND    hwnd;         // Window that receives this message
    UINT    wHitTestCode; // The result of hit-testing (HT_*)
    DWORD   dwExtraInfo;  // Extra info associated with the current message
} MOUSEHOOKSTRUCT, FAR *LPMOUSEHOOKSTRUCT, *PMOUSEHOOKSTRUCT;
```

### HCBT\_KEYSKIPPED

Windows calls the WH\_CBT hook with this hook code when a keyboard event is removed from the system queue and the keyboard hook is set. Windows will call a systemwide hook when a keyboard event is removed from any input queue and either a systemwide keyboard hook or a thread-specific hook for the current thread is installed. This hook code is not generated unless a filter function is attached to the WH\_KEYBOARD hook. Despite its name, HCBT\_KEYSKIPPED is called not only for skipped keyboard events but also whenever a keyboard event is removed from the system queue. Its main use is to install a WH\_JOURNALPLAYBACK hook in response to a keyboard event. (See the "WM\_QUEUESYNC" section below for more information.)

The *wParam* parameter contains the virtual-key code—the same value as *wParam* of **GetMessage** or **PeekMessage** for WM\_KEY\* messages. The *lParam* parameter contains the same value as the *lParam* parameter of **GetMessage** or **PeekMessage** for WM\_KEY\* messages.

### WM\_QUEUESYNC

While executing, a CBT application often must react to events in the main application. Keyboard or mouse events usually trigger these events. For example, a user clicks an OK button in a dialog box, after which the CBT application wants to play a series of keystrokes to the main application. The CBT application can use a mouse hook to determine whether the OK button was clicked. Upon determining that it wants to play some keystrokes to the main application, the CBT application must wait until the main application completes the processing of the OK button before beginning to play the new keystrokes. The CBT application would not want to apply the keystrokes to the dialog box.

The CBT application can use the WM\_QUEUESYNC message to monitor the main application and determine when an action is completed. The CBT application monitors the main application with a mouse or a keyboard hook and looks for events to which it must respond. By watching the main application with a mouse or a keyboard hook, the CBT application becomes aware of when an event that needs a response begins. The CBT application must wait until the event is completed before responding to it.

To determine when the action is complete, the CBT application takes these steps:

1. The CBT application waits until it receives the WH\_CBT hook with an HCBT\_CLICKSKIPPED or an HCBT\_KEYSKIPPED hook code from Windows. This happens when the event that is causing the action in the main application is removed from the system queue.
2. The CBT application installs a WH\_JOURNALPLAYBACK hook. The CBT application cannot install this hook until it receives either the HCBT\_CLICKSKIPPED or the HCBT\_KEYSKIPPED hook code. The WH\_JOURNALPLAYBACK hook plays a WM\_QUEUESYNC message to the CBT application. When the CBT application receives this message, it can respond to the original event. For example, the CBT application might play some keystrokes to the main application.

### HCBT\_SETFOCUS

Windows calls the WH\_CBT hook with this hook code when Windows is about to set the focus to any window. In the case of thread-specific hooks, the window must belong to the thread. If the filter function returns TRUE, the focus does not change.

The *wParam* parameter contains the handle to the window that receives the focus. The *lParam* parameter contains the handle to the window that loses the focus.

### HCBT\_QS

Windows calls the WH\_CBT hook with this hook code when a WM\_QUEUESYNC message is removed from the system queue while a window is being resized or moved. The hook is not called at any other time. In the case of thread-specific hooks, the window must belong to the thread.

Both the *wParam* and *lParam* parameters contain zero.

### WH\_DEBUG

Windows calls this hook when Windows is about to call a filter function. Filters cannot modify the values for the hook

but can stop Windows from calling the original filter function by returning a nonzero value.

The *wParam* parameter contains the ID of the hook to be called, for example, WH\_MOUSE. The *lParam* parameter contains a pointer to the following structure:

```
typedef struct tagDEBUGHOOKINFO
{
    DWORD    idThread;    // The thread ID for the current thread
    LPARAM   reserved;
    LPARAM   lParam;      // The lParam for the target filter function
    WPARAM   wParam;      // The wParam for the target filter function
    int      code;
} DEBUGHOOKINFO, *PDEBUGHOOKINFO, NEAR *NPDEBUGHOOKINFO, FAR* LPDEBUGHOOKINFO;
```

### WH\_FOREGROUNDIDLE

Windows calls this hook when there is no user input to process for the current thread. In the case of thread-specific hooks, Windows calls the hook only when that thread is the current thread and there is no input for the thread. This is a notification-only hook; both the *wParam* and *lParam* parameters are zero.

### WH\_GETMESSAGE

Windows calls this hook when the **GetMessage** or the **PeekMessage** function is about to return a message. The filter functions receive a pointer to a structure containing the actual message from Windows. The message, including any modifications, is sent to the application that originally called **GetMessage** or **PeekMessage**. The *lParam* parameter contains a pointer to a MSG structure:

```
typedef struct tagMSG {    /* msg */
    HWND    hwnd;        \\ The window whose Winproc will receive the message
    UINT    message;     \\ The message number
    WPARAM  wParam;
    LPARAM  lParam;
    DWORD   time;        \\ The time the message was posted
    POINT   pt;          \\ The cursor position in screen coordinates
                          \\ of the message
} MSG;
```

### WH\_HARDWARE

This hook is not currently implemented in Win32.

### Journal Hooks

Journal hooks are used to record and playback events. They are available only as systemwide hooks and should, therefore, be used as little as possible. These hooks affect all Windows-based applications; although the desktop allows no other hooks, journal hooks can record and play back events from and to the desktop. Another side-effect of journal hooks is that all system input queues are attached though the thread that installed the hook. This means that all system input must pass through this one point of execution.

Win32 takes special steps to allow a user to cancel a journal hook so that it does not lock the system. Windows will uninstall a record or playback journal hook when the user presses CTRL+ESC, ALT+ESC, or CTRL+ALT+DEL. Windows then notifies the application that had a journal hook installed by posting a WM\_CANCELJOURNAL message.

### WM\_CANCELJOURNAL

This message is posted with a NULL window handle so that it is not dispatched to a window procedure. The best way to catch this message is to install a WH\_GETMESSAGE filter function that watches for the message. The Win32 documentation also mentions that an application can catch the WM\_CANCELJOURNAL message between a call to **GetMessage** (or **PeekMessage**) and **DispatchMessage**. Although the message can be caught at this point, the application may not be there when the message is sent. For example, if the application is in a dialog box, its main message loop will not be called.

The CTRL+ESC, ALT+ESC, and CTRL+ALT+DEL key combinations are built into the system so the user can always stop a journal hook. It would be nice if every application that uses a journal hook could also supply a way for the user to stop journalling. The suggested way to stop journalling is by using VK\_CANCEL (CTRL+BREAK).

### WH\_JOURNALRECORD

Windows calls this hook when it removes an event from the system queue. Thus, these filters are called for all mouse and keyboard events except for those played back by a journal playback hook. Filters may process the message (that is, record or save the event in memory or on disk or both), but cannot modify or discard the message. Filters for this hook may reside in a DLL or an .EXE file. Only the HC\_ACTION hook code is implemented in Win32.

### HC\_ACTION

Windows calls the WH\_JOURNALRECORD hook with this hook code when it takes an event from the system queue. The hook code signals the filter function that this is a normal event. The *lParam* parameter to the filter function contains a pointer to an **EVENTMSG** structure. The usual recording procedure is to take all **EVENTMSG** structures passed to the hook and store them in memory or, if events exceed memory storage capacity, write them to disk.

The **EVENTMSG** structure is defined in WINDOWS.H and has the following structure:

```
typedef struct tagEVENTMSG {
    UINT    message;
    UINT    paramL;
    UINT    paramH;
    DWORD   time;
    HWND    hwnd;
} EVENTMSG;

typedef struct tagEVENTMSG *PEVENTMSG, NEAR *NPEVENTMSG, FAR *LPEVENTMSG;
```

The message element of the **EVENTMSG** structure is the message ID for the message, the WM\_\* value. The *paramL* and *paramH* values depend on whether the event is a mouse or a keyboard event. If it is a mouse event, the values contain the *x* and *y* coordinates of the event. If it is a keyboard event, *paramL* contains the scan code in the HIBYTE and the virtual-key code in the LOBYTE, and *paramH* contains the repeat count. Bit 15 of the repeat count specifies whether the event is an extended key. The time element of the **EVENTMSG** structure contains the system time (when the event occurred), which it obtained from the return value of **GetTickCount**. The *hwnd* is the window handle for the event.

The amount of time between events is determined by comparing the time element of an event with the time of subsequent events. This time delta is needed when playing back the recorded events.

### WH\_JOURNALPLAYBACK

This hook is used to provide mouse and keyboard messages to Windows as if they were inserted in the system queue. This hook is generally used to play back events recorded with the WH\_JOURNALRECORD hook, but also provides the best way to send events to another application. Whenever a filter function is attached to this hook, Windows calls the first filter function in the function chain to get events. Windows discards any mouse moves while WH\_JOURNALPLAYBACK is installed. All other keyboard and mouse input is queued until the WH\_JOURNALPLAYBACK hook has no filter functions attached. Filters for this hook may reside in a DLL or an .EXE file. A filter function attached to this hook needs to be aware of the following hook codes:

- HC\_GETNEXT
- HC\_SKIP

### HC\_GETNEXT

Windows calls the WH\_JOURNALPLAYBACK hook with this hook code when it accesses a thread's input queue. In most cases, Windows makes this call many times for the same message. The *lParam* parameter to the filter function

contains a pointer to an **EVENTMSG** structure (see above). The filter function must put the message, the *paramL* value, and the *paramH* value into the **EVENTMSG** structure. These are usually copied directly from the recorded event made during **WH\_JOURNALRECORD**.

The filter function must tell Windows when to process the message that the filter function is giving Windows. Windows needs two values for its scheduling: (1) the amount of time Windows should wait before processing the message; (2) the time at which the message is to be processed. The usual method of calculating the time to wait before processing is to subtract the **EVENTMSG** time element of the previous message from the **EVENTMSG** time element of the current message. This technique plays back messages at the speed at which they were recorded. If the message is to be processed immediately for much faster playback, the amount of time returned from the function is zero.

The time at which the message should be processed is usually obtained by adding the amount of time Windows should wait before processing the message to the current system time obtained from **GetTickCount**. For immediate playback, use the value returned from **GetTickCount**.

If the system is not otherwise active, Windows uses the values that the filter function has supplied to process the event. If the system is active, Windows examines the system queue. Each time it does, it asks for the same event with an **HC\_GETNEXT** hook code. Each time the filter function receives **HC\_GETNEXT**, it should return the new amount of time to wait, assuming that time elapsed between calls. The time element of the **EVENTMSG** structure and of the message, the *paramH* value, and the *paramL* value will probably not need changing between calls.

#### **HC\_SKIP**

Windows calls the **WH\_JOURNALPLAYBACK** hook with this hook code when it has completed processing a message it received from **WH\_JOURNALPLAYBACK**. This occurs at the time that Windows would have removed the event from the system queue, if the event had been in the system queue instead of being generated by a **WH\_JOURNALPLAYBACK** hook. This hook code signals to the filter function that the event that the filter function returned on the prior **HC\_GETNEXT** call has been returned to an application. The filter function should prepare to return the next event on the next **HC\_GETEVENT** call. When the filter function determines that it has no more events to play back, it should unhook itself during this **HC\_SKIP** call.

#### **WH\_KEYBOARD**

Windows calls this hook when the **GetMessage** or the **PeekMessage** function is about to return a **WM\_KEYUP**, **WM\_KEYDOWN**, **WM\_SYSKEYUP**, **WM\_SYSKEYDOWN**, or **WM\_CHAR** message. In the case of thread-specific hooks, the message must be from the thread's input queue. The filter function receives the virtual-key code and the state of the keyboard at the time of the keyboard hook. Filters can tell Windows to discard the message. A filter function attached to this hook needs to be aware of the following two hook codes:

- **HC\_ACTION**
- **HC\_NOREMOVE**

#### **HC\_ACTION**

Windows calls the **WH\_KEYBOARD** hook with this hook code when an event is being removed from the system queue.

#### **HC\_NOREMOVE**

Windows calls the **WH\_KEYBOARD** hook with this hook code when there is a keyboard event that is not being removed because an application is calling **PeekMessage** with the **PM\_NOREMOVE** option. If this hook code is passed, the key-state table will not accurately reflect the previous key state. An application needs to be aware of the existence of this condition.

#### **WH\_MOUSE**

Windows calls this hook when a **GetMessage** or a **PeekMessage** function is called and Windows has a mouse message to process. Like the **WH\_KEYBOARD** hook, this filter function receives a hook code, which indicates

whether the message is being removed (HC\_NOREMOVE), an identifier specifying the mouse message, and the *x* and *y* coordinates of the mouse. Filters can tell Windows to discard the message. Filters for this hook must reside in a DLL.

### WH\_MSGFILTER

Windows calls this hook when a dialog box, a message box, a scroll bar, or a menu retrieves a message, or when the user presses the ALT+TAB or ALT+ESC keys while the application that set the hook is active. This hook is thread specific, so it is always safe for its filter functions to reside in an application or in a DLL. The filter receives the following hook codes:

- MSGF\_DIALOGBOX: The message is for a dialog box or a message box.
- MSGF\_MENU: The message is for a menu.
- MSGF\_SCROLLBAR: The message is for a scroll bar.
- MSGF\_NEXTWINDOW: The next window action is about to take place.

There are other MSGF\_ values defined in WINUSER.H but they are not used in WH\_MSGFILTER hooks at this time.

The *lParam* parameter contains a pointer to a structure containing the message. The WH\_SYMSGFILTER hooks are called before the WH\_MSGFILTER hooks. If any of the WH\_SYMSGFILTER hook functions return TRUE, the WH\_MSGFILTER hooks are not called.

### WH\_SHELL

Windows calls this hook when actions occur to top-level (that is, unowned) windows. In the case of thread-specific hooks, Windows calls this hook only for windows that belong to the thread. This is a notification-only hook, so the filter function cannot modify or discard the event. The *wParam* parameter contains the handle to the window; the *lParam* parameter is not used. Three hook codes are defined in WINUSER.H for this hook:

- HSHELL\_WINDOWCREATED: Windows calls the WH\_SHELL hook when a top-level window is created. The window already exists when this hook is called.
- HSHELL\_WINDOWDESTROYED: Windows calls the WH\_SHELL hook when a top-level window is about to be destroyed.
- HSHELL\_ACTIVATESHELLWINDOW: This hook code is not used at this time.

### WH\_SYMSGFILTER

This hook is identical to WH\_MSGFILTER except that it is a systemwide hook. Windows calls this hook when a dialog box, a message box, a scroll bar, or a menu retrieves a message, or when the user presses the ALT+TAB or ALT+ESC keys. The filter receives the same hook code as WH\_MSGFILTER.

The *lParam* parameter contains a pointer to a structure containing the message. The WH\_SYMSGFILTER hooks are called before the WH\_MSGFILTER hooks. If any of the WH\_SYMSGFILTER hook functions return TRUE, the WH\_MSGFILTER hooks are not called.



Print E-Mail Add to Favorites

**How would you rate the quality of this content?**

1 2 3 4 5 6 7 8 9  
Poor          Outstanding

**Tell us why you rated the content this way. (optional)**

Average rating:  
7 out of 9



246 people have rated this page

[Manage Your Profile](#) | [Legal](#) | [Contact Us](#) | [MSDN Flash Newsletter](#)

© 2006 Microsoft Corporation. All rights reserved. [Terms of Use](#) | [Trademarks](#) | [Privacy Statement](#)



**BEST AVAILABLE COPY**

PATENT COOPERATION TREATY

From the INTERNATIONAL SEARCHING AUTHORITY

PCT

NOTIFICATION OF TRANSMITTAL OF  
THE INTERNATIONAL SEARCH REPORT AND  
THE WRITTEN OPINION OF THE INTERNATIONAL  
SEARCHING AUTHORITY, OR THE DECLARATION

(PCT Rule 44.1)

|   |   |  |
|---|---|--|
| To: William S. GALLIANI<br>Coolay Godward, LLP<br>One Freedom Square<br>Reston Town Center<br>Reston, Virginia 20190-5601<br>United States of America |   | Date of mailing<br>(day/month/year) <b>05 JUL 2006</b> |
| Applicant's or agent's file reference<br>WEBR00201WO  | <b>FOR FURTHER ACTION</b> See paragraphs 1 and 4 below                        |  |
| International application No.<br>PCT/US05/34874   | International filing date<br>(day/month/year) <b>28 SEP 2005 (28.09.2005)</b> |  |
| Applicant <b>WEBROOT SOFTWARE, INC.</b>   |   |  |

1.  The applicant is hereby notified that the international search report and the written opinion of the International Searching Authority have been established and are transmitted herewith.

**Filing of amendments and statement under Article 19:**  
 The applicant is entitled, if he so wishes, to amend the claims of the international application (see Rule 46):

**When?** The time limit for filing such amendments is normally two months from the date of transmittal of the international search report.

**Where?** Directly to the International Bureau of WIPO, 34 chemin des Colombettes  
 1211 Geneva 20, Switzerland, Facsimile No.: +41 22 740 14 35

**For more detailed instructions, see the notes on the accompanying sheet.**

2.  The applicant is hereby notified that no international search report will be established and that the declaration under Article 17(2)(a) to that effect and the written opinion of the International Searching Authority are transmitted herewith.

3.  **With regard to the protest** against payment of (an) additional fee(s) under Rule 40.2, the applicant is notified that:

the protest together with the decision thereon has been transmitted to the International Bureau together with the applicant's request to forward the texts of both the protest and the decision thereon to the designated Offices.

no decision has been made yet on the protest; the applicant will be notified as soon as a decision is made.

4. **Reminders**


Shortly after the expiration of 18 months from the priority date, the international application will be published by the International Bureau. If the applicant wishes to avoid or postpone publication, a notice of withdrawal of the international application, or of the priority claim, must reach the International Bureau as provided in Rules 90bis.1 and 90bis.3, respectively, before the completion of the technical preparations for international publication.

The applicant may submit comments on an informal basis on the written opinion of the International Searching Authority to the International Bureau. The International Bureau will send a copy of such comments to all designated Offices unless an international preliminary examination report has been or is to be established. These comments would also be made available to the public but not before the expiration of 30 months from the priority date.

Within 19 months from the priority date, but only in respect of some designated Offices, a demand for international preliminary examination must be filed if the applicant wishes to postpone the entry into the national phase until 30 months from the priority date (in some Offices even later); otherwise, the applicant must, within 20 months from the priority date, perform the prescribed acts for entry into the national phase before those designated Offices.

In respect of other designated Offices, the time limit of 30 months (or later) will apply even if no demand is filed within 19 months.

See the Annex to Form PCT/IB/301 and, for details about the applicable time limits, Office by Office, see the *PCT Applicant's Guide*, Volume II, National Chapters and the WIPO Internet site.

|   |   |
|---|---|
| Name and mailing address of the ISA/US<br>Mail Stop PCT, Attn: ISA/US<br>Commissioner for Patents<br>P.O. Box 1450, Alexandria, Virginia 22313-1450<br>Facsimile No. 571-273-3201 | Authorized officer:<br><br>Blaine R. Copenhagen<br>Telephone No. 571-272-7774 |
|---|---|

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

|  |   |  |
|--|---|--|
| Applicant's or agent's file reference<br>WEBR00201WO | <b>FOR FURTHER ACTION</b>   | see Form PCT/ISA/220<br>as well as, where applicable, item 5 below.                |
| International application No.<br>PCT/US05/34874      | International filing date ( <i>day/month/year</i> )<br>28 September 2005 (28.09.2005) | (Earliest) Priority Date ( <i>day/month/year</i> )<br>01 October 2004 (01.10.2004) |
| Applicant<br>WEBROOT SOFTWARE, INC.                  |   |  |

This international search report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This international search report consists of a total of 2 sheets.

It is also accompanied by a copy of each prior art document cited in this report.

1. Basis of the report

a. With regard to the language, the international search was carried out on the basis of:

- the international application in the language in which it was filed  
 a translation of the international application into \_\_\_\_\_, which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b))

b.  With regard to any nucleotide and/or amino acid sequence disclosed in the international application, see Box No. I.

2.  Certain claims were found unsearchable (see Box No. II)

3.  Unity of invention is lacking (see Box No. III)

4. With regard to the title,

- the text is approved as submitted by the applicant  
 the text has been established by this Authority to read as follows:

5. With regard to the abstract,

- the text is approved as submitted by the applicant  
 the text has been established, according to Rule 38.2(b), by this Authority as it appears in Box No. IV. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority

6. With regard to the drawings,

- a. the figure of the drawings to be published with the abstract is Figure No. 7  
 as suggested by the applicant  
 as selected by this Authority, because the applicant failed to suggest a figure  
 as selected by this Authority, because this figure better characterizes the invention
- b.  none of the figures is to be published with the abstract

## INTERNATIONAL SEARCH REPORT

International application No.

PCT/US05/34874

| <b>A. CLASSIFICATION OF SUBJECT MATTER</b><br>IPC(8) - G06F 11/30 (2006.01)<br>USPC - 726/22<br>According to International Patent Classification (IPC) or to both national classification and IPC   |  |  |   |  |  |   |  |   |   |  |   |  |   |  |      |  |
|---|--|--|---|--|--|---|--|---|---|--|---|--|---|--|------|--|
| <b>B. FIELDS SEARCHED</b><br>Minimum documentation searched (classification system followed by classification symbols)<br>U.S. : 726/11,13,22 713/ 188, 154, 152, 165<br>Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched<br>NONE<br>Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)<br>PUBWEST --PGPB, USPT, EPAB, and JPAB--searched spyware, malware, pestware, adware, malicious, quarantine, detect, find, firewall, compare, registry, scan, packet   |  |  |   |  |  |   |  |   |   |  |   |  |   |  |      |  |
| <b>C. DOCUMENTS CONSIDERED TO BE RELEVANT</b>   |  |  |   |  |  |   |  |   |   |  |   |  |   |  |      |  |
| <table border="1"> <thead> <tr> <th>Category*</th> <th>Citation of document, with indication, where appropriate, of the relevant passages</th> <th>Relevant to claim No.</th> </tr> </thead> <tbody> <tr> <td>X</td> <td>US 2004/0034794 A1 (MAYER et al.) 19 February 2004 (19.02.2004) see claim 2, 3, 4, and paragraphs 108, 115, 119, 127, and 128</td> <td>1-17</td> </tr> <tr> <td>A</td> <td>US 2004/0187023 A1 (ALAGNA et al.) 23 September 2004 (23.09.2004) see claim 5 and 6 and paragraphs 53,58, 75, 64, 93, 94, and 97</td> <td>1-32</td> </tr> <tr> <td>A</td> <td>US 6,633,835 B1 (MORAN et al.) 14 October 2003 (14.10.2003) see entire document</td> <td>1-32</td> </tr> <tr> <td>A</td> <td>US 2004/0143763 A1 (RADATTI) 22 July 2004 (22.07.2004) see entire document</td> <td>1-32</td> </tr> </tbody> </table>  | Category*  | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No.   | X  | US 2004/0034794 A1 (MAYER et al.) 19 February 2004 (19.02.2004) see claim 2, 3, 4, and paragraphs 108, 115, 119, 127, and 128  | 1-17  | A  | US 2004/0187023 A1 (ALAGNA et al.) 23 September 2004 (23.09.2004) see claim 5 and 6 and paragraphs 53,58, 75, 64, 93, 94, and 97  | 1-32  | A  | US 6,633,835 B1 (MORAN et al.) 14 October 2003 (14.10.2003) see entire document | 1-32   | A | US 2004/0143763 A1 (RADATTI) 22 July 2004 (22.07.2004) see entire document | 1-32 |  |
| Category*   | Citation of document, with indication, where appropriate, of the relevant passages   | Relevant to claim No.  |   |  |  |   |  |   |   |  |   |  |   |  |      |  |
| X   | US 2004/0034794 A1 (MAYER et al.) 19 February 2004 (19.02.2004) see claim 2, 3, 4, and paragraphs 108, 115, 119, 127, and 128  | 1-17   |   |  |  |   |  |   |   |  |   |  |   |  |      |  |
| A   | US 2004/0187023 A1 (ALAGNA et al.) 23 September 2004 (23.09.2004) see claim 5 and 6 and paragraphs 53,58, 75, 64, 93, 94, and 97   | 1-32   |   |  |  |   |  |   |   |  |   |  |   |  |      |  |
| A   | US 6,633,835 B1 (MORAN et al.) 14 October 2003 (14.10.2003) see entire document  | 1-32   |   |  |  |   |  |   |   |  |   |  |   |  |      |  |
| A   | US 2004/0143763 A1 (RADATTI) 22 July 2004 (22.07.2004) see entire document   | 1-32   |   |  |  |   |  |   |   |  |   |  |   |  |      |  |
| <input type="checkbox"/> Further documents are listed in the continuation of Box C.   |  |  |   |  |  |   |  |   |   |  |   |  |   |  |      |  |
| <input type="checkbox"/> See patent family annex.   |  |  |   |  |  |   |  |   |   |  |   |  |   |  |      |  |
| <table border="0"> <tr> <td>* Special categories of cited documents:</td> <td>"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention</td> </tr> <tr> <td>"A" document defining the general state of the art which is not considered to be of particular relevance</td> <td>"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone</td> </tr> <tr> <td>"E" earlier application or patent but published on or after the international filing date</td> <td>"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art</td> </tr> <tr> <td>"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)</td> <td>"&amp;" document member of the same patent family</td> </tr> <tr> <td>"O" document referring to an oral disclosure, use, exhibition or other means</td> <td></td> </tr> <tr> <td>"P" document published prior to the international filing date but later than the priority date claimed</td> <td></td> </tr> </table> |  | * Special categories of cited documents:   | "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention | "A" document defining the general state of the art which is not considered to be of particular relevance | "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone | "E" earlier application or patent but published on or after the international filing date | "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art | "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) | "&" document member of the same patent family | "O" document referring to an oral disclosure, use, exhibition or other means |   | "P" document published prior to the international filing date but later than the priority date claimed |   |  |      |  |
| * Special categories of cited documents:  | "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention  |  |   |  |  |   |  |   |   |  |   |  |   |  |      |  |
| "A" document defining the general state of the art which is not considered to be of particular relevance  | "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone   |  |   |  |  |   |  |   |   |  |   |  |   |  |      |  |
| "E" earlier application or patent but published on or after the international filing date   | "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art |  |   |  |  |   |  |   |   |  |   |  |   |  |      |  |
| "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)   | "&" document member of the same patent family  |  |   |  |  |   |  |   |   |  |   |  |   |  |      |  |
| "O" document referring to an oral disclosure, use, exhibition or other means  |  |  |   |  |  |   |  |   |   |  |   |  |   |  |      |  |
| "P" document published prior to the international filing date but later than the priority date claimed  |  |  |   |  |  |   |  |   |   |  |   |  |   |  |      |  |
| Date of the actual completion of the international search<br>03 March 2006 (03.03.2006)   | Date of mailing of the international search report<br><b>05 JUL 2006</b>   |  |   |  |  |   |  |   |   |  |   |  |   |  |      |  |
| Name and mailing address of the ISA/US<br>Mail Stop PCT, Attn: ISA/US, Commissioner for Patents<br>P.O. Box 1450, Alexandria, Virginia 22313-1450<br>Facsimile No. 571-273-3201   | Authorized officer:<br><i>Blaine R. Copenheaver</i> 607<br>Blaine R. Copenheaver<br>Telephone No. 571-272-7774   |  |   |  |  |   |  |   |   |  |   |  |   |  |      |  |

**PATENT COOPERATION TREATY**

From the  
INTERNATIONAL SEARCHING AUTHORITY

**PCT**

WRITTEN OPINION OF THE  
INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43bis.1)

To: William S. GALLIANI  
Cooley Godward, LLP  
One Freedom Square  
Reston Town Center  
Reston, Virginia 20190-5601  
United States of America

Date of mailing (day/month/year) **05 JUL 2006**

|   |   |   |  |
|---|---|---|--|
| Applicant's or agent's file reference<br><b>WEBR00201WO</b>   |   | <b>FOR FURTHER ACTION</b><br>See paragraph 2 below                    |  |
| International application No.<br><b>PCT/US05/34874</b>  | International filing date (day/month/year)<br><b>28 September 2005 (28.09.2005)</b> | Priority date (day/month/year)<br><b>01 October 2004 (01.10.2004)</b> |  |
| International Patent Classification (IPC) or both national classification and IPC<br><b>IPC(8) - G06F 11/30 (2006.01)</b><br><b>USPC - 726/22</b> |   |   |  |
| Applicant <b>WEBROOT SOFTWARE, INC.</b>   |   |   |  |

1. This opinion contains indications relating to the following items:

- Box No. I Basis of the opinion
- Box No. II Priority
- Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- Box No. IV Lack of unity of invention
- Box No. V Reasoned statement under Rule 43bis.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- Box No. VI Certain documents cited
- Box No. VII Certain defects in the international application
- Box No. VIII Certain observations on the international application

2. FURTHER ACTION

If a demand for international preliminary examination is made, this opinion will be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notified the International Bureau under Rule 66.1bis(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

3. For further details, see notes to Form PCT/ISA/220.

|   |   |  |
|---|---|--|
| Name and mailing address of the ISA/US<br>Mail Stop PCT, Attn: ISA/US<br>Commissioner for Patents<br>P.O. Box 1450, Alexandria, Virginia 22313-1450<br>Facsimile No. 571-273-3201 | Date of completion of this opinion<br><b>03 March 2006 (03.03.2006)</b> | Authorized officer:<br><i>Blaine R. Copenheaver</i><br>Blaine R. Copenheaver<br>Telephone No. 571-272-7774 |
|---|---|--|

WRITTEN OPINION OF THE  
INTERNATIONAL SEARCHING AUTHORITY

International application No.  
PCT/US05/34874

Box No. 1 Basis of this opinion

1. With regard to the language, this opinion has been established on the basis of:
  - the international application in the language in which it was filed
  - a translation of the international application into \_\_\_\_\_, which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b)).
  
2. With regard to any nucleotide and/or amino acid sequence disclosed in the international application and necessary to the claimed invention, this opinion has been established on the basis of:
  - a. type of material
    - a sequence listing
    - table(s) related to the sequence listing
  
  - b. format of material
    - on paper
    - in electronic form
  
  - c. time of filing/furnishing
    - contained in the international application as filed
    - filed together with the international application in electronic form
    - furnished subsequently to this Authority for the purposes of search
  
3.  In addition, in the case that more than one version or copy of a sequence listing and/or table(s) relating thereto has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.
  
4. Additional comments:

**WRITTEN OPINION OF THE  
INTERNATIONAL SEARCHING AUTHORITY**

International application No.

PCT/US05/34874

**Box No. V Reasoned statement under Rule 43bis.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement**

**1. Statement**

|                               |        |              |     |
|-------------------------------|--------|--------------|-----|
| Novelty (N)                   | Claims | <u>1-32</u>  | YES |
|                               | Claims | <u>NONE</u>  | NO  |
| Inventive step (IS)           | Claims | <u>18-32</u> | YES |
|                               | Claims | <u>1-17</u>  | NO  |
| Industrial applicability (IA) | Claims | <u>1-32</u>  | YES |
|                               | Claims | <u>NONE</u>  | NO  |

**2. Citations and explanations:**

Claim 1-17 lack an inventive step under PCT Article 33(3) as being obvious over Mayer (US 2004/0034794 A1). Per claim 1, Mayer discloses in receiving a data packet from a protected computer (paragraph 128 by "identifying the packets that are being sent out"), the data packet including a destination IP address (paragraph 111); comparing the destination IP address against a list of IP addresses associated ( paragraph 128 where a list or database of "applications allowed to access communication channels" is maintained) with pestware; and blocking the data packet from being delivered to the destination IP address when the destination IP address matches an entry in the list of IP addresses (paragraph 130 where communication initiation is checked for permission) associated with pestware. Mayer does not explicitly disclose the association of a destination ip address with pestware. The term pestware refers to any program that collects information about a person or an organization and then attempts to communicate the collected information to another device. See paragraph 3 of the instant application. Mayer recognizes that programs for collecting information (paragraph 111) and then use certain communication channels for conveying to another device (paragraph 128) exist. Mayer just fails to call these program pestware as does the instant application. Nevertheless, those in the art at the time of the invention would have recognized that pestware as defined in the claims is taught by Mayer.

Per claim 2, Mayer discloses in claim 3 presenting a user with the option of blocking the data packet from being delivered to the destination IP address when the destination IP address matches an entry in the list of IP addresses associated with pestware; and responsive to the user selecting to block the data packet, blocking the data packet.

Per claim 3, Mayer discloses in paragraph 128 middle of col. 2 receiving the data packet at a firewall appliance.

Per claim 4, Mayer discloses in claim 2 point A detecting an initial pestware activity on a protected computer; claim 3d recording the initial pestware activity; claim 2c receiving an instruction from a user of the protected computer to block the initial pestware activity; blocking the initial pestware activity; and claim 4g detecting a subsequent pestware activity; comparing the subsequent pestware activity with the initial pestware activity; and responsive to the subsequent pestware activity matching the initial pestware activity, automatically blocking the subsequent pestware activity.

Per claim 5, Mayer discloses in claim 2b detecting the initial pestware activity with an operating system shield.

Per claim 6, Mayer discloses in paragraph 108 detecting the initial pestware activity with a browser shield.

Per claim 7, Mayer discloses in paragraph 115 detecting an alteration of a registry file associated with the protected computer.

Per claim 8, Mayer discloses in page 14 col. 1 lines 17-19 detecting an attempted installation at the protected computer of a plug-in.

Per claim 9, Mayer discloses in paragraph 119 detecting the attempted startup at the protected computer of a pestware program.

Per claim 10, Mayer discloses in claim 3c comparing an indication of the pestware program with a definition of the pestware program.

Per claim 11, Mayer discloses in claim 4a detecting the attempted installation at the protected computer of a pestware program.

Per claim 12, Mayer discloses in claim 4a comparing an indication of the pestware program with a definition of the pestware program.

Per claim 13, Mayer discloses in paragraph 128 halfway down second column sending data from the protected computer to a host computer, the data indicating the subsequent pestware activity.

Per claim 14, Mayer discloses in paragraph 128 halfway down second column collecting information from the registry file about the subsequent pestware activity; and sending the collected information from the protected computer to a host computer.

Per claim 15, Mayer discloses in paragraph 128 halfway down second column identifying the process responsible for the subsequent pestware activity; and sending an identification of the process from the protected computer to a host computer.

Per claim 16, Mayer discloses in paragraph 127 identifying the process responsible for the subsequent pestware activity; and injecting termination code into the process.

Per claim 17, Mayer discloses in paragraph 127 identifying the file responsible for the subsequent pestware activity; and injecting termination code into the file.

See continuation in Supplemental Box below.

## NOTES TO FORM PCT/ISA/220

These Notes are intended to give the basic instructions concerning the filing of amendments under Article 19. The Notes are based on the requirements of the Patent Cooperation Treaty, the Regulations and the Administrative Instructions under that Treaty. In case of discrepancy between these Notes and those requirements, the latter are applicable. For more detailed information, see also the *PCT Applicant's Guide*, a publication of WIPO.

In these Notes, "Article," "Rule" and "Section" refer to the provisions of the PCT, the PCT Regulations and the PCT Administrative Instructions, respectively.

### INSTRUCTIONS CONCERNING AMENDMENTS UNDER ARTICLE 19

The applicant has, after having received the international search report and the written opinion of the International Searching Authority, one opportunity to amend the claims of the international application. It should however be emphasized that, since all parts of the international application (claims, description and drawings) may be amended during the international preliminary examination procedure, there is usually no need to file amendments of the claims under Article 19 except where, e.g. the applicant wants the latter to be published for the purposes of provisional protection or has another reason for amending the claims before international publication. Furthermore, it should be emphasized that provisional protection is available in some States only (see *PCT Applicant's Guide*, Volume I/A, Annexes B1 and B2).

The attention of the applicant is drawn to the fact that amendments to the claims under Article 19 are not allowed where the International Searching Authority has declared, under Article 17(2), that no international search report would be established (see *PCT Applicant's Guide*, Volume I/A, paragraph 296).

#### What parts of the international application may be amended ?

Under Article 19, only the claims may be amended.

During the international phase, the claims may also be amended (or further amended) under Article 34 before the International Preliminary Examining Authority. The description and drawings may only be amended under Article 34 before the International Preliminary Examining Authority.

Upon entry into the national phase, all parts of the international application may be amended under Article 28 or, where applicable, Article 41.

**When ?** Within 2 months from the date of transmittal of the international search report or 16 months from the priority date, whichever time limit expires later. It should be noted, however, that the amendments will be considered as having been received on time if they are received by the International Bureau after the expiration of the applicable time limit but before the completion of the technical preparations for international publication (Rule 46.1).

#### Where not to file the amendments ?

The amendments may only be filed with the International Bureau and not with the receiving Office or the International Searching Authority (Rule 46.2).

Where a demand for international preliminary examination has been/is filed, see below.

**How ?** Either by cancelling one or more entire claims, by adding one or more new claims or by amending the text of one or more of the claims as filed.

A replacement sheet must be submitted for each sheet of the claims which, on account of an amendment or amendments, differs from the sheet originally filed.

All the claims appearing on a replacement sheet must be numbered in Arabic numerals. Where a claim is cancelled, no renumbering of the other claims is required. In all cases where claims are renumbered, they must be renumbered consecutively (Section 205(b)).

**The amendments must be made in the language in which the international application is to be published.**

#### What documents must/may accompany the amendments ?

##### Letter (Section 205(b)):

The amendments must be submitted with a letter.

The letter will not be published with the international application and the amended claims. It should not be confused with the "Statement under Article 19(1)" (see below, under "Statement under Article 19(1)").

**The letter must be in English or French, at the choice of the applicant. However, if the language of the international application is English, the letter must be in English; if the language of the international application is French, the letter must be in French.**





UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

Table with 8 columns: APPLICATION NUMBER, FILING or 371(c) DATE, GRP ART UNIT, FIL FEE REC'D, ATTY.DOCKET.NO, DRAWINGS, TOT CLAIMS, IND CLAIMS. Row 1: 11/104,202, 04/12/2005, 2131, 1000, WEBR-011/00US, 3, 17, 3

CONFIRMATION NO. 1284

CORRECTED FILING RECEIPT

22903
COOLEY GODWARD KRONISH LLP
ATTN: PATENT GROUP
Suite 500
1200 - 19th Street, NW
WASHINGTON, DC20036-2402

Date Mailed: 01/30/2007

Receipt is acknowledged of this regular Patent Application. It will be considered in its order and you will be notified as to the results of the examination. Be sure to provide the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION when inquiring about this application. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. If an error is noted on this Filing Receipt, please mail to the Commissioner for Patents P.O. Box 1450 Alexandria Va 22313-1450. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections (if appropriate).

Applicant(s)

Michael Burtscher, Longmont, CO;

Power of Attorney: The patent practitioners associated with Customer Number 22903

Domestic Priority data as claimed by applicant

Foreign Applications

If Required, Foreign Filing License Granted: 05/16/2005

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is US11/104,202

Projected Publication Date: Not Applicable

Non-Publication Request: No

Early Publication Request: No

Title

System and method for directly accessing data from a data storage medium

Preliminary Class

## PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at <http://www.uspto.gov/web/offices/pac/doc/general/index.html>.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, <http://www.stopfakes.gov>. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4158).

---

### LICENSE FOR FOREIGN FILING UNDER

#### Title 35, United States Code, Section 184

#### Title 37, Code of Federal Regulations, 5.11 & 5.15

#### **GRANTED**

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of

Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign Assets Control, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

**NOT GRANTED**

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

In re Application of Michael BURTSCHER                      Confirmation No.: 1284  
Serial No.: 11/104,202    Group Art Unit: 2161  
Filed: 04/12/2005    Examiner: Not Yet Assigned

FOR: SYSTEM AND METHOD FOR DIRECTLY ACCESSING DATA FROM A DATA STORAGE MEDIUM

**Mail Stop Amendment**

Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

**INFORMATION DISCLOSURE STATEMENT  
UNDER 37 C.F.R. §1.97(b)**

In accordance with the duty of disclosure set forth in 37 C.F.R. §1.56, Applicant(s) hereby submits the following information in conformance with 37 C.F.R. §§1.97 and 1.98.

- No copies of any U.S. patents or U.S. patent application publications listed on the attached Form PTO/SB/08 are being provided pursuant to 37 C.F.R. §1.98.
- Publications listed on the attached Form PTO/SB/08 were cited in a foreign search or examination report corresponding to PCT/US2007/064490 mailed July 23, 2007.

This Information Disclosure Statement is filed within any one of the following time periods:


- within three months from the filing date of this national application other than a CPA under 37 C.F.R. § 1.53(d);
- within three months from the date of entry of the national stage as set forth in 37 C.F.R. §1.491 in this international application;
- before the mailing date of a first office action on the merits; or
- before the mailing of a first office action after the filing of a request for continued examination under 37 C.F.R. § 1.114.

It is respectfully requested that the Examiner consider the above-noted information and return an initialed copy of the attached Form PTO/SB/08 to the undersigned.

Dated: October 8, 2007

COOLEY GODWARD KRONISH LLP  
ATTN: Patent Group  
777 6<sup>th</sup> Street NW, Suite 1100  
Washington, DC 20001  
Tel: (720) 566-4044  
Fax: (202) 842-7899

Respectfully submitted,  
**COOLEY GODWARD KRONISH LLP**

By:   
Thomas M. Croft  
Reg. No. 44,051

Please type a plus sign (+) inside this box → +

|   |        |                          |                           |
|---|--------|--------------------------|---------------------------|
| Substitute for form 1449A/PTO<br><br><b>INFORMATION DISCLOSURE<br/>STATEMENT BY APPLICANT</b><br><br><i>(use as many sheets as necessary)</i> |        | <i>Complete if Known</i> |                           |
|   |        | Application Number       | 11/104,202                |
|   |        | Filing Date              | 04/12/2005                |
|   |        | First Named Inventor     | Michael BURTSCHER         |
|   |        | Group Art Unit           | 2161                      |
|   |        | Examiner Name            | Not Yet Assigned          |
| Sheet   | 1 of 1 | Attorney Docket Number   | WEBR-011/00US 303666-2011 |

| U.S. PATENT DOCUMENTS |                       |  |                                |   |   |
|-----------------------|-----------------------|--|--------------------------------|---|---|
| Examiner Initials*    | Cite No. <sup>1</sup> | Document Number                          | Publication Date<br>MM-DD-YYYY | Name of Patentee or Applicant of Cited Document | Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear |
|                       |                       | Number-Kind Code <sup>2</sup> (if known) |                                |   |   |
|                       |                       | US-2005/0120242 A1                       | 06-02-2005                     | Mayer   |   |

|                    |  |                 |  |
|--------------------|--|-----------------|--|
| Examiner Signature |  | Date Considered |  |
|--------------------|--|-----------------|--|

\*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. <sup>1</sup>Unique citation designation number (optional). <sup>2</sup>See attached Kinds of U.S. Patent Documents. This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

*If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.*

## Electronic Acknowledgement Receipt

|   |  |
|---|--|
| <b>EFS ID:</b>                              | 2289939  |
| <b>Application Number:</b>                  | 11104202   |
| <b>International Application Number:</b>    |  |
| <b>Confirmation Number:</b>                 | 1284   |
| <b>Title of Invention:</b>                  | System and method for directly accessing data from a data storage medium |
| <b>First Named Inventor/Applicant Name:</b> | Michael Burtscher  |
| <b>Customer Number:</b>                     | 22903  |
| <b>Filer:</b>                               | Thomas M. Croft/Sherry Bitler  |
| <b>Filer Authorized By:</b>                 | Thomas M. Croft  |
| <b>Attorney Docket Number:</b>              | WEBR-011/00US  |
| <b>Receipt Date:</b>                        | 08-OCT-2007  |
| <b>Filing Date:</b>                         | 12-APR-2005  |
| <b>Time Stamp:</b>                          | 18:58:27   |
| <b>Application Type:</b>                    | Utility under 35 USC 111(a)  |

### Payment information:

|                        |    |
|------------------------|----|
| Submitted with Payment | no |
|------------------------|----|

### File Listing:

| Document Number | Document Description                         | File Name          | File Size(Bytes) /Message Digest                                 | Multi Part /.zip | Pages (if appl.) |
|-----------------|--|--------------------|--|------------------|------------------|
| 1               | Information Disclosure Statement (IDS) Filed | WEBR01100USids.pdf | 93980<br><small>ab10f16426904d260d8aa88fb0076f5f9d1e8f5b</small> | no               | 3                |

### Warnings:

|  |
|--|
|  |
|--|

**Information:**

This is not an USPTO supplied IDS fillable form

**Total Files Size (in bytes):**

93980

**This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.**

**New Applications Under 35 U.S.C. 111**

**If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.**

**National Stage of an International Application under 35 U.S.C. 371**

**If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.**

**New International Application Filed with the USPTO as a Receiving Office**

**If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.**





# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

| APPLICATION NO.  | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO.          | CONFIRMATION NO. |
|--|-------------|----------------------|------------------------------|------------------|
| 11/104,202   | 04/12/2005  | Michael Burtscher    | WEBR-011/00US<br>303666-2011 | 1284             |
| 22903  | 7590        | 04/17/2008           | EXAMINER                     |                  |
| COOLEY GODWARD KRONISH LLP<br>ATTN: PATENT GROUP<br>Suite 1100<br>777 - 6th Street, NW<br>WASHINGTON, DC 20001 |             |                      | BARRON JR, GILBERTO          |                  |
|  |             |                      | ART UNIT                     | PAPER NUMBER     |
|  |             |                      | 2132                         |                  |
|  |             |                      | MAIL DATE                    | DELIVERY MODE    |
|  |             |                      | 04/17/2008                   | PAPER            |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.



UNITED STATES PATENT AND TRADEMARK OFFICE

COMMISSIONER FOR PATENTS  
UNITED STATES PATENT AND TRADEMARK OFFICE  
P.O. BOX 1450  
ALEXANDRIA, VA 22313-1450  
[www.uspto.gov](http://www.uspto.gov)

Cooley Godward LLP  
ATTN: Patent Group  
One Freedom Square  
Reston Town Center  
11951 Freedom Drive  
Reston, VA 20190-5656

In Re Application of: Michael Burtscher et al )  
Application No. 11/104,202 ) Petition under 37 CFR 1.48(a)  
Attorney Docket No. WEBR-011/00US )  
Filed: April 1, 2005 )  
For: System And Method For Directly Accessing )  
Data From A Data Storage Medium )

In view of the papers filed July 5, 2005, it has been found that this nonprovisional application, as filed, through error and without deceptive intent, improperly set forth the inventorship, and accordingly, this application has been corrected in compliance with 37 CFR 1.48(a). The inventorship of this application has been changed by adding of Tony Nichols, such that the current inventorship is now Michael Burtscher and Tony Nichols.

The petition has been **Granted**.

The application will be forwarded to the Office of Initial Patent Examination (OIPE) for issuance of a corrected filing receipt, and correction of Office records to reflect the inventorship as corrected.

Inquiries to this decision may be made to Primary Examiner Christopher Revak at (571) 272-3794.

Christopher Revak  
Primary Examiner  
Technology Center 2100

/Christopher Revak/  
April 14, 2008

Application/Control Number: 11/104,202  
Art Unit: 2131

Page 3

**Application Number**



**Application/Control No.**

11/104,202

**Applicant(s)/Patent under Reexamination**

BURTSCHER, MICHAEL

**Examiner**

Christopher A. Revak

**Art Unit**

2131

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

In re application of Michael Burtscher

Examiner: Not Yet Assigned

Serial No.: 11/104,202

Art Unit: 2131

Filed: April 12, 2005

Confirmation No.: 1284

FOR: SYSTEM AND METHOD FOR DIRECTLY ACCESSING DATA FROM A DATA STORAGE MEDIUM

---

**Mail Stop Amendment**

Commissioner for Patents

P.O. Box 1450

Alexandria, VA 22313-1450

**INFORMATION DISCLOSURE STATEMENT UNDER 37 C.F.R. §1.97(b)**

In accordance with the duty of disclosure set forth in 37 C.F.R. §1.56, Applicant(s) hereby submits the following information in conformance with 37 C.F.R. §§1.97 and 1.98.

- No copies of any U.S. patents or U.S. patent application publications listed on the attached Form PTO/SB/08 are being provided pursuant to 37 C.F.R. §1.98.

This Information Disclosure Statement is filed within any one of the following time periods:

- within three months from the filing date of this national application other than a CPA under 37 C.F.R. § 1.53(d);
- within three months from the date of entry of the national stage as set forth in 37 C.F.R. §1.491 in this international application;
- before the mailing date of a first office action on the merits; or
- before the mailing of a first office action after the filing of a request for continued examination under 37 C.F.R. § 1.114.

It is respectfully requested that the Examiner consider the above-noted information and return an initialed copy of the attached Form PTO/SB/08 to the undersigned.

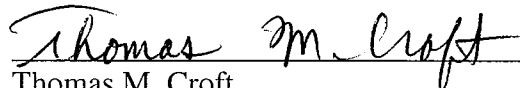
COOLEY GODWARD KRONISH LLP  
ATTN: Patent Group  
777 6<sup>th</sup> Street NW, Suite 1100  
Washington, DC 20001

Tel: (720) 566-4044

Fax: (202) 842-7899

Respectfully submitted,  
COOLEY GODWARD KRONISH LLP

By:



Thomas M. Croft

Reg. No. 44,051

|   |                  |                          |                           |
|---|------------------|--------------------------|---------------------------|
| Substitute for form 1449A/PTO<br><br><b>INFORMATION DISCLOSURE<br/>STATEMENT BY APPLICANT</b><br><br><i>(use as many sheets as necessary)</i> |                  | <i>Complete if Known</i> |                           |
|   |                  | Application Number       | 11/104,202                |
|   |                  | Filing Date              | 04/12/2005                |
|   |                  | First Named Inventor     | Michael BURTSCHER         |
|   |                  | Group Art Unit           | 2161                      |
| Examiner Name   | Not Yet Assigned |                          |                           |
| Sheet   | 1 of 1           | Attorney Docket Number   | WEBR-011/00US 303666-2011 |

| U.S. PATENT DOCUMENTS |                          |   |                                |  |  |
|-----------------------|--------------------------|---|--------------------------------|--|--|
| Examiner<br>Initials* | Cite<br>No. <sup>1</sup> | Document Number                             | Publication Date<br>MM-DD-YYYY | Name of Patentee or Applicant of<br>Cited Document | Pages, Columns, Lines, Where Relevant<br>Passages or Relevant Figures Appear |
|                       |                          | Number-Kind Code <sup>2</sup> (if<br>known) |                                |  |  |
|                       |                          | US-2006/0074896 A1                          | 04/06/2006                     | Thomas   |  |
|                       |                          | US-2006/0075501 A1                          | 04/06/2006                     | Thomas   |  |
|                       |                          | US-2006/0085528 A1                          | 04/20/2006                     | Thomas   |  |
|                       |                          | US-2006/0288416 A1                          | 12/21/2006                     | Costea   |  |
|                       |                          | US-5,715,455 A                              | 02/03/1998                     | Macon  |  |
|                       |                          | US-6,173,291                                | 01/09/2001                     | Jenevein   |  |
|                       |                          | US-7,346,611                                | 10/12/2006                     | Burtscher  |  |
|                       |                          | US-6,667,751                                | 12/23/2003                     | Wynn   |  |

|                       |  |                    |  |
|-----------------------|--|--------------------|--|
| Examiner<br>Signature |  | Date<br>Considered |  |
|-----------------------|--|--------------------|--|

\*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. <sup>1</sup>Unique citation designation number (optional). <sup>2</sup>See attached Kinds of U.S. Patent Documents. <sup>3</sup>Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). <sup>4</sup>For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. <sup>5</sup>Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. <sup>6</sup>Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

*If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.*

## Electronic Acknowledgement Receipt

|   |  |
|---|--|
| <b>EFS ID:</b>                              | 3914591  |
| <b>Application Number:</b>                  | 11104202   |
| <b>International Application Number:</b>    |  |
| <b>Confirmation Number:</b>                 | 1284   |
| <b>Title of Invention:</b>                  | System and method for directly accessing data from a data storage medium |
| <b>First Named Inventor/Applicant Name:</b> | Michael Burtscher  |
| <b>Customer Number:</b>                     | 22903  |
| <b>Filer:</b>                               | Thomas M. Croft/Sherry Bitler  |
| <b>Filer Authorized By:</b>                 | Thomas M. Croft  |
| <b>Attorney Docket Number:</b>              | WEBR-011/00US 303666-2011  |
| <b>Receipt Date:</b>                        | 09-SEP-2008  |
| <b>Filing Date:</b>                         | 12-APR-2005  |
| <b>Time Stamp:</b>                          | 19:55:38   |
| <b>Application Type:</b>                    | Utility under 35 USC 111(a)  |

### Payment information:

|                        |    |
|------------------------|----|
| Submitted with Payment | no |
|------------------------|----|

### File Listing:

| Document Number | Document Description                                    | File Name          | File Size(Bytes)/<br>Message Digest                              | Multi Part /.zip | Pages (if appl.) |
|-----------------|---|--------------------|--|------------------|------------------|
| 1               | Information Disclosure Statement (IDS)<br>Filed (SB/08) | WEBR01100USids.pdf | 92838<br><small>8b893a4ddb6063ca83941151a0821d5e88863efa</small> | no               | 3                |

### Warnings:

### Information:



Total Files Size (in bytes):

92838

**This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.**

**New Applications Under 35 U.S.C. 111**

**If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.**

**National Stage of an International Application under 35 U.S.C. 371**

**If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.**

**New International Application Filed with the USPTO as a Receiving Office**

**If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.**

PLUS Search Results for S/N 11104202, Searched Thu Sep 11 11:28:29 EDT 2008  
The Patent Linguistics Utility System (PLUS) is a USPTO automated search system for U.S. Patents from 1971 to the present PLUS is a query-by-example search system which produces a list of patents that are most closely related linguistically to the application searched. This search was prepared by the staff of the Scientific and Technical Information Center, SIRA.

|                |            |
|----------------|------------|
| 20060277182 90 | 5745701 48 |
| 20060277183 90 |            |
| 7346611 84     |            |
| 7349931 84     |            |
| 20060230290 84 |            |
| 20060230291 84 |            |
| 20060236389 84 |            |
| 20060236397 84 |            |
| 20070006311 84 |            |
| 20070073792 84 |            |
| 20070124267 84 |            |
| 20060265761 82 |            |
| 20060074896 76 |            |
| 20070074289 68 |            |
| 20070094496 68 |            |
| 20070203884 67 |            |
| 20070250817 66 |            |
| 20070250928 66 |            |
| 20070261117 66 |            |
| 20070169198 65 |            |
| 20070226704 63 |            |
| 20060085528 59 |            |
| 20060212940 59 |            |
| 20060236396 59 |            |
| 20070094732 59 |            |
| 20070169197 58 |            |
| 20070168694 55 |            |
| 20080010310 50 |            |
| 20080034430 50 |            |
| 20080052679 50 |            |
| 20070094726 49 |            |
| 20070094733 49 |            |
| 20070168982 49 |            |
| 20070169191 49 |            |
| 20070180520 49 |            |
| 20070226800 49 |            |
| 20070250818 49 |            |
| 20070300303 49 |            |
| 20080127352 49 |            |
| 4757533 48     |            |
| 6122629 48     |            |
| 6148402 48     |            |
| 5586301 48     |            |
| 5657470 48     |            |
| 5944821 48     |            |
| 6154751 48     |            |
| 5361359 48     |            |
| 5475625 48     |            |
| 5740433 48     |            |



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

| APPLICATION NO.  | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO.          | CONFIRMATION NO. |
|--|-------------|----------------------|------------------------------|------------------|
| 11/104,202   | 04/12/2005  | Michael Burtscher    | WEBR-011/00US<br>303666-2011 | 1284             |
| 22903  | 7590        | 09/17/2008           | EXAMINER                     |                  |
| COOLEY GODWARD KRONISH LLP<br>ATTN: PATENT GROUP<br>Suite 1100<br>777 - 6th Street, NW<br>WASHINGTON, DC 20001 |             |                      | CERVETTI, DAVID GARCIA       |                  |
|  |             |                      | ART UNIT                     | PAPER NUMBER     |
|  |             |                      | 2136                         |                  |
|  |             |                      | MAIL DATE                    | DELIVERY MODE    |
|  |             |                      | 09/17/2008                   | PAPER            |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

|                              |  |   |  |
|------------------------------|--|---|--|
| <b>Office Action Summary</b> | <b>Application No.</b><br>11/104,202     | <b>Applicant(s)</b><br>BURTSCHER, MICHAEL |  |
|                              | <b>Examiner</b><br>David García Cervetti | <b>Art Unit</b><br>2136                   |  |

**-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --**

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1)  Responsive to communication(s) filed on 12 April 2005.
- 2a)  This action is **FINAL**.
- 2b)  This action is non-final.
- 3)  Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4)  Claim(s) 1-17 is/are pending in the application.  
4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5)  Claim(s) \_\_\_\_\_ is/are allowed.
- 6)  Claim(s) 1-17 is/are rejected.
- 7)  Claim(s) \_\_\_\_\_ is/are objected to.
- 8)  Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9)  The specification is objected to by the Examiner.
- 10)  The drawing(s) filed on 12 April 2005 is/are: a)  accepted or b)  objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11)  The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12)  Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).  
a)  All    b)  Some \*    c)  None of:  
1.  Certified copies of the priority documents have been received.  
2.  Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.  
3.  Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- 1)  Notice of References Cited (PTO-892)
- 2)  Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3)  Information Disclosure Statement(s) (PTO/SB/08)  
Paper No(s)/Mail Date 9/9/08, 10/8/07, 9/1/06.
- 4)  Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_
- 5)  Notice of Informal Patent Application
- 6)  Other: \_\_\_\_\_

### **DETAILED ACTION**

1. Claims 1-17 are pending and have been examined.

#### ***Requirement for Information***

2. An issue of public use or on sale activity has been raised in this application. In order for the examiner to properly consider patentability of the claimed invention under 35 U.S.C. 102(b), additional information (such as user manual and technical specifications) regarding this issue is required as follows: "Spy Sweeper" and other Webroot corporation products.

3. Applicant is reminded that failure to fully reply to this requirement for information will result in a holding of abandonment.

#### ***Specification***

4. The disclosure is objected to because of the following informalities: the reference to application numbers provided in page 1 needs to be updated to reflect applications that have matured into patents. Appropriate correction is required.

#### ***Double Patenting***

5. Claims 1-17 are provisionally rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1-19 of Patent No. 7,346,611. Although the conflicting claims are not identical, they are not patentably distinct from each other because

- "a method for scanning files on a protected computer for pestware comprising: identifying a location of each of at least a first file, a second file and a third file in a file storage device of the protected computer; retrieving, while

Art Unit: 2136

substantially circumventing an operating system of the protected computer, information from the first file; and analyzing the information from the first file to determine whether the first file is a potential pestware file” (claim 1, instant application) is analogous to

- “A method for scanning files on a protected computer for pestware comprising: identifying a location of each of at least a first file, a second file and a third file in at least one file storage device of the protected computer; retrieving information from the first file; analyzing the information from the first file to determine whether the first file is a potential pestware file; accessing, after retrieving the information from the first file, the second file before accessing the third file in response to the time required to access the second file being less than the time required to access the third file; retrieving information from the second file; analyzing the information from the second file to determine whether the second file is a potential pestware file; and reporting results of the analyzing the information from the first and second files to a user” (claim 1, patent 7,346,611).

6. This is a provisional obviousness-type double patenting rejection because the conflicting claims of the instant application have not in fact been patented.

7. Claims 1-19 of Patent No. 7,346,611 contain every element of claims 1-17 of the instant application and thus anticipate the claims of the instant application. Claims 1-17 of the instant application therefore are not patently distinct from the copending application claims and as such are unpatentable for obvious-type double patenting. A

Art Unit: 2136

later patent/application claim is not patentably distinct from an earlier claim if the later claim is anticipated by the earlier claim.

8. “A later patent claim is not patentably distinct from an earlier patent claim if the later claim is obvious over, or anticipated by, the earlier claim. In re Longi, 759 F.2d at 896, 225 USPQ at 651 (affirming a holding of obviousness-type double patenting because the claims at issue were obvious over claims in four prior art patents); In re Berg, 140 F.3d at 1437, 46 USPQ2d at 1233 (Fed. Cir. 1998) (affirming a holding of obviousness-type double patenting where a patent application claim to a genus is anticipated by a patent claim to a species with that genus). “ELI LILLY AND COMPANY v BARR LABORATORIES, INC., United States Court of Appeals for the Federal Circuit, ON PETITION FOR REHEARING EN BANC (DECIDED: May 30, 2001).

9. “Claim 12 and Claim 13 are generic to the species of invention covered by claim 3 of the patent. Thus, the generic invention is “anticipated” by the species of the patented invention. Cf., Titanium Metals Corp. v. Banner, 778 F.2d 775, 227 USPQ 773 (Fed. Cir. 1985) (holding that an earlier species disclosure in the prior art defeats any generic claim) 4. This court’s predecessor has held that, without a terminal disclaimer, the species claims preclude issuance of the generic claim. In re Van Ornum, 686 F.2d 937, 944, 214 USPQ 761, 767 (CCPA 1982); Schneller, 397 F.2d at 354. Accordingly, absent a terminal disclaimer, claims 12 and 13 were properly rejected under the doctrine of obviousness-type double patenting.” (In re Goodman (CA FC) 29 USPQ2d 2010 (12/3/1993)

***Claim Rejections - 35 USC § 112***

10. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

11. Claims 1-3, 7-8, and 12-13 rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

12. The term "substantially" in the claims is a relative term which renders the claim indefinite. The term is not defined by the claim, the specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention. The metes and bounds of the claims are not clearly defined and what type of OS functionality is circumvented.

***Claim Rejections - 35 USC § 101***

13. 35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

14. Claims 1-17 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

15. Claims 1-11 are directed towards methods considered non-statutory because there is no useful, concrete, and tangible result produced that can be utilized in a useful way.

16. Claims 12-17 are directed towards a system or apparatus comprising only software since the modules are software, and as such are non-statutory.



***Claim Rejections - 35 USC § 102***

17. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

**18. Claims 1-17 are rejected under 35 U.S.C. 102(e) as being anticipated by Costea et al. (US 2006/0101282, hereinafter Costea).**

**Regarding claims 1, 7, and 12,** Costea teaches

identifying a location of each of at least a first file, a second file and a third file in a file storage device of the protected computer (par. 38, file's location);

retrieving, while substantially circumventing an operating system of the protected computer, information from the first file (par.38, information about files); and

analyzing the information from the first file to determine whether the first file is a potential pestware file (par.38, state of the file).

**Regarding claim 2,** Costea teaches wherein the identifying includes identifying the location of each of at least the first file, the second file and the third file while substantially circumventing the operating system (par.38, information about files and file's location, par. 51-54).

**Regarding claims 3, 8, and 13,** Costea teaches wherein the identifying includes: accessing a master file table of the file storage device, while substantially circumventing

Art Unit: 2136

the operating system; and identifying the location of each of at least the first file, the second file and the third file by analyzing the data of the master file table (par.38, mft, par.61-63).

**Regarding claims 4, 9, and 14**, Costea teaches wherein the identifying includes utilizing the operating system to identify the first file, the second file and the third file (par.38, information about files and file's location, par.57-59).

**Regarding claims 5, 10, and 15**, Costea teaches wherein the identifying includes identifying a cluster number of each of the a first file, a second file and a third file in a disk drive of the protected computer (par.38, inherent to file I/O routines by an OS, par.45-48).

**Regarding claims 6, 11, and 16**, Costea teaches sorting, by location on the file storage device, the first, second and third files so as to generated a sorted list, wherein the retrieving includes retrieving information from the first, the second and the third files by sequentially accessing the first, second and third files in the order the first, second and third files are listed in the sorted list (par.38, information about files and file's location, par.42-43).

**Regarding claim 17**, Costea teaches wherein the protected computer includes a plurality of storage devices, and wherein the plurality of files are distributed among the plurality of storage device (par.38, information about files and file's location, par.45-48).

***Conclusion***

19. Any inquiry concerning this communication or earlier communications from the examiner should be directed to David García Cervetti whose telephone number is (571)272-5861. The examiner can normally be reached on Monday-Tuesday and Thursday-Friday.

20. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on (571)272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

21. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/David García Cervetti/  
Examiner, Art Unit 2136

|                                   |                                       |   |             |
|-----------------------------------|---------------------------------------|---|-------------|
| <b>Notice of References Cited</b> | Application/Control No.<br>11/104,202 | Applicant(s)/Patent Under Reexamination<br>BURTSCHER, MICHAEL |             |
|                                   | Examiner<br>David García Cervetti     | Art Unit<br>2136  | Page 1 of 1 |

**U.S. PATENT DOCUMENTS**

| * |   | Document Number<br>Country Code-Number-Kind Code | Date<br>MM-YYYY | Name              | Classification |
|---|---|--|-----------------|-------------------|----------------|
| * | A | US-2003/0120947 A1                               | 06-2003         | Moore et al.      | 713/200        |
| * | B | US-2004/0199763 A1                               | 10-2004         | Freund, Gregor P. | 713/154        |
| * | C | US-2005/0155031 A1                               | 07-2005         | Wang et al.       | 717/170        |
| * | D | US-2005/0268112 A1                               | 12-2005         | Wang et al.       | 713/188        |
| * | E | US-2006/0010485 A1                               | 01-2006         | Gorman, Jim       | 726/003        |
| * | F | US-2006/0031940 A1                               | 02-2006         | Rozman et al.     | 726/027        |
| * | G | US-2006/0095967 A1                               | 05-2006         | Durham et al.     | 726/023        |
| * | H | US-2006/0101264 A1                               | 05-2006         | Costea et al.     | 713/165        |
| * | I | US-2006/0101282 A1                               | 05-2006         | Costea et al.     | 713/188        |
| * | J | US-2006/0200863 A1                               | 09-2006         | Ray et al.        | 726/024        |
| * | K | US-7,114,185 B2                                  | 09-2006         | Moore et al.      | 726/24         |
| * | L | US-7,302,584 B2                                  | 11-2007         | Tarbotton et al.  | 713/188        |
| * | M | US-7,383,581 B1                                  | 06-2008         | Moore et al.      | 726/24         |


**FOREIGN PATENT DOCUMENTS**

| * |   | Document Number<br>Country Code-Number-Kind Code | Date<br>MM-YYYY | Country | Name | Classification |
|---|---|--|-----------------|---------|------|----------------|
|   | N |  |                 |         |      |                |
|   | O |  |                 |         |      |                |
|   | P |  |                 |         |      |                |
|   | Q |  |                 |         |      |                |
|   | R |  |                 |         |      |                |
|   | S |  |                 |         |      |                |
|   | T |  |                 |         |      |                |

**NON-PATENT DOCUMENTS**

| * |   | Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages) |
|---|---|---|
|   | U |   |
|   | V |   |
|   | W |   |
|   | X |   |

\*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)  
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

|  |  |  |
|--|--|--|
| <b><i>Index of Claims</i></b><br><br> | <b>Application/Control No.</b><br><br>11104202 | <b>Applicant(s)/Patent Under Reexamination</b><br><br>BURTSCHER, MICHAEL |
|  | <b>Examiner</b><br><br>David García Cervetti   | <b>Art Unit</b><br><br>2136  |

|   |                 |
|---|-----------------|
| ✓ | <b>Rejected</b> |
| = | <b>Allowed</b>  |


|   |                   |
|---|-------------------|
| - | <b>Cancelled</b>  |
| ÷ | <b>Restricted</b> |

|   |                     |
|---|---------------------|
| N | <b>Non-Elected</b>  |
| I | <b>Interference</b> |

|   |                 |
|---|-----------------|
| A | <b>Appeal</b>   |
| O | <b>Objected</b> |

Claims renumbered in the same order as presented by applicant
  CPA
  T.D.
  R.1.47

| CLAIM |          | DATE       |  |  |  |  |  |  |  |
|-------|----------|------------|--|--|--|--|--|--|--|
| Final | Original | 09/11/2008 |  |  |  |  |  |  |  |
|       | 1        | ✓          |  |  |  |  |  |  |  |
|       | 2        | ✓          |  |  |  |  |  |  |  |
|       | 3        | ✓          |  |  |  |  |  |  |  |
|       | 4        | ✓          |  |  |  |  |  |  |  |
|       | 5        | ✓          |  |  |  |  |  |  |  |
|       | 6        | ✓          |  |  |  |  |  |  |  |
|       | 7        | ✓          |  |  |  |  |  |  |  |
|       | 8        | ✓          |  |  |  |  |  |  |  |
|       | 9        | ✓          |  |  |  |  |  |  |  |
|       | 10       | ✓          |  |  |  |  |  |  |  |
|       | 11       | ✓          |  |  |  |  |  |  |  |
|       | 12       | ✓          |  |  |  |  |  |  |  |
|       | 13       | ✓          |  |  |  |  |  |  |  |
|       | 14       | ✓          |  |  |  |  |  |  |  |
|       | 15       | ✓          |  |  |  |  |  |  |  |
|       | 16       | ✓          |  |  |  |  |  |  |  |
|       | 17       | ✓          |  |  |  |  |  |  |  |

|  |  |  |
|--|--|--|
| <b>Search Notes</b><br><br> | <b>Application/Control No.</b><br><br>11104202 | <b>Applicant(s)/Patent Under Reexamination</b><br><br>BURTSCHER, MICHAEL |
|  | <b>Examiner</b><br><br>David García Cervetti   | <b>Art Unit</b><br><br>2136  |

| SEARCHED |          |         |          |
|----------|----------|---------|----------|
| Class    | Subclass | Date    | Examiner |
| 713      | 182,188  | 9/11/08 | DGC      |
| 726      | 22,23,24 | 9/11/08 | DGC      |
| 717      | 127,131  | 9/11/08 | DGC      |

| SEARCH NOTES  |         |          |
|---|---------|----------|
| Search Notes  | Date    | Examiner |
| Inventor name search, ACM, IEEE, Springer, Altavista, Google, Scholar, ACE, PLUS, EAST history attached | 9/11/08 | DGC      |

| INTERFERENCE SEARCH |          |      |          |
|---------------------|----------|------|----------|
| Class               | Subclass | Date | Examiner |
|                     |          |      |          |

|   |  |
|---|--|
| /David García Cervetti/<br>Examiner.Art Unit 2136 |  |
|---|--|



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
 United States Patent and Trademark Office  
 Address: COMMISSIONER FOR PATENTS  
 P.O. Box 1450  
 Alexandria, Virginia 22313-1450  
 www.uspto.gov

BIB DATA SHEET

CONFIRMATION NO. 1284

|   |   |                               |   |  |                                |
|---|---|-------------------------------|---|--|--------------------------------|
| <b>SERIAL NUMBER</b><br>11/104,202  | <b>FILING or 371(c) DATE</b><br>04/12/2005<br><b>RULE</b>   | <b>CLASS</b><br>707           | <b>GROUP ART UNIT</b><br>2136   | <b>ATTORNEY DOCKET NO.</b><br>WEBR-011/00US<br>303666-2011 |                                |
| <b>APPLICANTS</b><br>Michael Burtscher, Longmont, CO; Tony Nichols, Erie, CO /DGC/<br>** CONTINUING DATA ***** 9/12/2008<br>** FOREIGN APPLICATIONS *****<br>** IF REQUIRED, FOREIGN FILING LICENSE GRANTED **<br>05/16/2005  |   |                               |   |  |                                |
| Foreign Priority claimed <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No<br>35 USC 119(a-d) conditions met <input type="checkbox"/> Yes <input type="checkbox"/> No<br>Verified and /DAVID GARCIA<br>CERVETTI/<br>Acknowledged Examiner's Signature | <input type="checkbox"/> Met after Allowance<br>DGC<br>Initials   | <b>STATE OR COUNTRY</b><br>CO | <b>SHEETS DRAWINGS</b><br>3   | <b>TOTAL CLAIMS</b><br>17                                  | <b>INDEPENDENT CLAIMS</b><br>3 |
| <b>ADDRESS</b><br>COOLEY GODWARD KRONISH LLP<br>ATTN: PATENT GROUP<br>Suite 1100<br>777 - 6th Street, NW<br>WASHINGTON, DC 20001<br>UNITED STATES   |   |                               |   |  |                                |
| <b>TITLE</b><br>System and method for directly accessing data from a data storage medium  |   |                               |   |  |                                |
| <b>FILING FEE RECEIVED</b><br>1000  | FEES: Authority has been given in Paper<br>No. _____ to charge/credit DEPOSIT ACCOUNT<br>No. _____ for following: |                               | <input type="checkbox"/> All Fees<br><input type="checkbox"/> 1.16 Fees (Filing)<br><input type="checkbox"/> 1.17 Fees (Processing Ext. of time)<br><input type="checkbox"/> 1.18 Fees (Issue)<br><input type="checkbox"/> Other _____<br><input type="checkbox"/> Credit |  |                                |

## EAST Search History

| Ref # | Hits | Search Query  | DBs                | Default Operator | Plurals | Time Stamp          |
|-------|------|---|--------------------|------------------|---------|---------------------|
| S1    | 50   | ("7346611"  <br>"20060230290"  <br>"20060230291"  <br>"20070124267"  <br>"20060277182"  <br>"20060277183"  <br>"7349931"  <br>"20060074896"  <br>"20060236397"  <br>"20070006311"  <br>"20080028466"  <br>"20070250818"  <br>"20080028462"  <br>"20070250817"  <br>"20060075501"  <br>"20070094496"  <br>"20070203884"  <br>"20060236389"  <br>"20060236396"  <br>"20070074289"  <br>"4757533"   "5144659"  <br>"5289540"   "5307497"  <br>"5881287"   "6105140"  <br>"6233576"   "6272611"  <br>"6317742"   "6993642"  <br>"6993649"   "7024581"  <br>"7318163"   "7395394"  <br>"20030023839"  <br>"20040111250"  <br>"20040117610"  <br>"20050039032"  <br>"20060031937"  <br>"20070186070"  <br>"20070226704"  <br>"20070261117"  <br>"20080010310"  <br>"20080028388"  <br>"4761737"   "7053936"  <br>"7120763"   "7203865"  <br>"20030011687"  <br>"20040143736").PN. | US-PGPUB;<br>USPAT | OR               | ON      | 2008/09/11<br>10:27 |



|     |      |  |                    |    |    |                     |
|-----|------|--|--------------------|----|----|---------------------|
| S2  | 50   | ("20060230291"  <br>"20060277182"  <br>"20060277183"  <br>"20070124267"  <br>"7346611"   "7349931"  <br>"20060230290"  <br>"20060236389"  <br>"20060236397"  <br>"20070006311"  <br>"20070073792"  <br>"20060265761"  <br>"20070203884"  <br>"20070074289"  <br>"20070094496"  <br>"20070226704"  <br>"4757533"   "5586301"  <br>"5657470"   "5926652"  <br>"5944821"   "5745701"  <br>"5974547"   "6154751"  <br>"6971018"   "5032979"  <br>"5261089"   "5289540"  <br>"5361359"   "5363446"  <br>"5475625"   "5537540"  <br>"5675833"   "5694583"  <br>"5710941"   "5758174"  <br>"5842002"   "5881287"  <br>"5892902"   "6092198"  <br>"6101607"   "6112312"  <br>"6175924"   "6199166"  <br>"6233576"   "6237023"  <br>"6269456"   "6366988"  <br>"6385645"   "6769075").<br>PN. | US-PGPUB;<br>USPAT | OR | ON | 2008/09/11<br>10:28 |
| S3  | 18   | S1 and S2  | US-PGPUB;<br>USPAT | OR | ON | 2008/09/11<br>10:28 |
| S4  | 1575 | 713/182.ccls.  | US-PGPUB;<br>USPAT | OR | ON | 2008/09/11<br>10:28 |
| S5  | 618  | 713/183.ccls.  | US-PGPUB;<br>USPAT | OR | ON | 2008/09/11<br>10:28 |
| S6  | 518  | 713/188.ccls.  | US-PGPUB;<br>USPAT | OR | ON | 2008/09/11<br>10:28 |
| S7  | 756  | 726/24.ccls.   | US-PGPUB;<br>USPAT | OR | ON | 2008/09/11<br>10:29 |
| S8  | 888  | 726/23.ccls.   | US-PGPUB;<br>USPAT | OR | ON | 2008/09/11<br>10:29 |
| S9  | 1286 | 726/22.ccls.   | US-PGPUB;<br>USPAT | OR | ON | 2008/09/11<br>10:29 |
| S10 | 812  | 717/127.ccls.  | US-PGPUB;<br>USPAT | OR | ON | 2008/09/11<br>10:29 |
| S11 | 555  | 717/131.ccls.  | US-PGPUB;<br>USPAT | OR | ON | 2008/09/11<br>10:29 |

|     |    |   |                    |    |    |                     |
|-----|----|---|--------------------|----|----|---------------------|
| S12 | 1  | "20060085528".pn.   | US-PGPUB;<br>USPAT | OR | ON | 2008/09/11<br>11:39 |
| S13 | 28 | (pestware spyware<br>malware adware<br>scumware spamware)<br>near5 circumvent\$   | US-PGPUB;<br>USPAT | OR | ON | 2008/09/11<br>12:30 |
| S14 | 3  | (pestware spyware<br>malware adware<br>scumware spamware)<br>near5 (analyz\$) near8<br>location   | US-PGPUB;<br>USPAT | OR | ON | 2008/09/11<br>12:34 |
| S15 | 1  | pestpatrol  | US-PGPUB;<br>USPAT | OR | ON | 2008/09/11<br>12:45 |
| S16 | 3  | pestpatrol pest adj patrol  | US-PGPUB;<br>USPAT | OR | ON | 2008/09/11<br>12:48 |
| S17 | 1  | spysweeper spy adj<br>sweeper   | US-PGPUB;<br>USPAT | OR | ON | 2008/09/11<br>12:50 |
| S18 | 9  | ad-aware  | US-PGPUB;<br>USPAT | OR | ON | 2008/09/11<br>12:50 |
| S19 | 50 | ("20060277182"<br>"20060277183"<br>"7346611" "7349931"<br>"20060230290"<br>"20060230291"<br>"20060236389"<br>"20060236397"<br>"20070006311"<br>"20070073792"<br>"20070124267"<br>"20060265761"<br>"20060074896"<br>"20070074289"<br>"20070094496"<br>"20070203884"<br>"20070250817"<br>"20070250928"<br>"20070261117"<br>"20070169198"<br>"20070226704"<br>"20060085528"<br>"20060212940"<br>"20060236396"<br>"20070094732"<br>"20070169197"<br>"20070168694"<br>"20080010310"<br>"20080034430"<br>"20080052679"<br>"20070094726"<br>"20070094733"<br>"20070168982"<br>"20070169191"<br>"20070180520" | US-PGPUB;<br>USPAT | OR | ON | 2008/09/11<br>12:53 |

|     |     |  |                    |    |    |                     |
|-----|-----|--|--------------------|----|----|---------------------|
|     |     | "20070226800"<br>"20070250818"<br>"20070300303"<br>"20080127352"<br>"4757533" "6122629"<br>"6148402" "5586301"<br>"5657470" "5944821"<br>"6154751" "5361359"<br>"5475625" "5740433"<br>"5745701" ).pn. |                    |    |    |                     |
| S20 | 401 | (pestware spyware<br>malware adware<br>scumware spamware).<br>clm.   | US-PGPUB;<br>USPAT | OR | ON | 2008/09/11<br>16:20 |
| S21 | 137 | (pestware spyware<br>malware adware<br>scumware spamware).<br>clm. with file.clm.  | US-PGPUB;<br>USPAT | OR | ON | 2008/09/11<br>16:20 |
| S22 | 26  | (pestware spyware<br>malware adware<br>scumware spamware).<br>clm. with file.clm. and<br>table.clm.  | US-PGPUB;<br>USPAT | OR | ON | 2008/09/11<br>16:21 |
| S23 | 7   | (pestware spyware<br>malware adware<br>scumware spamware).<br>clm. and master adj file<br>adj table.clm.   | US-PGPUB;<br>USPAT | OR | ON | 2008/09/11<br>16:21 |
| S24 | 5   | (pestware spyware<br>malware adware<br>scumware spamware).<br>clm. and master adj file<br>adj table.clm. and scan\$.<br>clm.   | US-PGPUB;<br>USPAT | OR | ON | 2008/09/11<br>16:25 |

9/12/2008 2:20:38 PM

C:\Documents and Settings\dcervetti\My Documents\EASTWorkspaces\11-104-202-09-11-2008.  
wsp



Please type a plus sign (+) inside this box → +

|   |        |                          |                   |
|---|--------|--------------------------|-------------------|
| Substitute for form 1449A/PTO<br><br><b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b><br><br><i>(use as many sheets as necessary)</i> |        | <b>Complete if Known</b> |                   |
|   |        | Application Number       | 11/104,202        |
|   |        | Filing Date              | 04/12/05          |
|   |        | First Named Inventor     | Michael Burtscher |
|   |        | Group Art Unit           | 2161              |
|   |        | Examiner Name            | Not Yet Assigned  |
| Sheet   | 1 of 2 | Attorney Docket No.      | WEBR-011/00US     |

| U.S. PATENT DOCUMENTS |                       |                      |   |   |  |
|-----------------------|-----------------------|----------------------|---|---|--|
| Examiner Initials*    | Cite No. <sup>1</sup> | U.S. Patent Document |   | Name of Patentee or Applicant of Cited Document | Date of Publication of Cited Document MM-DD-YYYY |
|                       |                       | Number               | Kind Code <sup>2</sup><br><i>(if known)</i> |   |  |
| /DGC/                 |                       | 5,623,600            |   | JI, ET AL.                                      | 04/22/97   |
| /DGC/                 |                       | 6,069,628            |   | FARRY, ET AL.                                   | 05/30/00   |
| /DGC/                 |                       | 6,073,241            |   | ROSENBERG, ET AL.                               | 06/06/00   |
| /DGC/                 |                       | 6,092,194            |   | TOUBOUL   | 07/18/00   |
| /DGC/                 |                       | 6,154,844            |   | TOUBOUL   | 11/28/00   |
| /DGC/                 |                       | 6,167,520            |   | TOUBOUL   | 12/26/00   |
| /DGC/                 |                       | 6,310,630            |   | KULKARNI, ET AL.                                | 10/30/01   |
| /DGC/                 |                       | 6,397,264            |   | STASNICK, ET AL.                                | 05/28/02   |
| /DGC/                 |                       | 6,460,060            |   | MADDALOZZO, JR., ET AL.                         | 10/01/02   |
| /DGC/                 |                       | 6,480,962            |   | TOUBOUL   | 11/12/02   |
| /DGC/                 |                       | 6,535,931            |   | CELI, JR.                                       | 03/18/03   |
| /DGC/                 |                       | 6,611,878            |   | DE ARMAS, ET AL.                                | 08/26/03   |
| /DGC/                 |                       | 6,633,835            |   | MORAN ET AL.                                    | 10/14/03   |
| /DGC/                 |                       | 6,667,751            |   | WYNN, ET AL.                                    | 12/23/03   |
| /DGC/                 |                       | 6,701,441            |   | BALASUBRAMANIAM, ET AL.                         | 03/02/04   |
| /DGC/                 |                       | 6,785,732            |   | BATES, ET AL.                                   | 08/31/04   |
| /DGC/                 |                       | 6,804,780            |   | TOUBOUL   | 10/12/04   |
| /DGC/                 |                       | 6,813,711            |   | DIMENSTEIN                                      | 11/02/04   |
| /DGC/                 |                       | 6,829,654            |   | JUNGKE  | 12/07/04   |
| /DGC/                 |                       | 6,965,968            |   | TOUBOUL   | 11/15/05   |
| /DGC/                 |                       | 7,058,822            |   | EDERY ET AL.                                    | 06/06/06   |
| /DGC/                 |                       | US 2003/0217287      | A1  | KRUGLENKO                                       | 11/20/03   |
| /DGC/                 |                       | US 2004/0030914      | A1  | KELLEY, ET AL.                                  | 02/12/04   |
| /DGC/                 |                       | US 2004/0034794      | A1  | MAYER ET AL.                                    | 02/19/04   |
| /DGC/                 |                       | US 2004/0064736      | A1  | OBRECHT, MARK ERIC, ET AL.                      | 04/01/04   |
| /DGC/                 |                       | US 2004/0080529      | A1  | WOJCIK, PAUL KAZIMIERZ                          | 04/29/04   |
| /DGC/                 |                       | US 2004/0143763      | A1  | RADATTI   | 07/22/04   |
| /DGC/                 |                       | US 2004/0187023      | A1  | ALAGNA, MICHAEL ANTHONY, ET AL.                 | 09/23/04   |
| /DGC/                 |                       | US 2004/0225877      | A1  | HUANG   | 11/11/04   |
| /DGC/                 |                       | US 2005/0138433      | A1  | LINETSKY, GENE                                  | 06/23/05   |

|                    |                         |                 |            |
|--------------------|-------------------------|-----------------|------------|
| Examiner Signature | /David Garcia Cervetti/ | Date Considered | 09/12/2008 |
|--------------------|-------------------------|-----------------|------------|

\*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

<sup>1</sup> Unique citation designation number.  
<sup>2</sup> See attached Kinds of U.S. Patent Documents.



|  |                  |                          |                   |
|--|------------------|--------------------------|-------------------|
| Substitute for form 1449A/PTO<br><br><b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b><br><br>(use as many sheets as necessary) |                  | <i>Complete if Known</i> |                   |
|  |                  | Application Number       | 11/104,202        |
|  |                  | Filing Date              | 04/12/05          |
|  |                  | First Named Inventor     | Michael Burtscher |
|  |                  | Group Art Unit           | 2161              |
| Examiner Name  | Not Yet Assigned | Attorney Docket No.      | WEBR-011/00US     |
| Sheet  | 2 of 2           |                          |                   |

| FOREIGN PATENT DOCUMENTS |                       |                         |                     |                                   |   |  |                |
|--------------------------|-----------------------|-------------------------|---------------------|-----------------------------------|---|--|----------------|
| Examiner Initials*       | Cite No. <sup>1</sup> | Foreign Patent Document |                     |                                   | Name of Patentee or Applicant of Cited Document | Date of Publication of Cited Document MM-DD-YYYY | T <sup>4</sup> |
|                          |                       | Office <sup>1</sup>     | Number <sup>2</sup> | Kind Code <sup>3</sup> (if known) |   |  |                |
|                          |                       |                         |                     |                                   |   |  |                |
|                          |                       |                         |                     |                                   |   |  |                |
|                          |                       |                         |                     |                                   |   |  |                |
|                          |                       |                         |                     |                                   |   |  |                |
|                          |                       |                         |                     |                                   |   |  |                |

| OTHER – NON PATENT LITERATURE DOCUMENTS |                       |  |                |
|---|-----------------------|--|----------------|
| Examiner Initials*                      | Cite No. <sup>1</sup> | Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.            | T <sup>2</sup> |
| /DGC/                                   | I.                    | Codeguru, Three Ways to Inject Your Code Into Another Process, by Robert Kuster, August 4, 2003, 22 pgs.   |                |
| /DGC/                                   | II.                   | Codeguru, Managing Low-Level Keyboard Hooks With The Windows API for VB .Net, by Paul Kimmel, April 18, 2004, 10 pgs.  |                |
| /DGC/                                   | III.                  | Codeguru, Hooking The Keyboard, by Anoop Thomas, December 13, 2001, 6 pgs.   |                |
| /DGC/                                   | IV.                   | Illusive Security, Wolves In Sheep's Clothing: malicious DLLs Injected Into trusted Host Applications, Author Unknown, <a href="http://home.arcor.de/scheinsicherheit/dll.htm">http://home.arcor.de/scheinsicherheit/dll.htm</a> 13 pgs. Accessed 8/30/2006, dated 8/10/03 |                |
| /DGC/                                   | V.                    | DevX.com, Intercepting Systems API Calls, by Seung-Woo Kim, May 13, 2004, 6 pgs.   |                |
| /DGC/                                   | VI.                   | Microsoft.com, How To Subclass A Window in Windows 95, Article ID 125680, July 11, 2005, 2 pgs.  |                |
| /DGC/                                   | VII.                  | MSDN, by Kyle Marsh, July 29, 1993, 15 pgs.  |                |
| /DGC/                                   | VII.                  | PCT Search Report, PCT/US05/34874, 07/05/06, 7 Pages   |                |

|                    |                         |                 |            |
|--------------------|-------------------------|-----------------|------------|
| Examiner Signature | /David Garcia Cervetti/ | Date Considered | 09/12/2008 |
|--------------------|-------------------------|-----------------|------------|

\*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

<sup>1</sup> Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3).  
<sup>2</sup> For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document.  
<sup>3</sup> Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible.  
<sup>4</sup> Applicant is to place a check mark here if English language Translation is attached.

<sup>1</sup> Unique citation designation number.  
<sup>2</sup> Applicant is to place a check mark here if English language Translation attached.

|   |                  |                          |                           |
|---|------------------|--------------------------|---------------------------|
| Substitute for form 1449A/PTO<br><br><b>INFORMATION DISCLOSURE<br/>STATEMENT BY APPLICANT</b><br><br><i>(use as many sheets as necessary)</i> |                  | <i>Complete if Known</i> |                           |
|   |                  | Application Number       | 11/104,202                |
|   |                  | Filing Date              | 04/12/2005                |
|   |                  | First Named Inventor     | Michael BURTSCHER         |
|   |                  | Group Art Unit           | 2161                      |
| Examiner Name   | Not Yet Assigned |                          |                           |
| Sheet   | 1 of 1           | Attorney Docket Number   | WEBR-011/00US 303666-2011 |

| U.S. PATENT DOCUMENTS |                       |   |                                |  |  |
|-----------------------|-----------------------|---|--------------------------------|--|--|
| Examiner Initials*    | Cite No. <sup>1</sup> | Document Number                             | Publication Date<br>MM-DD-YYYY | Name of Patentee or Applicant of<br>Cited Document | Pages, Columns, Lines, Where Relevant<br>Passages or Relevant Figures Appear |
|                       |                       | Number-Kind Code <sup>2</sup> (if<br>known) |                                |  |  |
| /DGC/                 |                       | US-2006/0074896 A1                          | 04/06/2006                     | Thomas   |  |
| /DGC/                 |                       | US-2006/0075501 A1                          | 04/06/2006                     | Thomas   |  |
| /DGC/                 |                       | US-2006/0085528 A1                          | 04/20/2006                     | Thomas   |  |
| /DGC/                 |                       | US-2006/0288416 A1                          | 12/21/2006                     | Costea   |  |
| /DGC/                 |                       | US-5,715,455 A                              | 02/03/1998                     | Macon  |  |
| /DGC/                 |                       | US-6,173,291                                | 01/09/2001                     | Jenevein   |  |
| /DGC/                 |                       | US-7,346,611                                | 10/12/2006                     | Burtscher  |  |
| /DGC/                 |                       | US-6,667,751                                | 12/23/2003                     | Wynn   |  |

|                    |                         |                 |            |
|--------------------|-------------------------|-----------------|------------|
| Examiner Signature | /David Garcia Cervetti/ | Date Considered | 09/15/2008 |
|--------------------|-------------------------|-----------------|------------|

\*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. <sup>1</sup>Unique citation designation number (optional). <sup>2</sup>See attached Kinds of U.S. Patent Documents. <sup>3</sup>Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). <sup>4</sup>For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. <sup>5</sup>Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. <sup>6</sup>Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

*If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.*

Please type a plus sign (+) inside this box → +

PTO/SB/08A (07-05)  
Approved for use through 07/31/2006. OMB 0651-0031

|   |        |                          |                           |
|---|--------|--------------------------|---------------------------|
| Substitute for form 1449A/PTO<br><br><b>INFORMATION DISCLOSURE<br/>STATEMENT BY APPLICANT</b><br><br><i>(use as many sheets as necessary)</i> |        | <i>Complete if Known</i> |                           |
|   |        | Application Number       | 11/104,202                |
|   |        | Filing Date              | 04/12/2005                |
|   |        | First Named Inventor     | Michael BURTSCHER         |
|   |        | Group Art Unit           | 2161                      |
|   |        | Examiner Name            | Not Yet Assigned          |
| Sheet   | 1 of 1 | Attorney Docket Number   | WEBR-011/00US 303666-2011 |

| U.S. PATENT DOCUMENTS |                       |  |                                |   |   |
|-----------------------|-----------------------|--|--------------------------------|---|---|
| Examiner Initials*    | Cite No. <sup>1</sup> | Document Number                          | Publication Date<br>MM-DD-YYYY | Name of Patentee or Applicant of Cited Document | Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear |
|                       |                       | Number-Kind Code <sup>2</sup> (if known) |                                |   |   |
| /DGC/                 |                       | US-2005/0120242 A1                       | 06-02-2005                     | Mayer   |   |

|                    |                         |                 |            |
|--------------------|-------------------------|-----------------|------------|
| Examiner Signature | /David Garcia Cervetti/ | Date Considered | 09/12/2008 |
|--------------------|-------------------------|-----------------|------------|

\*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. <sup>1</sup>Unique citation designation number (optional). <sup>2</sup>See attached Kinds of U.S. Patent Documents. This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

*If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.*

**TERMINAL DISCLAIMER TO OBTAIN A DOUBLE PATENTING  
REJECTION OVER A "PRIOR" PATENT**

Docket Number (Optional)

WEBR-011/00US 303666-2011

In re Application of: Michael BURTSCHER et al.

Application No.: 11/104,202

Filed: 04/12/2005

For: System and Method for Directly Accessing Data From a Data Source Medium

The owner\*, Webroot Software, Inc., of 100 percent interest in the instant application hereby disclaims, except as provided below, the terminal part of the statutory term of any patent granted on the instant application which would extend beyond the expiration date of the full statutory term **prior patent** No. 7,346,611 as the term of said prior patent is defined in 35 U.S.C. 154 and 173, and as the term of said **prior patent** is presently shortened by any terminal disclaimer. The owner hereby agrees that any patent so granted on the instant application shall be enforceable only for and during such period that it and the **prior patent** are commonly owned. This agreement runs with any patent granted on the instant application and is binding upon the grantee, its successors or assigns.

In making the above disclaimer, the owner does not disclaim the terminal part of the term of any patent granted on the instant application that would extend to the expiration date of the full statutory term as defined in 35 U.S.C. 154 and 173 of the **prior patent**, "as the term of said **prior patent** is presently shortened by any terminal disclaimer," in the event that said **prior patent** later:

- expires for failure to pay a maintenance fee;
- is held unenforceable;
- is found invalid by a court of competent jurisdiction;
- is statutorily disclaimed in whole or terminally disclaimed under 37 CFR 1.321;
- has all claims canceled by a reexamination certificate;
- is reissued; or
- is in any manner terminated prior to the expiration of its full statutory term as presently shortened by any terminal disclaimer.

Check either box 1 or 2 below, if appropriate.

1.  For submissions on behalf of a business/organization (e.g., corporation, partnership, university, government agency, etc.), the undersigned is empowered to act on behalf of the business/organization.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

2.  The undersigned is an attorney or agent of record. Reg. No. 44051

Thomas M. Croft  
Signature

12/03/2008

Date

Thomas M. Croft  
Typed or printed name

7205664044

Telephone Number

- Terminal disclaimer fee under 37 CFR 1.20(d) included.

**WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.**

\*Statement under 37 CFR 3.73(b) is required if terminal disclaimer is signed by the assignee (owner).  
Form PTO/SB/96 may be used for making this certification. See MPEP § 324.

This collection of information is required by 37 CFR 1.321. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.



## Electronic Patent Application Fee Transmittal

|   |  |
|---|--|
| <b>Application Number:</b>                  | 11104202   |
| <b>Filing Date:</b>                         | 12-Apr-2005  |
| <b>Title of Invention:</b>                  | System and method for directly accessing data from a data storage medium |
| <b>First Named Inventor/Applicant Name:</b> | Michael Burtscher  |
| <b>Filer:</b>                               | Thomas M. Croft/Sherry Bitler  |
| <b>Attorney Docket Number:</b>              | WEBR-011/00US 303666-2011  |

Filed as Large Entity

### Utility under 35 USC 111(a) Filing Fees

| Description                              | Fee Code | Quantity | Amount | Sub-Total in USD(\$) |
|--|----------|----------|--------|----------------------|
| <b>Basic Filing:</b>                     |          |          |        |                      |
| <b>Pages:</b>                            |          |          |        |                      |
| <b>Claims:</b>                           |          |          |        |                      |
| <b>Miscellaneous-Filing:</b>             |          |          |        |                      |
| <b>Petition:</b>                         |          |          |        |                      |
| <b>Patent-Appeals-and-Interference:</b>  |          |          |        |                      |
| <b>Post-Allowance-and-Post-Issuance:</b> |          |          |        |                      |
| <b>Extension-of-Time:</b>                |          |          |        |                      |

| Description              | Fee Code | Quantity | Amount | Sub-Total in USD(\$) |
|--------------------------|----------|----------|--------|----------------------|
| <b>Miscellaneous:</b>    |          |          |        |                      |
| Statutory disclaimer     | 1814     | 1        | 140    | 140                  |
| <b>Total in USD (\$)</b> |          |          |        | <b>140</b>           |

## Electronic Acknowledgement Receipt

|   |  |
|---|--|
| <b>EFS ID:</b>                              | 4392085  |
| <b>Application Number:</b>                  | 11104202   |
| <b>International Application Number:</b>    |  |
| <b>Confirmation Number:</b>                 | 1284   |
| <b>Title of Invention:</b>                  | System and method for directly accessing data from a data storage medium |
| <b>First Named Inventor/Applicant Name:</b> | Michael Burtscher  |
| <b>Customer Number:</b>                     | 22903  |
| <b>Filer:</b>                               | Thomas M. Croft/Sherry Bitler  |
| <b>Filer Authorized By:</b>                 | Thomas M. Croft  |
| <b>Attorney Docket Number:</b>              | WEBR-011/00US 303666-2011  |
| <b>Receipt Date:</b>                        | 03-DEC-2008  |
| <b>Filing Date:</b>                         | 12-APR-2005  |
| <b>Time Stamp:</b>                          | 19:49:11   |
| <b>Application Type:</b>                    | Utility under 35 USC 111(a)  |

### Payment information:

|  |                 |
|--|-----------------|
| Submitted with Payment                   | yes             |
| Payment Type                             | Deposit Account |
| Payment was successfully received in RAM | \$140           |
| RAM confirmation Number                  | 5417            |
| Deposit Account                          | 501283          |
| Authorized User                          |                 |

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)

**File Listing:**

| Document Number                     | Document Description                               | File Name          | File Size(Bytes)/<br>Message Digest                 | Multi Part /.zip | Pages (if appl.) |
|-------------------------------------|--|--------------------|---|------------------|------------------|
| 1                                   | Amendment Copy Claims/Response to Suggested Claims | WEBR01100USroa.pdf | 8041667<br>916358f816b3d878c25e18c3335e91494ec1d0f8 | no               | 175              |
| <b>Warnings:</b>                    |  |                    |   |                  |                  |
| <b>Information:</b>                 |  |                    |   |                  |                  |
| 2                                   | Terminal Disclaimer Filed                          | WEBR01100UStd.pdf  | 75994<br>6750c4cfdab4cb999d4377c7167a159410fb54ac   | no               | 1                |
| <b>Warnings:</b>                    |  |                    |   |                  |                  |
| <b>Information:</b>                 |  |                    |   |                  |                  |
| 3                                   | Fee Worksheet (PTO-06)                             | fee-info.pdf       | 29791<br>a36cd8ff3346ee2e819bfe4f54aaac5c3b05d41d   | no               | 2                |
| <b>Warnings:</b>                    |  |                    |   |                  |                  |
| <b>Information:</b>                 |  |                    |   |                  |                  |
| <b>Total Files Size (in bytes):</b> |  |                    | 8147452   |                  |                  |

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

**New Applications Under 35 U.S.C. 111**

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

**National Stage of an International Application under 35 U.S.C. 371**

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

**New International Application Filed with the USPTO as a Receiving Office**

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

In Re Application of: Michael BURTSCHER Confirmation No.: 1284  
et al.

Serial No.: 11/104,202 Group Art Unit: 2136

Filed: 04/12/05 Examiner: David Garcia CERVETTI

FOR: **SYSTEM AND METHOD FOR DIRECTLY ACCESSING DATA FROM A DATA STORAGE  
MEDIUM**

---

**Mail Stop Amendment**

Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

**AMENDMENT/RESPONSE TO OFFICE ACTION**

In response to the Official Action dated September 17, 2008 (the "Office Action"), please amend the above-identified patent application in the following manner:

**Amendments to the Specification** begin on page 2 of this paper.

**Amendments to the Claims** are reflected on the listing of the claims which begins on page 3 of this paper.

**Remarks/Arguments** begin on page 8 of this paper.

**Amendments to the Specification:**

*Please replace paragraph no. [0001] with the following paragraph. The amendments to paragraph no. [0001] are indicated by strikethrough and underlining.*

[0001] The present application is related to the following commonly owned and assigned applications: application no. ~~(unassigned)~~10/956,578, Attorney Docket No. ~~WEBR-002/00US~~, entitled *System and Method for Monitoring Network Communications for Pestware*; application no. ~~(unassigned)~~10/956,573, Attorney Docket No. ~~WEBR-003/00US~~, entitled *System and Method For Heuristic Analysis to Identify Pestware*[[,]]; and application no. ~~(unassigned)~~10/956,574, Attorney Docket No. ~~WEBR-005/00US~~, entitled *System and Method for Pestware Detection and Removal*[[,]]; and application no. ~~(unassigned)~~, Attorney Docket No. ~~WEBR-011/00US~~, filed herewith, entitled *System and Method for Directly Accessing Data From a Data Storage Medium* each of which is incorporated by reference in their entirety.

**Amendments to the Claims:**

*Set forth below in ascending order, with status identifiers, is a complete listing of all claims currently under examination. Changes to any amended claims are indicated by strikethrough and underlining. This listing also reflects any cancellation and/or addition of claims.*

1. (currently amended) A method for scanning files on a protected computer for pestware, the method comprising:

identifying a location of each of at least a first file, a second file, and a third file ~~[[in]]~~on a file storage device of the protected computer;

sorting a listing of the first, second, and third files in accordance with their respective physical locations on the storage device to generate a sorted list;

retrieving, while ~~substantially~~ circumventing an operating system of the protected computer, information from the first, second, and third files by directly and sequentially accessing the first, second, and third files in the order the first, second, and third files are listed in the sorted list; and

analyzing the information from the first, second, and third files to determine whether or not each of the first, second, and third files is a potential pestware file; and

reporting results of the analyzing to a user.

2. (currently amended) The method of claim 1, wherein the identifying includes identifying the location of each of at least the first file, the second file, and the third file while ~~substantially~~ circumventing the operating system.

3. (currently amended) The method of claim 2, wherein the identifying includes:  
accessing a master file table of the file storage device[[,]] while ~~substantially~~  
circumventing the operating system; and  
identifying the location of each of at least the first file, the second file, and the third file  
by analyzing the data of the master file table.

4. (currently amended) The method of claim, 1 wherein the identifying includes  
utilizing the operating system to identify the first file, the second file, and the third file.

5. (currently amended) The method of claim 1, wherein the identifying includes  
identifying a cluster number of each of the [[a ]]first file, [[a]]the second file, and [[a]]the third  
file [[in]]on a disk drive of the protected computer.

6. (canceled)

7. (currently amended) A method for scanning files on a protected computer for  
pestware, the method comprising:

identifying, while ~~substantially~~ circumventing an operating system of the protected  
computer, a location of each of a plurality of files [[in]]on a file storage device of the protected  
computer;

sorting, by location on the file storage device, a listing of the plurality of files to generate  
a sorted list;



retrieving information from each of the plurality of files by directly and sequentially accessing each of the plurality of files in the order the plurality of files are listed in the sorted list;[[ and]]

analyzing the information from each of the plurality of files ~~so as to~~ determine whether any of the plurality of files are potential pestware files; and reporting results of the analyzing to a user.

8. (currently amended) The method of claim 7, wherein the identifying includes: accessing a master file table of the file storage device[[,]] while ~~substantially~~ circumventing the operating system; and identifying the location of each of the plurality of files by analyzing the data of the master file table.

9. (currently amended) The method of claim 7, wherein the retrieving includes utilizing the operating system to retrieve information from each of the plurality of files.

10. (currently amended) The method of claim 7, wherein the identifying includes identifying a cluster number of each of the plurality of files [[in]]on a disk drive of the protected computer.

11. (canceled)

12. (currently amended) A system for managing pestware, the system comprising:

a processor; and

a memory including a plurality of program instructions, the plurality of program instructions including:

a pestware detection module configured to cause the processor to detect pestware on a file storage device of a protected computer, ~~the protected computer including at least one file storage device and a program memory;~~ and

a sweep speedup module configured to cause the processor to:

identify, while ~~substantially circumventing~~ an operating system of the protected computer, a location of each of a plurality of files ~~[[in]]~~ on the at least one file storage device of the protected computer;

sort, by location on the file storage device, a listing of the plurality of files to generate a sorted list; and

retrieve information from each of the plurality of files by directly and sequentially accessing each of the plurality of files in the order the plurality of files are listed in the sorted list;

wherein the pestware detection module is configured to analyze the information from each of the plurality of files ~~so as to~~ determine whether any of the plurality of files are potential pestware files and to report results of the analysis to a user.

13. (currently amended) The system of claim 12, wherein the sweep speedup module is configured to cause the processor to:

access, while ~~substantially circumventing~~ the operating system, a master file table of the file storage device; and

identify the location of each of the plurality of files by analyzing the data of the master file table.

14. (currently amended) The system of claim 12, wherein the sweep speedup module is configured to cause the processor to utilize the operating system to retrieve information from each of the plurality of files.

15. (currently amended) The system of claim 12, wherein the sweep speedup module is configured to cause the processor to identify a cluster number of each of the plurality of files [[in]]on a disk drive of the protected computer.

16. (canceled)

17. (currently amended) The system of claim 12, wherein the protected computer includes a plurality of file storage devices, and wherein the plurality of files are distributed among the plurality of file storage devices.

## **REMARKS**

Claims 1-5, 7-10, 12-15, and 17 have been currently amended. Claims 6, 11, and 16 have been canceled. Claims 1-5, 7-10, 12-15, and 17 thus remain pending in the application.

### **Requirement for Information**

The Office Action requests additional information from Applicant to permit the Examiner “to properly consider patentability of the claimed invention under 35 U.S.C. 102(b).” Specifically, the Office Action requests information “such as user manual and technical specifications” for “Spy Sweeper and other Webroot corporation products.”

In response to this request, Applicant has submitted herewith, as Appendix A, a declaration of Michael Burtscher, one of the joint inventors on the instant application. Attached to Mr. Burtscher’s declaration are eight supporting exhibits, including, among other things, user documentation for two Webroot products, Webroot Spy Sweeper and Webroot Enterprise.

### **Objections to the Specification**

The Office Action objects to the specification because the identifying numbers of related applications cited on the first page of the application need to be updated.

Applicant has amended Para. 0001 of the specification to update the serial numbers as requested. An erroneous circular citation to the instant application (the citation to “WEBR-011/00US”) has also been deleted. Withdrawal of the objection to the specification is respectfully requested.

### **Provisional Double Patenting Rejection**

The Office Action provisionally rejects claims 1-17 under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1-19 of U.S. Patent No. 7,346,611 (hereinafter the “611 Patent”).

Without conceding that the Office Action is correct in its assertion that claims 1-19 of the '611 patent "anticipate the claims of the instant application," Applicant has filed herewith a terminal disclaimer to overcome the obviousness-type double patenting rejection. Withdrawal of this rejection is respectfully requested.

### **Claim Rejections Under 35 U.S.C. § 112**

The Office Action rejects claims 1-3, 7-8, and 12-13 under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter that Applicant regards as the invention. Specifically, the Office Action asserts that the term "substantially" in the claims is a relative term that renders them indefinite.

Applicant has currently amended the claims to remove the term "substantially" throughout. The current amendments have not introduced any new matter, and withdrawal of the rejections of the above-listed claims under § 112, second paragraph, is respectfully requested.

### **Claim Rejections Under 35 U.S.C. § 101**

The Office Action rejects claims 1-17 under 35 U.S.C. § 101 as being directed to non-statutory subject matter. Specifically, the Office Action asserts that the method of claims 1-11 fail to produce a "useful, concrete, and tangible result" and that the system of claims 12-17 are directed to "a system or apparatus comprising only software since the modules are software, and as such are non-statutory."

Applicant has amended independent method claim 1 to recite "reporting results of the analyzing to a user." Reporting the results of a pestware scan of a computer storage device to a user is undoubtedly a "useful, concrete, and tangible result." The current amendment to claim 1 adding the "reporting" action does not introduce any new matter into the application, and support for the amendment may be found at, e.g., Para. 0005 of the specification.

Applicant disagrees that independent claim 12 is directed to “a system or apparatus comprising only software” for at least the reason that “only software” cannot possibly accomplish the recited actions in the context of “[a] system for managing pestware.” That is, program instructions (software) *per se* could not possibly scan a storage device of a computer for the presence of pestware. Nevertheless, in the interest of advancing prosecution, Applicant has amended claim 12 to recite “a processor” and “a memory containing a plurality of program instructions . . . .” Claim 12 thus unquestionably falls within the statutory category of “machine” under § 101. No new matter has been introduced by way of the current amendments to claim 12, and ample support for these amendments may be found at, e.g., Paras. 0016 and 0018 and in FIGURE 1 of the application.

In light of the current amendments to independent claims 1 and 12, withdrawal of the rejections, under § 101, of claims 1-17 is respectfully requested.

### **Claim Rejections Under 35 U.S.C. § 102**

The Office Action rejects claims 1-17 under 35 U.S.C. § 102(e) as being anticipated by Costea et al. (U.S. Patent Publ. 2006/0101282, hereinafter “Costea”). Applicant believes the current amendments to independent claims 1, 7, and 12 overcome these rejections for at least the reasons explained below.

**Claim 1.** Currently amended independent claim 1 recites, among other things, the limitations “sorting a listing of the first, second, and third files in accordance with their respective physical locations on the storage device to generate a sorted list” and “. . . directly and sequentially accessing the first, second, and third files in the order the first, second, and third files are listed in the sorted list.” At least these limitations are neither taught nor suggested in Costea.

The Office Action asserts, on p. 7 in connection with now-canceled claims 6, 11, and 16, that Costea teaches the generation of the recited “sorted list” at Paras. 0038 and 0042-0043. This is incorrect. The cited paragraphs in Costea, though they do mention a Master File Table (MFT) and the file attributes stored therein, really concern a method for keeping track of the state of files (“known malware,” “known good,” or “unknown”) with respect to an anti-virus application (see Para. 0038). Costea says nothing whatsoever about sorting a listing of files “in accordance with [the files’] respective physical locations on the storage device” and “. . . directly and sequentially accessing the . . . files in the order the . . . files are listed in the sorted list.”

Because Costea fails to teach each and every limitation recited in currently amended claim 1, Costea does not anticipate currently amended claim 1, and Applicant believes currently amended claim 1 to be allowable. Each of claims 2-5 is thus also allowable at least by virtue of its depending from allowable claim 1. Withdrawal of the rejection, under § 102(e), of claims 1-5 is respectfully requested.

*Claim 7.* Currently amended independent claim 7 recites limitations similar to those discussed above in connection with claim 1. Therefore, arguments similar to those above in connection with claim 1 also apply to claim 7.

Additionally, claim 7, among other things, recites the limitation “identifying, while circumventing an operating system of the protected computer, a location of each of a plurality of files on a file storage device of the protected computer.” Costea does not teach identifying file locations “while circumventing an operating system of the protected computer,” as recited in claim 7.

Because Costea fails to teach each and every limitation recited in currently amended claim 7, Costea does not anticipate currently amended claim 7, and Applicant believes currently

amended claim 7 to be allowable. Each of claims 8-10 is thus also allowable at least by virtue of its depending from allowable claim 7. Withdrawal of the rejection, under § 102(e), of claims 7-10 is respectfully requested.

**Claim 12.** Currently amended independent claim 12 recites limitations similar to those discussed above in connection with claim 1 but in the context of a system for managing pestware. Therefore, arguments similar to those above in connection with claim 1 also apply to claim 12.

Because Costea fails to teach each and every limitation recited in currently amended claim 12, Costea does not anticipate currently amended claim 12, and Applicant believes currently amended claim 12 to be allowable. Each of claims 13-15 and 17 is thus also allowable at least by virtue of its depending from allowable claim 12. Withdrawal of the rejection, under § 102(e), of claims 12-15 and 17 is respectfully requested.

## **CONCLUSION**

In view of the foregoing, Applicant respectfully submits that no further impediments exist to the allowance of this application and, therefore, requests an indication of allowability. However, the Examiner is requested to call the undersigned if any questions or comments arise.

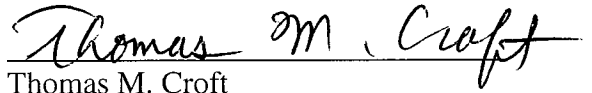
The Director is hereby authorized to charge any appropriate fees under 37 C.F.R. §§1.16, 1.17, and 1.21 that may be required by this paper, and to credit any overpayment, to Deposit Account No. 50-1283.



COOLEY GODWARD KRONISH LLP  
ATTN: Patent Group  
777 6<sup>th</sup> Street NW, Suite 1100  
Washington, DC 20001

Tel: (720) 566-4044  
Fax: (202) 842-7899

Respectfully submitted,  
COOLEY GODWARD KRONISH LLP

By:   
Thomas M. Croft  
Reg. No. 44,051

**Appendix A: Declaration of Michael Burtscher**

**Attorney Docket No. WEBR-011/00US 303666-2011**

**PATENT**

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

In Re Application of: Michael BURTSCHER Confirmation No.: 1284  
et al.

Serial No.: 11/104,202 Group Art Unit: 2136

Filed: 04/12/05 Examiner: David Garcia CERVETTI

FOR: **SYSTEM AND METHOD FOR DIRECTLY ACCESSING DATA FROM A DATA STORAGE MEDIUM**

---

**DECLARATION OF MICHAEL BURTSCHER**

1. I, Michael Burtscher, am one of the joint inventors of the invention described and claimed in U.S. Patent Application No. 11/104,202, entitled "System and Method for Directly Accessing Data from a Data Storage Medium," which was filed on April 12, 2005 (hereinafter the "'202 Application").

2. I am currently employed by Webroot Software, Inc. ("Webroot"), the assignee of the entire interest in the '202 application, in Boulder, Colorado. As a Principal Software Architect, my responsibilities include architecting, prototyping and implementing software systems, as well as reviewing other software engineers' designs and identifying and improving performance bottlenecks in Webroot's software applications.

3. Two Webroot commercial products include the features described and claimed in the '202 Application: (1) Webroot Spy Sweeper and (2) Webroot Enterprise.

4. The earliest version of Webroot Spy Sweeper to include the features described and claimed in the '202 Application was Version 3.5 (hereinafter "Spy Sweeper 3.5"). The earliest

version of Webroot Enterprise to include the features described and claimed in the '202 Application was Version 2.0 (hereinafter "Enterprise 2.0").

5. On information and belief, Spy Sweeper 3.5 was first made available for public beta testing in the U.S. on or about December 2, 2004.
6. On information and belief, Spy Sweeper 3.5 was first offered for sale to customers in the U.S. on or about December 6, 2004.
7. On information and belief, Enterprise 2.0 was first made available for public beta testing in the U.S. on or about November 24, 2004.
8. On information and belief, Enterprise 2.0 was first offered for sale to customers in the U.S. on or about December 19, 2004.
9. The following documents are attached hereto in support of the above statements and in response to the Examiner's Requirement for Information in the Office Action mailed on September 17, 2008: (1) a *User Guide* for Spy Sweeper 3.5 (Exhibit 1); (2) a *System Administrator Guide* for Enterprise 2.0 and an associated "Quick Start Guide" and "Release Notes" (Exhibit 2); (3) side-by-side screenshots comparing directory listings for Versions 3.2 and 3.5 of Webroot Spy Sweeper (Exhibit 3); (4) side-by-side screenshots comparing directory listings for Versions 1.5 and 2.0 of Webroot Enterprise (Exhibit 4); (5) a printout of a Webroot Intranet page maintained by Webroot Quality Assurance showing program version and build numbers with corresponding release dates for various versions of Webroot Spy Sweeper (Exhibit 5); (6) an e-mail message from the Director of Enterprise Product Management Brian Kellner dated December 19, 2004, regarding the commercial release of the Enterprise 2.0 product

(Exhibit 6); (7) an e-mail message from Product Manager Sarah Mood dated December 2, 2004, regarding the external beta release of Spy Sweeper 3.5 (Exhibit 7); and (8) an e-mail message from Brian Kellner dated November 24, 2004, regarding the beta release of the Enterprise 2.0 product (Exhibit 8).

10. “Faster sweeps” on p. 2 of Exhibit 1 (*User Guide* for Spy Sweeper 3.5) refers to the speed up of malware scans provided by the invention described and claimed in the ’202 Application. The statement “Full system sweeps are approximately 20% faster” on p. 1 of the “Release Notes” for Enterprise 2.0 (following the *System Administrator Guide* and “Quick Start Guide” in Exhibit 2) also refers to the speed up of malware scans provided by the invention described and claimed in the ’202 Application.

11. The side-by-side screenshots in Exhibit 3 from Webroot’s source control server show that the folder “FastFileScan” is present for Spy Sweeper 3.5 (top left, build 186) but not for the preceding Version 3.2 (bottom left, build 150). This “FastFileScan” folder relates to the features described and claimed in the ’202 Application. Version 3.2 did not include the features described and claimed in the ’202 Application.

12. The side-by-side screenshots in Exhibit 4 from Webroot’s source control server show that the folder “FastFileScan” is present for Enterprise 2.0 (top left) but not for the preceding Version 1.5 (bottom left). This “FastFileScan” folder relates to the features described and claimed in the ’202 Application. Version 1.5 did not include the features described and claimed in the ’202 Application.

13. Exhibit 5 lists program version and build numbers with corresponding release dates for Webroot Spy Sweeper. The earliest commercial release date listed for Spy Sweeper 3.5 (Build 186) is December 6, 2004.
14. On information and belief based on the e-mail message in Exhibit 6 sent by Brian Kellner, Director of the Enterprise Product Management, to other Webroot employees, Enterprise 2.0 was first commercially released on or about December 19, 2004.
15. On information and belief based on the e-mail message in Exhibit 7 sent by Product Manager Sarah Mood to other Webroot employees, Spy Sweeper 3.5 was first made available for external beta testing on or about December 2, 2004.
16. On information and belief based on the e-mail message in Exhibit 8 sent by Director of Enterprise Product Management Brian Kellner to other Webroot Employees, Enterprise 2.0 was first made available for external beta testing on or about November 24, 2004.
17. I hereby declare that all statements made herein are based either on my own personal knowledge or on information that I obtained from available Webroot records or, where necessary, from other Webroot personnel with personal knowledge; that all statements made herein are true; that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine, imprisonment, or both under Section 1001 of Title 18 of the United States Code; and that such willful false statements may jeopardize the validity of the '592 application or any patent issued thereon.

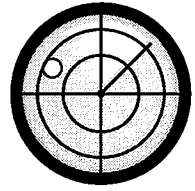
Executed on:

12/3/2008

By:

  
Michael Burtscher

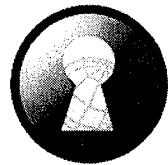
**Exhibit 1: *User Guide* for Webroot Spy Sweeper Version 3.5**



webroot®

# Spy Sweeper™

## User Guide



webroot®

SOFTWARE, INC.

Webroot Software, Inc.  
PO Box 19816  
Boulder, CO 80308  
[www.webroot.com](http://www.webroot.com)



Webroot Spy Sweeper 3.5 User Guide

Copyright © 2003–2004 Webroot Software, Inc.

Webroot is a registered trademark of and Spy Sweeper is a trademark of Webroot Software, Inc.

Other product and company names may be trademarks of their respective owners.

# Contents

---

|   |           |
|---|-----------|
| <b>1: Getting Started</b>                         | <b>1</b>  |
| About This Guide                                  | 1         |
| Conventions                                       | 1         |
| Technical Support                                 | 1         |
| New in Webroot Spy Sweeper 3.5                    | 2         |
| Understanding Spyware and Other Online Threats    | 2         |
| Installing Webroot Spy Sweeper                    | 2         |
| Updating Webroot Spy Sweeper                      | 12        |
| Updating Webroot Spy Sweeper Definitions          | 13        |
| Starting Webroot Spy Sweeper                      | 14        |
| Understanding the Webroot Spy Sweeper Window      | 14        |
| Understanding the Error about User Accounts       | 15        |
| Closing Webroot Spy Sweeper                       | 16        |
| <b>2: Running Sweeps</b>                          | <b>17</b> |
| Setting Sweep Options                             | 17        |
| Protecting Settings with a Password               | 19        |
| Running a Sweep                                   | 20        |
| Viewing Sweep Results                             | 23        |
| Handling Quarantined Items                        | 24        |
| Deleting Items Permanently                        | 24        |
| Restoring Items                                   | 25        |
| <b>3: Customizing Webroot Spy Sweeper</b>         | <b>27</b> |
| Setting Webroot Spy Sweeper Program Options       | 27        |
| Scheduling Sweeps                                 | 28        |
| Setting Up Continuous Monitoring (Active Shields) | 29        |
| Setting Up the Internet Explorer Shields          | 30        |
| Setting Up the Windows System Shields             | 32        |
| Setting Up the Hosts File Shields                 | 32        |
| Working with the Common Ad Sites Shield           | 34        |
| Setting Up the Startup Programs Shield            | 35        |
| Handling Alerts                                   | 36        |
| Setting Up Items to Always Keep                   | 38        |
| Setting Up Items to Always Remove                 | 39        |
| Reporting Spyware                                 | 40        |
| Viewing Spy News                                  | 40        |
| Glossary  | 47        |
| <b>Index</b>                                      | <b>51</b> |



# 1: Getting Started

---

Webroot Spy Sweeper™ lets you protect your privacy and your computer from a variety of spyware and unwanted programs, from those that monitor all of your computer's activities (system monitors), to those that can steal or destroy data (Trojan horses). It also detects programs that pop up advertising on your computer (adware) and cookies that may contain personal information (tracking cookies).

Spy Sweeper "sweeps" your computer looking for evidence of threats, reports its findings, and lets you decide whether to quarantine and remove the item or keep it. The quarantine-and-remove function disables the item until you decide to delete it completely or restore it.




## About This Guide

---

This *Guide* describes how to set up and use Spy Sweeper to protect your privacy and your computer from spyware, adware, and other unwanted programs. It assumes that you have a basic understanding of how to use the Windows operating system.

## Conventions

This *Guide* uses several typographical conventions to help explain how to use Spy Sweeper.

| Convention   | Definition  |
|--|---|
| <b>Bold</b>  | Words in <b>bold</b> show items to select or click, such as menu items or buttons.  |
|  <b>Note</b>    | This symbol means the following information is a note that gives you important information that may affect how you use Spy Sweeper.                       |
|  <b>Caution</b> | This symbol means the following information is a caution that warns you about actions that may affect your ability to use some programs on your computer. |
|                 | This symbol means that the following information is a procedure.  |

## Technical Support

---

Technical support is available from the Webroot Web site. Submit a trouble ticket to our service representatives:

[www.webroot.com/support](http://www.webroot.com/support)

We make every effort to respond to your request on the same day you send it in, but please allow up to 48 hours.

## New in Spy Sweeper 3.5

---

Spy Sweeper 3.5 has the following new features and functions:

- Faster sweeps.
- Sweep cookies option to let you decide whether to include cookies in sweeps. For more information, see “Setting Sweep Options” on page 17.
- Additional options to protect default pages that Internet Explorer displays from being hijacked. For more information, see “Setting Up the Internet Explorer Shields” on page 30.

## Understanding Spyware and Other Online Threats

---

Online threats come in many forms. Typically, spyware, adware, and other unwanted programs get installed on your computer without your knowledge or consent. They may be part of a program that you installed or they may install themselves as you visit various Web sites. The following information is not meant to be a complete discussion of all online threats. We hope that it will acquaint you with some of the threats that Spy Sweeper can address for you.

Spyware is any application that makes surreptitious changes to your computer while collecting information about your computer activities. This information is then sent to a third party for malicious purposes, without your knowledge or consent.

Spyware arrives bundled with freeware or shareware, through e-mail or instant messages, as an ActiveX installation, or by someone with access to your computer. Once on your drive, spyware secretly installs itself and goes to work. Unlike traditional personalization or session cookies, spyware is difficult to detect, and difficult (if not impossible) for the average user to remove.

You can set up Spy Sweeper to detect and remove unwanted items. However, in some cases, the program that installed the spyware, adware, or unwanted program may not work without the unwanted program installed. You should test your programs before deleting items permanently.

## Installing Spy Sweeper

---

Depending on how you purchased Spy Sweeper, you may be installing it from a CD or from a file you download from the Webroot® Web site.



### Note

To access Spy Sweeper using Windows 2000 or XP, you must have Administrator privileges for the user account that you use to log in to your computer. If you do not have Administrator privileges, you will not be able to start Spy Sweeper.

You must have a valid key code to install Spy Sweeper, unless you are installing the trial version. The key code is a unique number that identifies the rights and privileges associated with this individual program's installation, such as free updates and support. The key code is associated *only* with Spy Sweeper and does *not* include any information related to your computer or its configuration. Webroot does not use the key code in any way to track individual use of its products. Your key code comes in an e-mail message.

**Note**

If you are upgrading from a previous version of Spy Sweeper, do *not* uninstall the old version first. Installing the new version over the old one retains the quarantine information from previous sweeps and automatically retains your Spy Sweeper settings.

You can install Spy Sweeper one of two ways:

- Typical—Use this option to quickly install Spy Sweeper using the configuration settings that Webroot recommends. (See page 3.)
- Custom—Use this option to select various configuration settings yourself. (See page 7.)

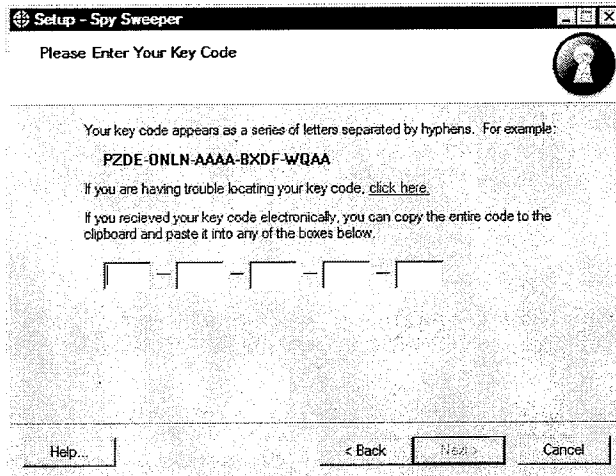


To do a Typical Spy Sweeper installation:

1. Close all other programs that you have open on your computer.
2. Start the installation program.

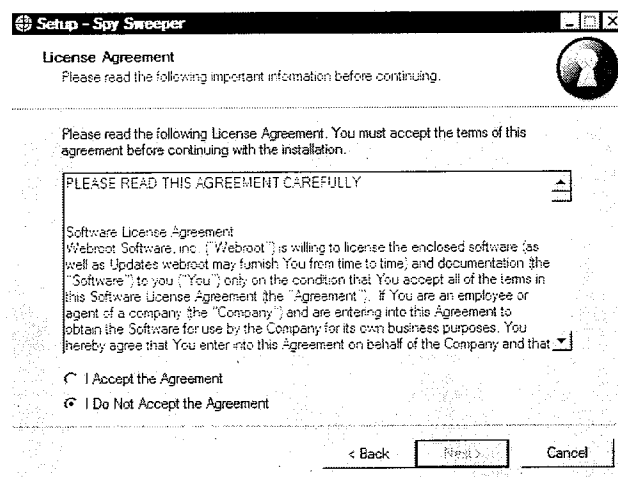
| To install from a CD   | To install from a downloaded file   |
|--|---|
| <ol style="list-style-type: none"> <li>1. Insert the CD into your CD drive.               <ul style="list-style-type: none"> <li>• The installation options should display automatically. If they do not, use Windows Explorer to navigate to your CD drive. Then double-click install.exe to start the installation.</li> </ul> </li> <li>2. Click <b>Install Spy Sweeper</b> to start the installation.               <ul style="list-style-type: none"> <li>• The Welcome to the Spy Sweeper Setup Wizard window displays.</li> </ul> </li> </ol> | <ol style="list-style-type: none"> <li>1. Follow the instructions on the Web site to download the file.</li> <li>2. Using Windows Explorer, navigate to where you downloaded the file.               <ul style="list-style-type: none"> <li>• If you downloaded the file to your Windows Desktop, close all open programs and you will see an icon on your desktop for the file you downloaded.</li> <li>• If you downloaded the file to a different location, use Windows Explorer to navigate to the file.</li> </ul> </li> <li>3. Double-click the file you downloaded to start the installation.               <ul style="list-style-type: none"> <li>• The Welcome to the Spy Sweeper Setup Wizard window displays.</li> </ul> </li> </ol> |

3. Click **Next** to install Spy Sweeper.
  - The Please Enter Your Key Code window displays.

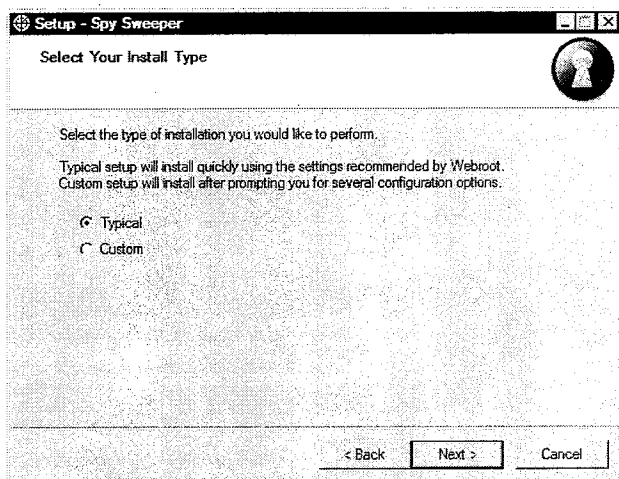


4. Enter your key code and click **Next**.

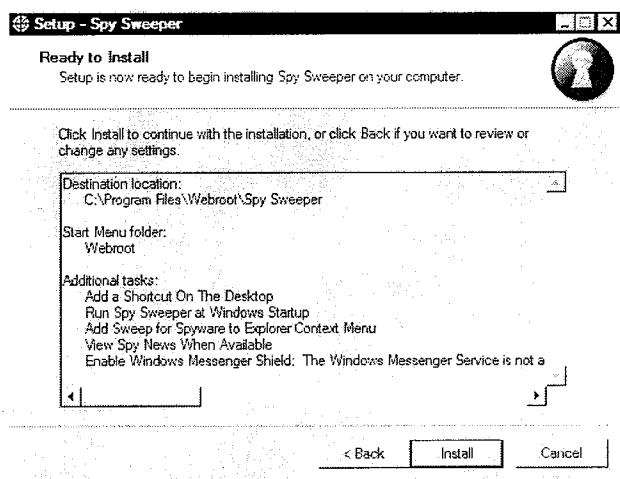
- You received your key code in an e-mail message. You can copy the whole key code from the message and paste it into any field in the window. The key code will automatically fill in all the fields.
- The key code contains only letters, no numbers. You can enter the letters in lower or upper case; the key code is not case sensitive.
- The **Next** button stays unavailable (dimmed) until you enter a valid key code. If the button does not become available, check the accuracy of the key code you entered.
- If you are installing the trial version, the Activate software window displays. Enter your e-mail address to hear about new versions and special offers and click **Send** or click **Skip**. If you have previously installed the trial version, you cannot install it again.
- The License Agreement window displays.



5. Read the license agreement, select the I Accept the Agreement option if you agree with the content, and click **Next**.
  - The Select Your Install Type window displays.



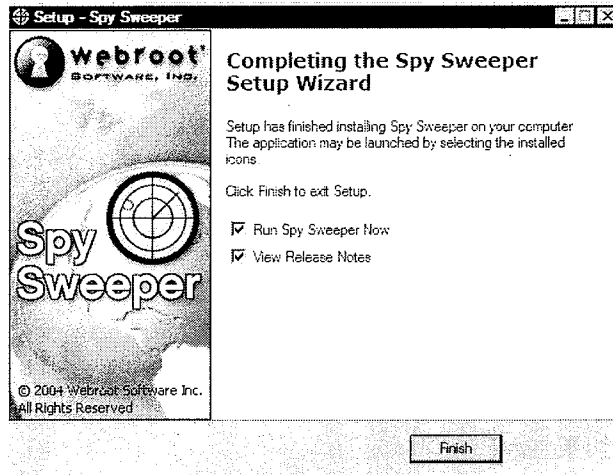
6. Select Typical and click **Next**.
  - The Ready to Install window displays, showing the installation location and recommended options.





7. Click **Install**.

- The installation may ask you to restart your computer. If it does, Spy Sweeper will start when you restart Windows.
- The Completing the Spy Sweeper Setup Wizard window displays.



8. Select the options you want and click **Finish**.

| Option              | Description   |
|---------------------|---|
| Run Spy Sweeper Now | This starts Spy Sweeper when you finish the installation, so you can review the default settings and run a sweep.   |
| View Release Notes  | This option opens the Release Notes (readme.txt) file in Notepad. This lets you review the most current information about this release. Close the file when you are finished. |

- If you have Internet access, the Spy Sweeper Product Registration Page displays in your browser. Enter your registration information to ensure that you receive free updates and technical support for one year.
- If you selected the option to run Spy Sweeper now, the Spy Sweeper splash screen displays, followed by the Check for Updated Definitions panel. We recommend that you update your definitions now.

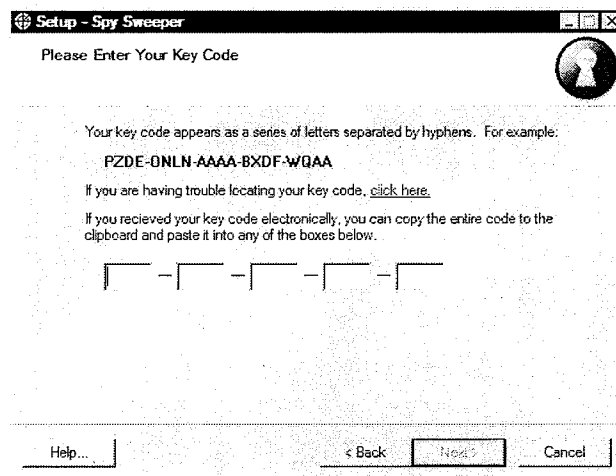


To do a Custom Spy Sweeper installation:

1. Close all other programs that you have open on your computer.
2. Start the installation program.

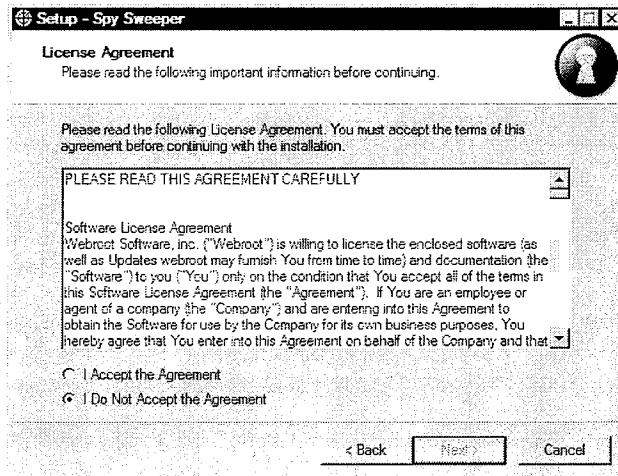
| To install from a CD  | To install from a downloaded file  |
|---|--|
| <ol style="list-style-type: none"><li>1. Insert the CD into your CD drive.<ul style="list-style-type: none"><li>• The installation options should display automatically. If they do not, use Windows Explorer to navigate to your CD drive. Then double-click install.exe to start the installation.</li></ul></li><li>2. Click <b>Install Spy Sweeper</b> to start the installation.<ul style="list-style-type: none"><li>• The Welcome to the Spy Sweeper Setup Wizard window displays.</li></ul></li></ol> | <ol style="list-style-type: none"><li>1. Follow the instructions on the Web site to download the file.</li><li>2. Using Windows Explorer, navigate to where you downloaded the file.<ul style="list-style-type: none"><li>• If you downloaded the file to your Windows Desktop, close all open programs and you will see an icon on your desktop for the file you downloaded.</li><li>• If you downloaded the file to a different location, use Windows Explorer to navigate to the file.</li></ul></li><li>3. Double-click the file you downloaded to start the installation.<ul style="list-style-type: none"><li>• The Welcome to the Spy Sweeper Setup Wizard window displays.</li></ul></li></ol> |

3. Click **Next** to install Spy Sweeper.
  - The Please Enter Your Key Code window displays.



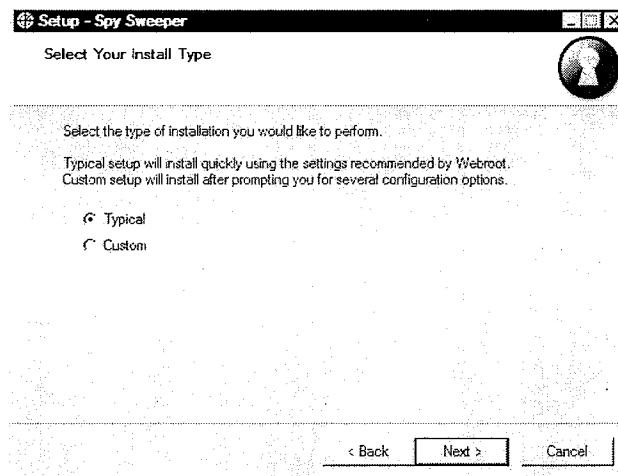
4. Enter your key code and click **Next**.
  - You received your key code in an e-mail message. You can copy the whole key code from the message and paste it into any field in the window. The key code will automatically fill in all the fields.
  - The key code contains only letters, no numbers. You can enter the letters in lower or upper case; the key code is not case sensitive.
  - The **Next** button stays unavailable (dimmed) until you enter a valid key code. If the button does not become available, check the accuracy of the key code you entered.

- If you are installing the trial version, the Activate software window displays. Enter your e-mail address to hear about new versions and special offers and click **Send** or click **Skip**. If you have previously installed the trial version, you cannot install it again.
- The License Agreement window displays.



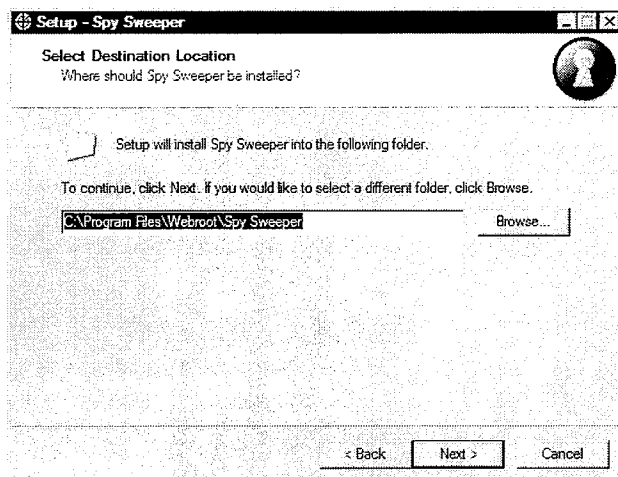
5. Read the license agreement, select the I Accept the Agreement option if you agree with the content, and click **Next**.

- The Select Your Install Type window displays.



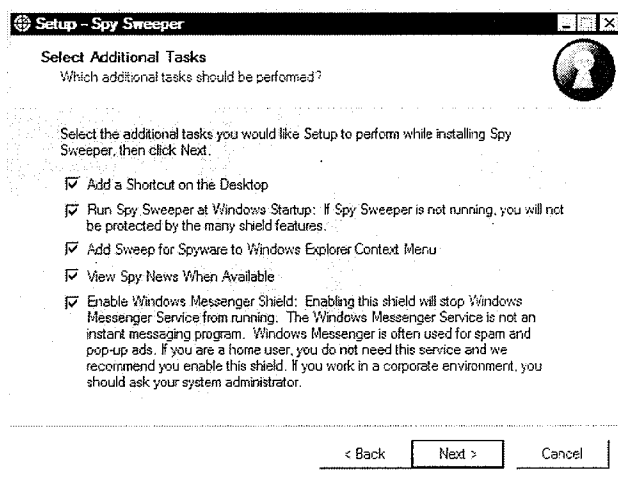
6. Select Custom and click **Next**.

- The Select a Destination Location window displays.



7. Select where you want to install Spy Sweeper and click **Next**.

- For most users, we recommend letting Spy Sweeper install to the default location that displays. To install to another location, click **Browse**.
- The Select Additional Tasks window displays.

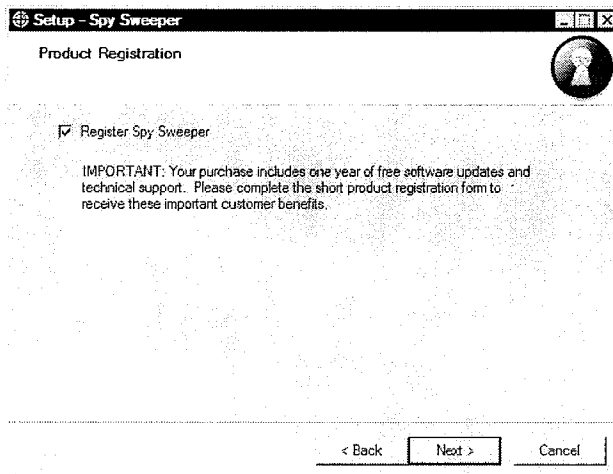


8. Select or deselect the options you want and click **Next**.

| Option  | Description   |
|---|---|
| Add a Shortcut on the Desktop                     | This option adds a Spy Sweeper shortcut to your desktop. You can then double-click the shortcut icon to start Spy Sweeper.                            |
| Run Spy Sweeper at Windows Startup                | This option starts Spy Sweeper automatically when you start Windows and Spy Sweeper stays open in your system tray. We recommend using this option.   |
| Add Sweep Option to Windows Explorer Context Menu | This option adds a menu option to sweep a folder for spyware, adware, and other unwanted programs from Windows Explorer by right-clicking the folder. |

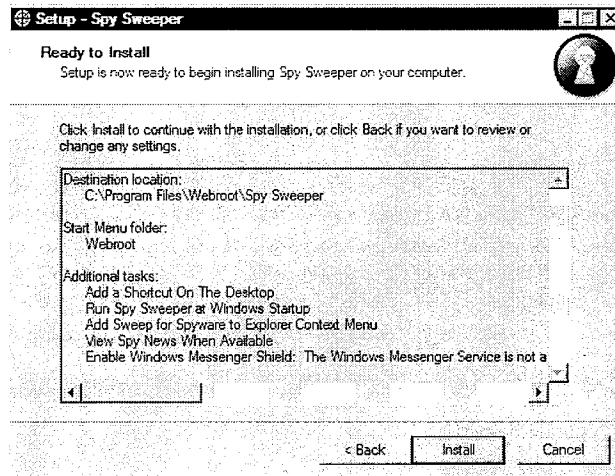
| Option                          | Description  |
|---------------------------------|--|
| View Spy News When Available    | This option has Spy Sweeper check for new Spy News each time it checks for program updates.  |
| Enable Windows Messenger Shield | <p>(Applies only to Windows NT, 2000, and XP.) This option turns off and actively watches the Microsoft Messenger Service in Windows. This service is not an instant messaging program and does not affect your use of instant messaging. This service is often used for sending spam (unwanted e-mail) and creating pop-up advertisements. Turning off the service stops these types of spam and pop-ups.</p> <p>If your computer is in your home, you can turn off this service without any problem.</p> <p>If you work in a corporate environment, contact your system administrator to find out if your company uses the service to communicate with company employees. If you are not sure, leave the service turned on until you find out.</p> |

- The Product Registration window displays.



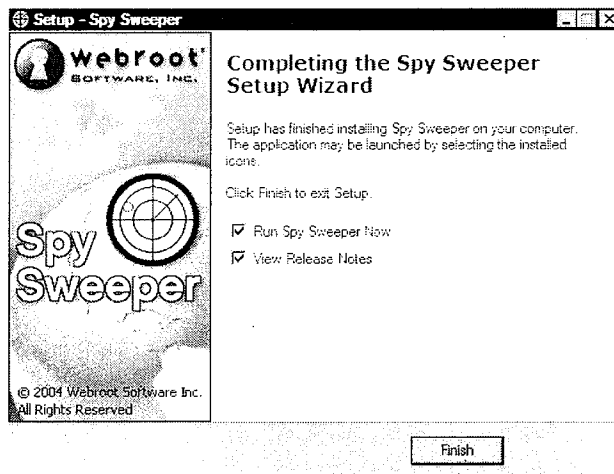
9. Select the registration option to ensure that you receive free updates and technical support for one year and click **Next**.

- The Ready to Install window displays, showing the installation location and your selected options.
- If you need to make changes, click **Back** until you return to the window you want to change.



10. Click **Install**.

- The installation may ask you to restart your computer. If it does, Spy Sweeper will start when you restart Windows.
- The Completing the Spy Sweeper Setup Wizard window displays.



11. Select the options you want and click **Finish**.

| Option              | Description   |
|---------------------|---|
| Run Spy Sweeper Now | This starts Spy Sweeper when you finish the installation, so you can review the default settings and run a sweep.   |
| View Release Notes  | This option opens the Release Notes (readme.txt) file in Notepad. This lets you review the most current information about this release. Close the file when you are finished. |

- If you selected the registration option, your browser opens and takes you to the registration page.
- If you selected the option to run Spy Sweeper now, the Spy Sweeper splash screen displays, followed by the Check for Updated Definitions panel. We recommend that you update your definitions now.

## Updating Spy Sweeper

Webroot updates the Spy Sweeper program to keep up with changes in threats. You should update the program at least once a month to ensure that you are using the latest version.



### Note

If you are upgrading from a previous version of Spy Sweeper, do *not* uninstall the old version first. Installing the new version over the old one retains the quarantine information from previous sweeps and lets you automatically retain your Spy Sweeper settings.

Spy Sweeper can notify you whenever a new version is available. You can also check for updates anytime. While your subscription is valid, you can download and install the updated version.

To see what version you have, click **About** in the icon panel.



### Note

You must connect to the Internet to update Spy Sweeper.



To update Spy Sweeper:

1. Start Spy Sweeper, if it is not already open, and display the main window.
  - For more information, see “Starting Webroot Spy Sweeper” on page 14.
2. In the icon panel, click **Options**.
  - For information about the Spy Sweeper window, see “Understanding the Webroot Spy Sweeper Window” on page 14.
  - The Options panel displays.
3. Click the **Program Options** tab.
  - The Program Options tab displays.
4. Click **Update Program**.

- If you want Spy Sweeper to automatically notify you of updates, select the Automatic Check for Updates option.
  - Spy Sweeper opens your Internet browser and takes you to the Webroot Web site.
5. See if the Web site says that an updated version is available.
  6. Follow the instructions on the Web site to download the file that contains the updated version.
    - Be sure you remember where you download the file on your computer.
  7. Follow the installation instructions in “Installing Webroot Spy Sweeper” on page 2.

## Updating Spy Sweeper Definitions

Webroot is constantly updating the software definitions that Spy Sweeper uses to detect spyware, adware, and other unwanted programs. You should update the definitions at least once a week to ensure that you are using the latest definitions.

Spy Sweeper can notify you whenever new definitions are available. You can also check for updated definitions anytime. While your subscription is valid, you can download and install the updated definitions.



### Note

You must connect to the Internet to update Spy Sweeper definitions.

---



To update the Spy Sweeper definitions:

1. Start Spy Sweeper, if it is not already open, and display the main window.
  - For more information, see “Starting Webroot Spy Sweeper” on page 14.
2. In the icon panel, click **Options**.
  - For information about the Spy Sweeper window, see “Understanding the Webroot Spy Sweeper Window” on page 14.
  - The Options panel displays.
3. Click the **Program Options** tab.
  - The Program Options tab displays.
4. Click **Update Definitions**.
  - If new definitions are available, Spy Sweeper downloads and installs them from the Webroot Web site. The Download Progress bar and Information box show the status of the download.
  - If no new definitions are available, the Information box tells you that your definitions are up to date.
  - If you want Spy Sweeper to automatically notify you of updates, select the Automatic Check for Updates option.






# Starting Spy Sweeper

---

You can start Spy Sweeper and display the main window a number of ways, depending on the options you selected when you installed it.



Start Spy Sweeper and display the main window using one of the following methods:

- If Spy Sweeper is open in your system tray (you should see the Spy Sweeper icon  in the lower-right corner of your screen), do one of the following to display the Spy Sweeper main window:
  - Double-click the Spy Sweeper icon.
  - Right-click the Spy Sweeper icon and select **Restore** from the pop-up menu.
    - The Spy Sweeper main window displays. This is where you can change your Spy Sweeper settings and run sweeps. For more information, see “Understanding the Webroot Spy Sweeper Window” on page 14, “Chapter 2, Running Sweeps” on page 17, and “Chapter 3, Customizing Webroot Spy Sweeper” on page 27.
    - Click **Minimize**  to close the Spy Sweeper window, but keep Spy Sweeper open in your system tray and monitoring your computer.
- If you did not select the Run Spy Sweeper Now option during installation or you closed Spy Sweeper completely, click **Start**, point to **Programs**, point to **Webroot**, point to **Spy Sweeper**, click **Spy Sweeper** or double-click the Spy Sweeper icon  on your computer desktop.
  - This starts Spy Sweeper and displays the main window. If you see an error message and the window does not display, see “Understanding the Error about User Accounts” on page 15.
  - If you are using the trial version, a reminder window displays letting you know how many days are left in your trial. To continue using the trial version, click **Continue Trial**. To buy Spy Sweeper, click **Buy It Now**. If your trial period has expired, click **Buy It Now** to buy Spy Sweeper. You must be connected to the Internet for the **Buy It Now** button to work.



## Note

If you want Spy Sweeper to start automatically when you start Windows and run in your system tray, click **Options** in the icon panel, click the **Program Options** tab, and select the Load at Windows Startup option. We recommend using this option.

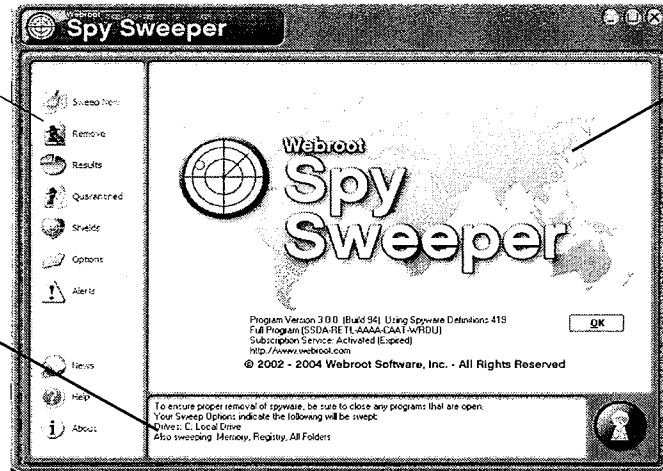
---

## Understanding the Spy Sweeper Window

The Spy Sweeper window lets you change your sweep settings, create customized settings, and run a sweep. Figure 1 shows the main window and describes its parts.

Icon panel—Click an icon to see the available settings and actions.

Information box—Displays information about the currently displayed panel or tab.



Main panel—Displays the options available for the selected icon. This panel is where you change the Spy Sweeper settings and run a sweep.

Figure 1: Spy Sweeper main window

Figure 2 shows the settings available when you click the **Options** icon, then click the **Sweep Options** tab. Some icons display tabs, as shown here, that give you access to additional options.

Click a tab to see more options.

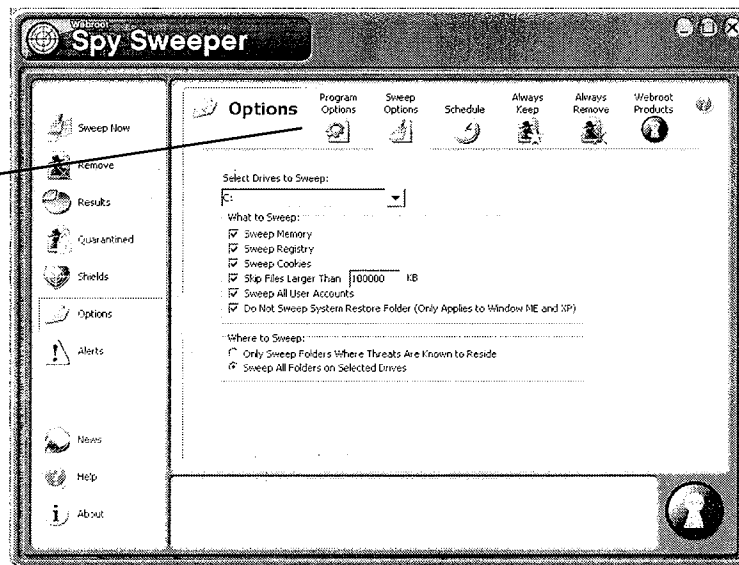
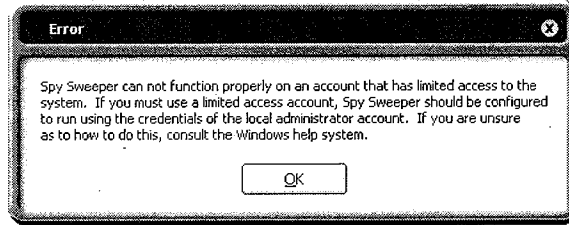


Figure 2: Spy Sweeper Options (Sweep Options tab)

## Understanding the Error about User Accounts




To access Spy Sweeper using Windows 2000 or XP, you must have Administrator privileges for the user account that you use to log in to your computer. If you do not have Administrator privileges, you will not be able to start Spy Sweeper.

If your user account does not have Administrator privileges, you will see the following error when you try to start Spy Sweeper.



To resolve the problem, contact your system administrator to see if your user account can have Administrator privileges.



## Closing Spy Sweeper

When you are viewing the Spy Sweeper window, as shown in “Understanding the Webroot Spy Sweeper Window” on page 14, you can click **Minimize**  when you are finished setting up Spy Sweeper. Clicking **Minimize**  closes the window, but keeps the Spy Sweeper program open. If you have set up any scheduled sweeps or have set Spy Sweeper shields (continuous monitoring), you should keep it open. You know it is open if you see the icon  in the system tray in the lower-right corner of your screen.

If you want to completely stop Spy Sweeper, you can close it. You need to completely close Spy Sweeper before you install a new version of Spy Sweeper.



To close Spy Sweeper completely:

1. Do one of the following:
  - Right-click the Spy Sweeper icon  in your system tray and select **Close** from the pop-up menu. The system tray is in the lower-right corner of your screen.
  - If the Spy Sweeper window is open, click **Close** .
    - If you have any shields turned on or any sweeps scheduled, Spy Sweeper warns you that your computer will not be protected if you shut down Spy Sweeper.
2. Click **Shut Down** to close Spy Sweeper.
  - To start Spy Sweeper, so that your shields and scheduled sweeps will run, see “Starting Webroot Spy Sweeper” on page 14.

# 2: Running Sweeps

---

Spy Sweeper lets you do the following related to running sweeps:

- Set sweep options (see page 17)
- Run sweeps (see page 20)
- View sweep results (see page 23)
- Handle quarantined items (see page 24)

## Setting Sweep Options

---

You can set a variety of options that control how Spy Sweeper sweeps your computer looking for threats. You should review the options before running a sweep to ensure that you are thoroughly protecting your computer from spyware, adware, and other unwanted programs.

You can also protect your options by setting up a password. For more information, see “Protecting Settings with a Password” on page 19.



To set sweep options:

1. Start Spy Sweeper, if it is not already open, and display the main window.
  - For more information, see “Starting Webroot Spy Sweeper” on page 14.
2. In the icon panel, click **Options**.
  - For information about the Spy Sweeper window, see “Understanding the Webroot Spy Sweeper Window” on page 14.
  - The Options panel displays.
3. Click the **Sweep Options** tab.
  - The Sweep Options tab displays.

4. Select the options you want to use for your next sweep.

| Option                             | Description  |
|------------------------------------|--|
| Select Drives to Sweep             | <p>Select the drives you want Spy Sweeper to sweep and click <b>Apply</b>. The drop-down list includes all local drives (hard drives and CD or DVD drives installed on your computer) and any mapped network drives.</p> <p>Typically, most spyware, adware, and unwanted programs install on the C: drive, but you should sweep all hard drives periodically.</p>   |
| What to Sweep                      |  |
| Sweep Memory                       | <p>Select this option to have Spy Sweeper sweep your computer's random access memory (RAM) for threats. Typically, you want to sweep memory each time you run a sweep. Spyware, adware, and unwanted programs commonly load into memory.</p>   |
| Sweep Registry                     | <p>Select this option to have Spy Sweeper sweep your computer's registry for threats. Typically, you want to sweep the registry each time you run a sweep. Spyware, adware, and unwanted programs commonly create entries in your computer's registry.</p>   |
| Sweep Cookies                      | <p>Select this option to have Spy Sweeper include all cookies in each sweep. This option will find all cookies and list them in the Removed panel after a sweep. You can then decide if there are cookies you want to keep. You may want to keep cookies that contain user names and passwords that let you log in to a Web site automatically or preferences you set for Web site.</p> <p>You may want to remove tracking cookies. Some Web sites now issue tracking cookies, which allow multiple Web sites to store and access cookies that may contain personal information (including surfing habits, user names and passwords, and areas of interest), then share the information they contain with other Web sites.</p> |
| Skip Files Larger Than             | <p>If you know that you have very large files that you do not want Spy Sweeper to sweep, select this option and enter a file size in kilobytes (KB). For example, you may want to use this option if you have large graphics or video files on your computer that you created and you know do not contain threats. This will save time during sweeps. Typically, spyware, adware, and unwanted program files are small.</p>  |
| Sweep All User Accounts            | <p>Select this option to have Spy Sweeper sweep all registry entries, even those related to another user or login ID on your computer. Spyware, adware, and unwanted programs commonly create entries in your registry. Using this option makes sure all registry entries are swept.</p>   |
| Do Not Sweep System Restore Folder | <p>(Applies only to Windows ME and XP.) Select this option to have Spy Sweeper skip the folder where Windows stores System Restore files. If a restore point contains a threat, Spy Sweeper will continuously report it found. However, Windows does not let Spy Sweeper quarantine or remove threats from a restore point. If the threat is installed on your computer, Spy Sweeper will find it and quarantine it.</p>   |
| Where to Sweep                     |  |

| Option   | Description  |
|--|--|
| Only Sweep Folders Where Threats Are Known to Reside | Select this option to make the sweep run faster. When you use this option, Spy Sweeper only looks in the folders where spyware, adware, and unwanted program files are typically found. Using this option performs a less thorough sweep. You should periodically sweep all folders. |
| Sweep All Folders on Selected Drives                 | Select this option to have Spy Sweeper look in all folders on the drives you select to sweep. This type of sweep will take longer to run. Using this option performs a more thorough sweep.  |

## Protecting Settings with a Password

You can protect your Spy Sweeper settings with a password. After you enable password protection, Spy Sweeper will require the password to access Options, Shields, Alerts, and quarantined items and to shut down Spy Sweeper.

Spy Sweeper “remembers” your password as long as you are actively using the program. After five minutes of inactivity or after you minimize the program, it will ask for the password again.

Be sure you remember or write down your password.



To protect settings with a password:

1. Start Spy Sweeper, if it is not already open, and display the main window.
  - For more information, see “Starting Webroot Spy Sweeper” on page 14.
2. In the icon panel, click **Options**.
  - For information about the Spy Sweeper window, see “Understanding the Webroot Spy Sweeper Window” on page 14.
  - The Options panel displays.
3. Click the **Program Options** tab.
  - The Program Options tab displays.
4. Select the Enable Password Protection option.
  - The Enable Password Protection window displays.
5. Enter the password you want to use in both text boxes.
  - Consider making the password difficult to guess by combining letters and numbers.
6. Click **OK**.

# Running a Sweep

You can run a sweep on your computer at any time. Running a sweep means that Spy Sweeper looks for threats installed on your computer and removes them. Initially, it quarantines the item, making it inoperable, but permitting you to restore it if you find you need it to continue using another program. The Quarantine folder is under the folder where you installed Spy Sweeper. You can view quarantined items from within Spy Sweeper.

Once you find that you do not need the item, you can delete it permanently. For more information, see “Deleting Items Permanently” on page 24.

You can sweep entire disk drives from Spy Sweeper or sweep a single folder from Windows Explorer. To run a sweep from Windows Explorer, you must enable the option for this feature. For more information, see “Setting Webroot Spy Sweeper Program Options” on page 27.

You can also set up Spy Sweeper to run sweeps automatically. For more information, see “Scheduling Sweeps” on page 28.



To run a sweep:

1. Close all programs that are open.
  - Spy Sweeper may not be able to remove threats associated with a particular program if that program is open. For best results, close all programs that are listed in the taskbar at bottom of your screen. You do not need to close programs shown in the system tray in the lower-right corner of your screen. These programs are only open in the background.

| To sweep one or more disk drives  | To sweep a specific folder   |
|---|--|
| <ol style="list-style-type: none"> <li>1. Start Spy Sweeper, if it is not already open, and display the main window.               <ul style="list-style-type: none"> <li>• For more information, see “Starting Webroot Spy Sweeper” on page 14.</li> </ul> </li> <li>2. In the icon panel, click <b>Sweep Now</b>.               <ul style="list-style-type: none"> <li>• For information about the Spy Sweeper window, see “Understanding the Webroot Spy Sweeper Window” on page 14.</li> <li>• The Step 1 Sweep System panel displays.</li> </ul> </li> <li>3. Click <b>Start</b>.</li> </ol> | <ol style="list-style-type: none"> <li>1. Start Spy Sweeper if it is not already open.               <ul style="list-style-type: none"> <li>• You do not need to display the Spy Sweeper window. It just needs to be open in the system tray. For more information, see “Starting Webroot Spy Sweeper” on page 14.</li> </ul> </li> <li>2. From Windows Explorer, right-click the folder you want to sweep.</li> <li>3. From the pop-up menu, select <b>Run a Sweep</b>.               <ul style="list-style-type: none"> <li>• The Step 1 Sweep System panel displays.</li> </ul> </li> </ol> |

- Spy Sweeper runs the sweep based on the options you selected. For more information about setting options, see “Setting Sweep Options” on page 17.
- The lower-left part of the panel shows what Spy Sweeper is currently scanning. After you run the sweep the first time, Spy Sweeper displays an estimate of how long the sweep will take.
- To pause the sweep, click **Pause**. An Information window displays, letting you know that the sweep is paused. When you want to resume the sweep where it left off, click **OK**.

- To stop the sweep, click **Stop**.
- The following fields display in the panel.

| Field                       | Description  |
|-----------------------------|--|
| Spyware Fingerprints Loaded | Displays the number of fingerprints that Spy Sweeper is looking for. Multiple fingerprints make up the definition of a spy. You should update your Spy Sweeper definitions regularly to ensure that you are using the most current version. For more information, see "Updating Webroot Spy Sweeper Definitions" on page 13. |
| Memory Items Inspected      | Displays the number of pieces of programs that Spy Sweeper swept in your computer's memory. Some of these pieces may be part of spyware, adware, or unwanted programs.   |
| Registry Items Inspected    | Displays the number of items in the Windows registry that Spy Sweeper swept. Some registry entries may be associated with spyware, adware, or unwanted programs.   |
| Files/Folders Inspected     | Displays the number of files and folders on the selected drives that Spy Sweeper swept.  |
| Items Found                 | Displays the number of spyware, adware, and unwanted programs items that Spy Sweeper found.  |
| Traces Found                | Displays the number of traces of spyware, adware, and unwanted programs that Spy Sweeper found. Traces are places where Spy Sweeper finds spyware fingerprints.  |

2. When the sweep is finished, click **Next**.
  - The Step 2 Remove Spies panel displays, with a list all of the threats found. The following fields display in the panel.

| Field                   | Description   |
|-------------------------|---|
| Items Found             | Displays the number of spyware, adware, or unwanted programs that Spy Sweeper found.  |
| Associated Traces Found | Displays the number of traces of spyware, adware, or unwanted programs that Spy Sweeper found. Traces are places where Spy Sweeper finds spyware fingerprints. Spy Sweeper looks for all known traces of each spyware, adware, or unwanted program.   |
| List of items found     | Displays the list of spyware, adware, or unwanted programs that Spy Sweeper found. Click the plus sign (+) next to an item to see the full path to the traces found. Select the check box next each item or trace to remove and hold the item or individual trace in the Quarantine folder. |
| Name                    | Displays the name of the currently selected item.   |
| Location                | Displays the number of traces found of the currently selected item. If you click the plus sign (+) and select lower level item, this displays the full path to the selected item.   |



| Field            | Description   |
|------------------|---|
| Fingerprint Type | <p>Displays how closely the currently selected fingerprint matched Spy Sweeper's database of fingerprints:</p> <ul style="list-style-type: none"> <li>• <b>Exact Match</b>—The fingerprint matches the database exactly, which means that Spy Sweeper is sure this is spyware, adware, or an unwanted program.</li> <li>• <b>Name Match</b>—Some or all of the name of this fingerprint match, but the fingerprint is not an exact match in all aspects to anything in the database. Spy Sweeper is not sure that this is spyware, adware, or an unwanted program.</li> </ul> |
| Category         | Displays the type of threat of the currently selected item. See the "Glossary" on page 47 for definitions of the types.   |

- To learn more about any item listed, select it and click **View more details online**.



**Note**

You must be connected to the Internet to see the additional information.

- Spy Sweeper opens your Internet browser, goes to the Webroot Web site, and displays information about the selected item. This information can help you decide if you want to remove or keep the item.
- Deselect any item that you want to keep.
    - By default, Spy Sweeper selects all of the listed items, which means Spy Sweeper will remove the item and put it in the Quarantine folder. You can permanently delete items from the Quarantine folder by manually deleting it or by setting an option to automatically delete it. For more information, see "Deleting Items Permanently" on page 24 and "Setting Webroot Spy Sweeper Program Options" on page 27.
    - You can restore items from the Quarantine folder if you find that a program you need will not work properly after removing the associated item. For more information, see "Restoring Items" on page 25.
  - Click **Next** to remove and quarantine all selected items.
    - The remove and quarantine process copies the item traces to the Quarantine folder. Spy Sweeper first encrypts each trace, removes it from its original location (so it will no longer run), then copies it. This process can take several minutes or longer depending on how many traces Spy Sweeper found and on the speed of your computer.
    - The Information box at the bottom of the panel shows the progress of the removal process and tells you when the process is complete.
    - The Step 3 Results panel displays the **Summary** tab with a summary of the sweep and remove processes. For more information about the results, see "Viewing Sweep Results" on page 23.
  - Click **Finish** to return to the Spy Sweeper main window.

# Viewing Sweep Results

---

After you run a sweep, you can view the results at any time. Spy Sweeper keeps the results from the last sweep as well as a log of all recent Spy Sweeper activity.



To view sweep results:

1. Start Spy Sweeper, if it is not already open, and display the main window.
  - For more information, see “Starting Webroot Spy Sweeper” on page 14.
2. In the icon panel, click **Results**.
  - For information about the Spy Sweeper window, see “Understanding the Webroot Spy Sweeper Window” on page 14.
  - The Step 3 Results panel displays the **Summary** tab with the results of the last sweep. The following fields display in the panel.

| Field                             | Description  |
|-----------------------------------|--|
| Memory Items Inspected            | Displays the number of pieces of programs that Spy Sweeper swept in your computer’s memory. Some of these pieces may be part of spyware, adware, or unwanted programs.                             |
| Registry Items Inspected          | Displays the number of items in the Windows registry that Spy Sweeper swept. Some registry entries may be associated with spyware, adware, or unwanted programs.                                   |
| Files/Folders Inspected           | Displays the number of files and folders on the selected drives that Spy Sweeper swept.  |
| Items Found                       | Displays the number of items that Spy Sweeper found.   |
| Traces Found                      | Displays the number of traces that Spy Sweeper found. Traces are places where Spy Sweeper finds fingerprints. Spy Sweeper looks for all known traces of each spyware, adware, or unwanted program. |
| Traces Ignored                    | Displays the number of traces that Spy Sweeper did not remove because they are either on your Keep List or because removing them could impair the operation of your computer.                      |
| Traces Quarantined                | Displays the number of traces that Spy Sweeper quarantined after the last sweep.   |
| Traces Removed Since Installation | Displays the number of traces Spy Sweeper has removed from your computer since you installed Spy Sweeper.  |

3. To see a log of all recent Spy Sweeper activity, click the **Session Log** tab.
  - The session log contains details about sweeps and definition updates.
  - To set how many sessions the log includes, change the Max Number of Session Histories Saved field. The maximum you can save is 20. A session begins when you start Spy Sweeper and ends when you close it completely.

- To save the session log to a file, click **Save to File**.
- To clear the session log, click **Clear Session History**.

## Handling Quarantined Items

---

When you run a sweep and remove spyware, adware, or other unwanted programs, Spy Sweeper does not permanently delete the item. It encrypts the item, copies it to the Quarantine folder, and removes it from its original location. The Quarantine folder is under the folder where you installed Spy Sweeper.

This ensures that the item can no longer run, but you gives you the following options for handing the quarantined items:

- Delete the item permanently (see page 24)
- Restore the item (see page 25)

## Deleting Items Permanently

When you run a sweep and remove spyware, adware, and other unwanted programs, Spy Sweeper does not permanently delete the item. The remove-and-quarantine process copies the item's traces to a Quarantine folder. Spy Sweeper first encrypts each trace, removes it from its original location (so it will no longer run), then copies it to the Quarantine folder.

If you find that a program you need will not work properly after removing the associated item, you can restore the it. For more information, see "Restoring Items" on page 25.

If you find that all of your programs run properly after removing the item, you can permanently delete it. This deletes the spyware, adware, or other unwanted programs from the Quarantine folder, and you will not be able to restore the item. You can also tell Spy Sweeper to automatically delete the item after a specific number of days. For more information, see "Setting Webroot Spy Sweeper Program Options" on page 27.

If you reinstall the program or visit a Web site that has the same threat, it could be installed again. If you find that some items keep showing up in your sweeps, you can tell Spy Sweeper to always remove that item automatically. For more information, see "Setting Up Items to Always Remove" on page 39.



To permanently delete items:

1. Start Spy Sweeper, if it is not already open, and display the main window.
  - For more information, see "Starting Webroot Spy Sweeper" on page 14.
2. In the icon panel, click **Quarantined**.
  - For information about the Spy Sweeper window, see "Understanding the Webroot Spy Sweeper Window" on page 14.
  - The Quarantined panel displays with a list of the items that you have quarantined, but have not permanently deleted.

3. Select each item that you want to permanently delete.
  - A check mark next to the item shows that it is selected and will be deleted.
  - To see the date you removed and quarantined the item and its current location, click the plus sign (+) next to the item name.
4. To learn more about any item listed, select it and click **View more details online**.



**Note**

You must be connected to the Internet to see the additional information.

---

- Spy Sweeper opens your Internet browser, goes to the Webroot Web site, and displays information about the selected item. This information can help you decide if you want to permanently delete the threat.
5. Click **Delete Selected**.
    - Spy Sweeper deletes the selected item and displays information about the deletion in the Information box at the bottom of the window.

## Restoring Items

When you run a sweep and remove spyware, adware, and other unwanted programs, Spy Sweeper does not permanently delete the item. It encrypts the item, copies it to the Quarantine folder, and removes it from its original location. This way, the unwanted program can no longer run, but you can restore it if necessary.

You may need to restore items if you find that a program on your computer is not working correctly after you run a sweep and remove them. Sometimes, the item is an integral part of a program and is required to run the program. If you find this to be the case, you can restore the item.

In some cases, components with copy protection may not restore from quarantine properly. You must reinstall these programs from the original media or installation file.



To restore items:

1. Start Spy Sweeper, if it is not already open, and display the main window.
  - For more information, see “Starting Webroot Spy Sweeper” on page 14.
2. In the icon panel, click **Quarantined**.
  - For information about the Spy Sweeper window, see “Understanding the Webroot Spy Sweeper Window” on page 14.
  - The Quarantined panel displays with a list of the items that you have quarantined, but have not permanently deleted.
3. Select each item that you want to restore.
  - A check mark next to the item shows that it is selected and will be restored.
  - To see the date you removed and quarantined the item and its current location, click the plus sign (+) next to the item name.

4. To learn more about any item listed, select it and click **View more details online**.



**Note**

You must be connected to the Internet to see the additional information.

---

- Spy Sweeper opens your Internet browser, goes to the Webroot Web site, and displays information about the selected item. This information can help you decide if you want to restore the item.
5. Click **Restore Selected**.
    - Spy Sweeper restores the selected item and displays information about the restore status in the Information box at the bottom of the window.

# 3: Customizing Spy Sweeper

---

You can customize Spy Sweeper to meet your needs in several ways:

- Set Spy Sweeper program options (see page 27)
- Schedule sweeps to run automatically (see page 28)
- Set up continuous monitoring of specific threat-related activities (see page 29)
- Set up items to always keep (see page 38)
- Set up items to always remove (see page 39)

In addition you can do the following:

- Report spyware that you find on your computer (see page 40)
- View Spy News (see page 40)

## Setting Spy Sweeper Program Options

---

You can set several options to customize how Spy Sweeper works from the Program Options tab.

You can update the program and spy definitions. For more information, see “Updating Webroot Spy Sweeper” on page 12 and “Updating Webroot Spy Sweeper Definitions” on page 13. You can also report spyware. For more information, see “Reporting Spyware” on page 40.



To set Spy Sweeper program options:

1. Start Spy Sweeper, if it is not already open, and display the main window.
  - For more information, see “Starting Webroot Spy Sweeper” on page 14.
2. In the icon panel, click **Options**.
  - For information about the Spy Sweeper window, see “Understanding the Webroot Spy Sweeper Window” on page 14.
  - The Options panel displays.
3. Click the **Program Options** tab.
  - The Program Options tab displays.

4. Select the options you want to use.

| Option   | Description   |
|--|---|
| Add Sweep Option to Windows Explorer Context Menu              | This option lets you run a sweep on a specific folder from Windows Explorer. This adds a <b>Run a Sweep</b> option to the menu you see when you right-click a folder, letting you run a sweep on the selected folder.   |
| Automatic Check for Updates                                    | This option tells Spy Sweeper to automatically let you know when an updated version is available for downloading. You must be connected to the Internet for this option to work.  |
| Automatically Delete Items in Quarantine More Than __ Days Old | This option automatically deletes each quarantined item after the number of days you specify. This ensures that quarantined items do not continue to grow and take up space on your computer's hard drive.  |
| Enable Password Protection                                     | This option lets you protect your settings with a password. The option asks you to create a password. After you create the password, you must use the password to access the Options, Shields, Alerts, and Quarantined panels and to shut down Spy Sweeper. For more information, see "Protecting Settings with a Password" on page 19. |
| Show Tooltip Hints   | This option turns on explanatory text that displays when you hold your mouse pointer over options and buttons in Spy Sweeper.   |
| Load at Windows Startup  | This option ensures that Spy Sweeper is always open on your computer. We recommend using this option.   |
| Disable Splash Screen  | This option turns off the Spy Sweeper splash screen that displays when you first start Spy Sweeper.   |
| View News on Startup   | This option takes you directly to the News panel whenever you start Spy Sweeper.  |
| Show Only Alert Pop-up from System Tray                        | This option displays the pop-up alert, rather than the Spy Sweeper Alerts panel, when Spy Sweeper detects certain activities. For more information, see "Handling Alerts" on page 36.   |

## Scheduling Sweeps

You can set up Spy Sweeper to run sweeps automatically based on a schedule that you set. You can set up the schedule in any way that works for you. Here are examples of what you can do (assuming that you have Spy Sweeper set to load at startup):

- Set Spy Sweeper to run a sweep one hour after you turn on your computer. This works well if you turn on your computer each morning, read your e-mail messages in the first hour, then turn to other work.
- Set Spy Sweeper to run a sweep every day at 3 a.m. This works well if your computer is on all night, and you are not working at 3 a.m.
- Set Spy Sweeper to run on a specific day at a specific time, say Monday at 2 p.m., when you have a weekly staff meeting.

You can also have sweeps run automatically when you start Windows or when you shut down Windows using the Sweep at Windows Startup and Sweep at Windows Shutdown options. Remember that sweeps may take from several minutes to more than an hour to run, depending on

your options. Using one of these scheduling options may delay your Windows startup or shutdown.



To schedule sweeps:

1. Start Spy Sweeper, if it is not already open, and display the main window.
  - For more information, see “Starting Webroot Spy Sweeper” on page 14.
2. In the icon panel, click **Options**.
  - For information about the Spy Sweeper window, see “Understanding the Webroot Spy Sweeper Window” on page 14.
  - The Options panel displays.
3. Click the **Schedule** tab.
  - The Schedule tab displays.
4. Select the Sweep When Scheduled option.

| To set up days of the week   | To set a time period  |
|--|---|
| <ol style="list-style-type: none"><li>1. Select the Day of the Week option.<ul style="list-style-type: none"><li>• Use this option when you want to schedule sweeps for one or more specific days of the week.</li></ul></li><li>2. Select one or more days in the Day of the Week list to run your sweep.</li></ol> | <ol style="list-style-type: none"><li>1. Select the Periodic option.<ul style="list-style-type: none"><li>• Use this option when you want to schedule sweeps to run daily, weekly, or monthly.</li></ul></li><li>2. Select the time period you want to use.</li></ol> |

5. Select a Sweep Time option.
  - Sweep at Set Hour—Use this option to set the sweep to run at a specific time.
  - Hours after Loading—Use this option to set the sweep to run a specific number of hours after starting Spy Sweeper.
6. Use the spin buttons (up and down arrows) to set the time or number of hours.
  - As long as you keep Spy Sweeper open and your computer is turned on, Spy Sweeper will run sweeps based on your schedule.

## Setting Up Continuous Monitoring (Active Shields)

---

You can set up Spy Sweeper to continuously monitor the following types of threat-related activities on your computer:

- Internet Explorer changes (see page 30)
- Windows system changes (see page 32)
- Hosts file changes (for advanced computer users) (see page 32)
- Startup programs changes (for advanced computer users) (see page 35)

Spy Sweeper calls these functions Shields. When Spy Sweeper detects activity related to any of the shields, it displays an alert. For more information, see “Handling Alerts” on page 36.



## Setting Up the Internet Explorer Shields

You can set up Spy Sweeper to continuously monitor several Internet Explorer settings. These are settings that some spyware, adware, or unwanted programs change if you are not protected.

When Spy Sweeper detects activity related to the IE Favorites, IE Hijack, or IE Home Page Shields, it displays an alert. For more information, see "Handling Alerts" on page 36.



To set up Internet Explorer Shields:

1. Start Spy Sweeper, if it is not already open, and display the main window.
  - For more information, see "Starting Webroot Spy Sweeper" on page 14.
2. In the icon panel, click **Shields**.
  - For information about the Spy Sweeper window, see "Understanding the Webroot Spy Sweeper Window" on page 14.
  - The Shields panel displays, showing a summary of the available shields and their status. A check mark means the shield is turned on. An X means the shield is not turned on.
3. Click the **Internet Explorer** tab.
  - The Internet Explorer tab displays.
4. If you want to reset all of the Internet Explorer options on this tab back to the defaults used when Internet Explorer was first installed, click **Reset All Settings to Defaults**.
5. Select the options you want to use.

| Option                     | Description   |
|----------------------------|---|
| IE Favorites Shield        | This actively protects your Internet Explorer favorites. Whenever a Web site tries to change your favorites, Spy Sweeper lets you know and gives you the option to accept or reject the change. Some Web sites add entries to your favorites without letting you know. This option ensures that you are aware whenever changes are made.<br><br>Even if Spy Sweeper is not open when your favorites change, Spy Sweeper will detect the changes and ask you about them when you next start Spy Sweeper. |
| IE Tracking Cookies Shield | This actively watches for tracking cookies as you visit Web sites and removes them. Tracking cookies are cookies that can track your Web activities. These <i>may</i> include cookies that contain user names, passwords, or similar information that you enter on some Web sites.<br><br>If you want to hear a sound when Spy Sweeper removes a tracking cookie, select the Enable Sound option.   |

| Option   | Description  |
|--|--|
| IE Hijack Shield                                   | <p>This actively protects various Internet Explorer functions, such as the search page, error pages, and other default pages that Internet Explorer displays. Whenever a program tries to change these pages, Spy Sweeper lets you know and gives you the option to accept or reject the change. Some programs change (“hijack”) these pages without letting you know. This option ensures that you are aware whenever changes are made.</p> <p>Even if Spy Sweeper is not open when these pages change, Spy Sweeper will detect the changes and ask you about them when you next start Spy Sweeper.</p> |
| Edit IE Hijack Shield Settings                     | <p>Select this option if you want to edit the individual IE Hijack Shield settings, including the default home and search pages for IE.</p>  |
| IE Home Page Shield                                | <p>This actively protects the Web site you set as your home page in Internet Explorer. Some programs change the home page that you set. The home page is the Web site that displays automatically when you start Internet Explorer or when you click the <b>Home</b> button.</p> <p>Enter the Web address of the Web site you want in the text field in the format: <code>http://www.webroot.com</code> and click <b>Save</b>.</p>   |
| Automatically Restore Default without Notification | <p>Select this option if you want Spy Sweeper to automatically change the home page back to the site listed in the text field when a program tries to change your home page. To avoid seeing alerts about changes to your home page, select this option.</p>   |
| IE Search Page Shield                              | <p>This actively protects the Web site you set as your search page in Internet Explorer. Some programs change the search page that you set. The search page is the Web site that displays automatically when you click the <b>Search</b> button in Internet Explorer.</p> <p>Enter the Web address of the Web site you want in the text field in the format: <code>http://www.webroot.com</code> and click <b>Save</b>.</p>  |
| Automatically Restore Default without Notification | <p>Select this option if you want Spy Sweeper to automatically change the search page back to the site listed in the text field when a program tries to change your search page. To avoid seeing alerts about changes to your search page, select this option.</p>   |
| Advanced Settings                                  | <p>These options are advanced configuration options used only in error conditions and/or when a system is severely infected. You can use these options to repair your Internet Explorer settings when a browser hijacker embeds itself deeply in your browser. Webroot customer support is available to assist.</p> <p>Enter the Web address of the Web site in the format: <code>http://www.webroot.com</code> or the path to the file you want in the text field and click <b>Save</b>.</p>  |
| Automatically Restore Default without Notification | <p>Select this option if you want Spy Sweeper to automatically change the pages listed in the Advanced Settings drop-down list back to the site or path listed in the text field when a program tries to change one of these pages. To avoid seeing alerts about changes to these pages select this option.</p>  |

## Setting Up the Windows System Shields

You can set up Spy Sweeper to continuously monitor several Windows system settings. These are settings that some spyware, adware, or unwanted programs change if you are not protected.



To set up Windows System Shields:

1. Start Spy Sweeper, if it is not already open, and display the main window.
  - For more information, see “Starting Webroot Spy Sweeper” on page 14.
2. In the icon panel, click **Shields**.
  - For information about the Spy Sweeper window, see “Understanding the Webroot Spy Sweeper Window” on page 14.
  - The Shields panel displays, showing a summary of the available shields and their status. A check mark means the shield is turned on. An x means the shield is not turned on.
3. Click the **Windows System** tab.
  - The Windows System tab displays.
4. Select the options you want to use.

| Option                           | Description  |
|----------------------------------|--|
| Memory Shield                    | This option sweeps your computer’s random access memory (RAM) frequently looking for spyware, adware, or unwanted programs. It only sweeps memory when Spy Sweeper is open in the system tray in the lower-right corner of your screen (minimized).  |
| Spy Installation Shield          | This option actively watches for programs that try to install themselves on your computer. Whenever a program tries to install itself, Spy Sweeper lets you know and gives you the option to accept or reject the change.  |
| Windows Messenger Service Shield | (Applies only to Windows NT, 2000, and XP.) This option turns off and actively watches the Microsoft Messenger Service. This service is not an instant messaging program and does not affect your use of instant messaging. This service is often used for sending spam (unwanted e-mail) and creating pop-up ads. Turning off the service stops these types of spam and pop-ups.<br><br>If your computer is in your home, you can turn off this service without any problem. If you work in a corporate environment, contact your system administrator to find out if your company uses the service to communicate with company employees. If you are not sure, leave the service turned on until you find out. |

## Setting Up the Hosts File Shields

You can set up Spy Sweeper to continuously monitor two functions related to the Hosts file. The Hosts file is a Windows file that helps direct your computer to a Web site using Internet Protocol (IP) addresses. Your Web browser, for example Internet Explorer, uses the IP address to actually connect you to a Web site.

When you go to a Web site, like [www.webroot.com](http://www.webroot.com), your computer first looks in the Hosts file to see if it already knows where to go. If the domain ([webroot.com](http://www.webroot.com)) is listed, your computer goes directly to the IP address listed in the Hosts file. If the domain is not in the Hosts file, your computer looks up the information from the Internet (a slightly slower process).

The Hosts file has two primary uses, one good and one bad:

- Good—You can block a lot of adware cookies and other monitoring by using the Hosts file to route certain domains, such as advertising sites, to a dead end.
- Bad—Some spyware, adware, or unwanted programs will route certain domains to false addresses, for example, by making a commonly used search site open to a porn site. We call this hijacking.

Using Spy Sweeper to manage the Hosts file, you can block a lot of unwanted adware activity, while preventing your Internet browsing from being hijacked.

When Spy Sweeper detects activity related to the Hosts File Shield, it displays an alert. For more information, see “Handling Alerts” on page 36.



#### Note

This section describes highly technical features associated with how your computer finds the actual address of a Web site. The features described here will not damage your computer or remove anything you need if you enable them, but the underlying technology is complex if you are not aware of how IP addressing works.

---



To set up Hosts File Shields:

1. Start Spy Sweeper, if it is not already open, and display the main window.
  - For more information, see “Starting Webroot Spy Sweeper” on page 14.
2. In the icon panel, click **Shields**.
  - For information about the Spy Sweeper window, see “Understanding the Webroot Spy Sweeper Window” on page 14.
  - The Shields panel displays, showing a summary of the available shields and their status. A check mark means the shield is turned on. An x means the shield is not turned on.
3. Click the **Hosts File** tab.
  - The Hosts File tab displays.

4. Select the options you want to use.

| Option                 | Description   |
|------------------------|---|
| Hosts File Shield      | This option actively watches the Hosts file for any changes. Some programs will add or change the IP address for a Web site in the Hosts file. When you try to go to the added or changed Web site, you will really go to a different Web site, such as an advertising site. This shield ensures that programs do not change an IP address without you being aware of it. For more information about what happens when an IP address changes, see "Handling Alerts" on page 36.   |
| Common Ad Sites Shield | This option adds known advertising sites to your Hosts file and sets the IP address for those sites to the IP address for your computer. This blocks banner and other advertising from these sites. When you go to a Web site that has advertising from one of the blocked sites, you may see a small graphic that indicates a broken link to a graphic (typically a red x in a box). This just shows where the blocked ad would display. Spy Sweeper updates these sites when you update your definitions. For more information, see "Working with the Common Ad Sites Shield" on page 34. |

### Working with the Common Ad Sites Shield

This shield helps stop annoying banner and other ads from displaying when you go to Web sites. Webroot maintains a list of common advertising sites and adds these sites to your Hosts file. Instead of listing the correct IP address for these sites, the Webroot list puts in the IP address for your computer. This effectively blocks banner and other advertising from the sites in the list.

When you go to a Web site that has advertising from one of the blocked sites, you may see a small graphic that indicates a broken link to a graphic (typically a red x in a box). This just shows where the blocked ad would display.

If you have this shield turned on, Spy Sweeper updates these sites when you update your definitions.

When you turn on this shield, the Hosts File panel should look similar to Figure 3. You do not see the list of blocked Web sites because the Do Not Show Blocked Sites option is selected. If you want to see the blocked sites, deselect that option, then click **View Hosts File**.

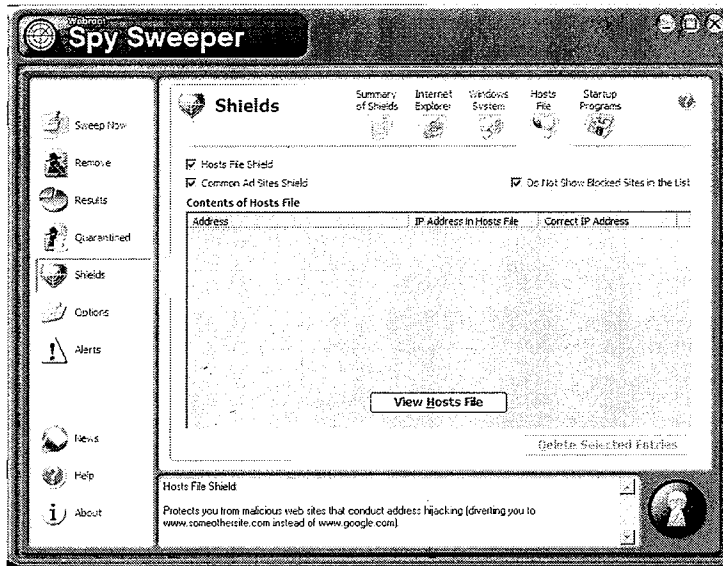


Figure 3: Hosts File tab

## Setting Up the Startup Programs Shield

You can set up Spy Sweeper to continuously monitor the list of programs that start every time you start Windows. Some spyware, adware, or unwanted programs add programs to this startup list if you are not protected.

When Spy Sweeper detects activity related to the Startup Shield, it displays an alert. For more information, see “Handling Alerts” on page 36.

Spy Sweeper also lets you edit the startup items.



### Caution

Editing startup items is for advanced users. Some items listed may be required by Windows or other programs. Deselecting items from the list could cause your computer to not start properly or cause some programs not to work. Edit with extreme caution.



To set up Windows Startup Programs Shields:

1. Start Spy Sweeper, if it is not already open, and display the main window.
  - For more information, see “Starting Webroot Spy Sweeper” on page 14.
2. In the icon panel, click **Shields**.
  - For information about the Spy Sweeper window, see “Understanding the Webroot Spy Sweeper Window” on page 14.
  - The Shields panel displays, showing a summary of the available shields and their status. A check mark means the shield is turned on. An x means the shield is not turned on.
3. Click the **Startup Programs** tab.
  - The Startup Programs tab displays.

- Select the options you want to use.

| Option             | Description   |
|--------------------|---|
| Startup Shield     | This option actively watches your startup items for any changes. Some programs will add startup items, so that the program will always run on your computer. This shield ensures that programs do not add something to the startup items without you being aware of it. For more information about what happens when the startup list changes, see “Handling Alerts” on page 36.  |
| Edit Startup Items | Editing startup items is for advanced users. Some items listed may be required by Windows or other programs. Deselecting items from the list could cause your computer to not start properly or cause some programs not to work. Edit with extreme caution.<br><br>Items listed as Spyware match something in Spy Sweeper’s definitions. To see more information about an item, select it and click <b>More Details</b> . Not all programs provide additional details. After you make a change, click <b>Save Changes</b> . |

## Handling Alerts

If you have turned on the corresponding Spy Sweeper shields, the following types of activities will cause Spy Sweeper to either display the Alerts panel (see Figure 4) or to display an alert pop-up near your system tray in the lower-right corner of your screen (see Figure 5):

- Changes to your Internet Explorer favorites, home page, or default pages (see “Setting Up the Internet Explorer Shields” on page 30)
- Changes to the Hosts file (see “Setting Up the Hosts File Shields” on page 32)
- Changes to the list of programs that start when Windows starts (see “Setting Up the Startup Programs Shield” on page 35)

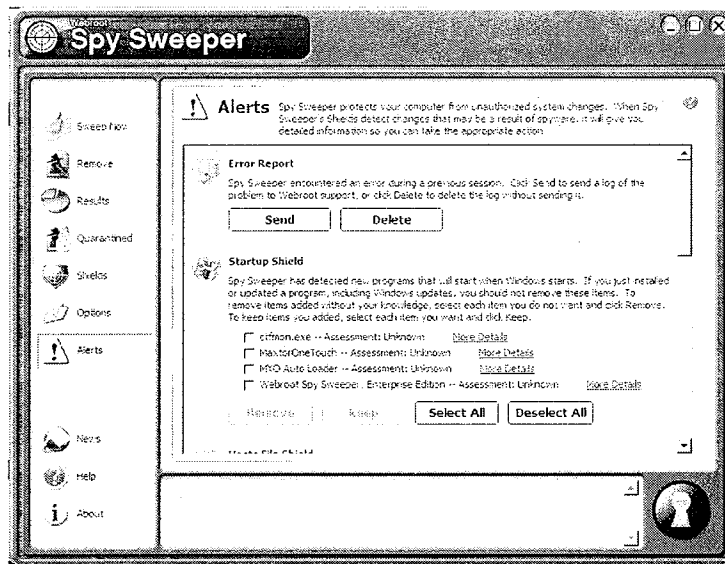


Figure 4: Example of the Alerts panel

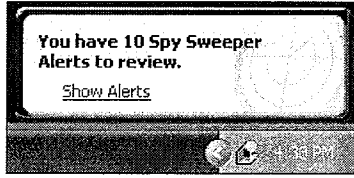


Figure 5: Example of the alert pop-up



**Note**



You can avoid Internet Explorer-related alerts if you use the Automatically Restore Default without Notification option on the Internet Explorer tab. For more information, see “Setting Up the Internet Explorer Shields” on page 30.

When you see the Alerts panel or an alert pop-up, you should take action as soon as possible to either keep the changes that you want or to remove changes spyware, adware, or unwanted programs caused.






To handle alerts:

1. When you see the Alerts panel as shown in Figure 4 or a pop-up alert as shown in Figure 5, do one of the following:
  - If the Alerts panel displays, continue with step 2.
    - If you do not want the Alerts panel to display automatically, select the Show Only Alert Pop-up from System Tray option. For more information, see “Setting Webroot Spy Sweeper Program Options” on page 27.
  - If the pop-up alert displays, click **Show Alerts**.
    - The pop-up alert displays if you have selected the Show Only Alert Pop-up from System Tray option or if you are using a password to protect your Spy Sweeper settings.
    - The Alerts panel of Spy Sweeper displays with information about any alerts.
2. Take action based on the type of alert.

| Alert type  | Actions  |
|---|--|
|  IE Favorites Shield | The alert shows the Web sites that have been added by a program to your Internet Explorer list of favorites. <ul style="list-style-type: none"> <li>• To keep the Web sites in your Internet Explorer favorites, select each site you want to keep and click <b>Keep</b>.</li> <li>• To remove the Web sites from your Internet Explorer favorites, select each site you want to remove and click <b>Remove</b>.</li> </ul>  |
|  IE Home Page Shield | The alert shows the Web site that a program changed as your Internet Explorer home page. It shows the site that was listed as your Internet Explorer home page and the new Web site that it was just changed to. <ul style="list-style-type: none"> <li>• To restore your Internet Explorer home page back to the page listed, click <b>Restore</b>.</li> <li>• To update your Internet Explorer home page to the new page listed, click <b>Keep New</b>.</li> </ul> |



| Alert type   | Actions  |
|--|--|
|  <p>IE Hijack Shield</p>        | <ul style="list-style-type: none"> <li>To restore your Internet Explorer default pages to the state they were in when you installed Spy Sweeper, click <b>Restore</b>.</li> <li>Most users do not change their default pages. Unless you or your system administrator made changes, you should click <b>Restore</b>.</li> <li>To update your Internet Explorer default page to the new pages, click <b>Keep New</b>.</li> </ul>  |
|  <p>Hosts File Shield</p>       | <p>The alert shows the IP address of Web sites that were added to your Hosts file and the IP address found after looking up the domain on the Internet.</p> <ul style="list-style-type: none"> <li>To remove the added items from your Hosts file, select each item that you did <i>not</i> add to the Hosts file yourself and click <b>Remove</b>.</li> <li>Most computer users do not add Web sites to their Hosts file. Removing these sites ensures that you will not be directed to an advertising or other site when you intend to go to a legitimate Web site.</li> <li>To keep items you want in your Hosts file, select each item that you added to your Hosts file yourself and click <b>Keep</b>.</li> </ul>                      |
|  <p>Startup Programs Shield</p> | <p>The alert shows the programs that have been added to your startup list along with an assessment. The assessment is either Spyware for known spyware, adware, or unwanted program or Unknown if the Spy Sweeper cannot match the item. To see more information about the item listed, if available, click <b>More Details</b>.</p> <ul style="list-style-type: none"> <li>To keep items in your startup list, select each item you want to start whenever Windows starts and click <b>Keep</b>.</li> <li>If you just installed or updated a program, including Windows updates, you should keep the items listed.</li> <li>To remove items from your startup list, select each item you want to remove and click <b>Remove</b>.</li> </ul> |

## Setting Up Items to Always Keep

If you find spyware, adware, or unwanted programs on your computer that you need to keep to make another program run properly, you can tell Spy Sweeper to always keep that item. Spy Sweeper will still detect the item and include it in its count of found items and traces, but it will not include it in the list of items to remove.



To set up items to always keep:

- Start Spy Sweeper, if it is not already open, and display the main window.
  - For more information, see “Starting Webroot Spy Sweeper” on page 14.
- In the icon panel, click **Options**.
  - For information about the Spy Sweeper window, see “Understanding the Webroot Spy Sweeper Window” on page 14.
  - The Options panel displays.

3. Click the **Always Keep** tab.
  - The Always Keep tab displays with a list of all items Spy Sweeper has found on your computer.
4. Select each item in the list that you want to keep.
  - A check mark next to the item shows that it is selected and will be kept. It will not display in the list of items to remove when you run a sweep.
5. To learn more about any item listed, select it and click **View more details online**.
  - You must be connected to the Internet to see the additional information.
  - Spy Sweeper opens your Internet browser, goes to the Webroot Web site, and displays information about the selected item. This information can help you decide if you want to keep the item.
  - To clear the list of everything that is not selected, click **Remove Unchecked Items**. This shortens the list to let you see only those items you want to always keep.

## Setting Up Items to Always Remove

---

If you find that some spyware, adware, or unwanted programs keep showing up in your sweeps, you can tell Spy Sweeper to always remove that item automatically. Spy Sweeper will still detect the item and include it in its count of found items and traces, but it will not include it in the list of items to remove. Spy Sweeper will remove it automatically.



To set up items to always remove:

1. Start Spy Sweeper, if it is not already open, and display the main window.
  - For more information, see “Starting Webroot Spy Sweeper” on page 14.
2. In the icon panel, click **Options**.
  - For information about the Spy Sweeper window, see “Understanding the Webroot Spy Sweeper Window” on page 14.
  - The Options panel displays.
3. Click the **Always Remove** tab.
  - The Always Remove tab displays with a list of all items Spy Sweeper has found on your computer.
4. Select each item in the list that you want Spy Sweeper to automatically remove.
  - A check mark next to the item shows that it is selected and will be removed. It will not display in the list of items to remove when you run a sweep.

5. To learn more about any item listed, select it and click **View more details online**.
  - You must be connected to the Internet to see the additional information.
  - Spy Sweeper opens your Internet browser, goes to the Webroot Web site, and displays information about the selected item. This information can help you decide if you want to remove the item.
  - To clear the list of everything that is not selected, click **Remove Unchecked Items**. This shortens the list to let you see only those items you want to always remove.

## Reporting Spyware

---

If you believe that Spy Sweeper is not finding spyware that you have on your computer, you can report it to Webroot. Webroot follows up on all reports to determine if it should add to its definitions.



### Note

You must connect to the Internet to report spyware.

---



To report spyware:

1. Start Spy Sweeper, if it is not already open, and display the main window.
  - For more information, see “Starting Webroot Spy Sweeper” on page 14.
2. In the icon panel, click **Options**.
  - For information about the Spy Sweeper window, see “Understanding the Webroot Spy Sweeper Window” on page 14.
  - The Options panel displays.
3. Click the **Program Options** tab.
  - The Program Options tab displays.
4. Click **Report Spyware**.
  - The Report Spyware window displays with space for you to provide your e-mail address and information about the symptoms you are seeing on your computer, as well as a button for you to send a report about possible spyware to Webroot.
  - If you want to view the report that will be sent, click **View Report**.
5. Complete the form if you want to provide additional information.
6. Click **Send Report**.

## Viewing Spy News

---

The Spy News provides you with tips, tricks, and information about spyware. You can set Spy Sweeper to display Spy News each time you display the main Spy Sweeper window. You can also view Spy News at any time.



To view Spy News:

1. Start Spy Sweeper, if it is not already open, and display the main window.
  - For more information, see “Starting Webroot Spy Sweeper” on page 14.
2. In the icon panel, click **News**.
  - For information about the Spy Sweeper window, see “Understanding the Webroot Spy Sweeper Window” on page 14.
  - The Spy News panel displays with the threat information.



# A: End User License Agreement

---

PLEASE READ THIS AGREEMENT CAREFULLY

Webroot Software, Inc.

## Software License Agreement

WEBROOT SOFTWARE, INC. (“WEBROOT”) IS WILLING TO LICENSE THE ENCLOSED SOFTWARE (AS WELL AS UPDATES WEBROOT MAY FURNISH YOU FROM TIME TO TIME) AND DOCUMENTATION (THE “SOFTWARE”) TO YOU (“YOU”) ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS IN THIS SOFTWARE LICENSE AGREEMENT (THE “AGREEMENT”). IF YOU ARE AN EMPLOYEE OR AGENT OF A COMPANY (THE “COMPANY”) AND ARE ENTERING INTO THIS AGREEMENT TO OBTAIN THE SOFTWARE FOR USE BY THE COMPANY FOR ITS OWN BUSINESS PURPOSES, YOU HEREBY AGREE THAT YOU ENTER INTO THIS AGREEMENT ON BEHALF OF THE COMPANY AND THAT YOU HAVE THE AUTHORITY TO BIND THE COMPANY TO THE TERMS AND CONDITIONS OF THIS AGREEMENT.

**BY CLICKING ON THE “ACCEPT” BUTTON BELOW, YOU ACKNOWLEDGE THAT YOU HAVE READ THIS AGREEMENT, UNDERSTAND IT, AND AGREE TO BE BOUND BY IT. IF YOU DO NOT AGREE TO ANY OF THE TERMS BELOW, WEBROOT IS UNWILLING TO LICENSE THE SOFTWARE TO YOU, AND YOU SHOULD CLICK ON THE “DO NOT ACCEPT” BUTTON BELOW TO DISCONTINUE THE INSTALLATION PROCESS. IN SUCH CASE, UPON REMOVAL, DESTRUCTION AND/OR RETURN OF THE SOFTWARE, ANY AMOUNTS ALREADY PAID BY YOU SHALL BE REFUNDED BY WEBROOT OR THE RETAILER FROM WHICH YOU PURCHASED THE SOFTWARE.**

1. **LICENSE.** Subject to the terms and conditions of this Agreement, Webroot hereby grants You a limited, non-exclusive, personal license to install, perform and use the Software, in machine-readable form only, solely for Your own personal or internal business use on a single computer in accordance with the instructions, specifications and documentation provided with the Software. You may make one (1) copy of the Software only for backup and archival purposes, *provided that* You reproduce all copyright and other proprietary notices that are on the original copy of the Software.
2. **RESTRICTIONS.** You may not use or copy the Software, or any copy thereof, in whole or in part, except as expressly provided in this Agreement. You may not modify, reproduce, create derivative works of, distribute, sell, resell, lend, loan, lease, license, sublicense or transfer (except as expressly provided herein) the Software or any portion thereof. You may not reverse engineer, disassemble, decompile, or translate the Software, or otherwise attempt to derive the source code of the Software, or authorize any third party to do any of the foregoing, except to the extent allowed under any applicable law. The Software contains trade secrets, trademarks, patents, and copyrights owned by Webroot,

and You shall maintain the Software in confidence. You shall not allow any access to or use of the Software by anyone other than You, or Your employees or agents, and any such use must be consistent with the terms, conditions and restrictions set forth in this Agreement. You may transfer the limited license granted herein solely in connection with the transfer of the Software, *provided, however*, that You deliver all copies of the Software to the transferee, that You do not keep any copies of the Software or related materials, and that the transferee is given a copy of this Agreement and acknowledges and agrees to be bound by its terms. Any attempt to transfer any of the rights, duties or obligations hereunder not in accordance with the foregoing is null and void and without any force or effect.

3. **LICENSE FEES.** You are responsible for paying Webroot or the retailer from whom you purchased the Software, the specified fees, and applicable taxes, for the license of the Software.
4. **OWNERSHIP.** The Software is licensed, not sold, to You for Your use only under the terms of this Agreement, and Webroot reserves all rights not expressly granted to You. You own the media, if any, on which the Software is recorded, but Webroot retains ownership of all copies of the Software itself.
5. **UPDATES/SUPPORT.** From time to time, Webroot may make new releases, revisions or enhancement to the Software (“**Updates**”) available to You. Your purchase must be recorded with Webroot either through product registration or a direct purchase through [www.webroot.com](http://www.webroot.com) for You to be notified of Updates. You may download and install those Updates, if any, within one (1) year of the Effective Date of this Agreement, or for as long as Your subscription is valid if You are licensing the Spy Sweeper Software on a subscription basis (offered only for the Spy Sweeper Software). Webroot will provide You with mail or telephone support for the Software for one (1) year from the Effective date, or for as long as Your subscription is valid.
6. **TERM/TERMINATION.** The Agreement becomes effective when You agree to the terms and conditions of this Agreement by opening, installing, using, accessing or manipulating the Software (the “**Effective Date**”), and this Agreement will terminate immediately upon notice to You if You materially breach any term or condition of this Agreement. You agree upon termination to promptly destroy the Software and all copies thereof.
7. **TRIAL.** If you are using the Software on a trial basis, and are authorized to do so, then You shall have a license under this Agreement to use the Software for the number of days indicated in the materials accompany the Software (the “**Trial Period**”) from the date You install it, solely for the purpose of evaluating the Software to determine whether to purchase an ongoing license to the Software. At the end of the Trial Period, the Software will stop working. During the Trial Period, the Software is provided to You “as is” and Your use is entirely at Your own risk.
8. **WARRANTY DISCLAIMER.** THE SOFTWARE IS PROVIDED TO YOU “AS IS” AND WEBROOT AND ITS SUPPLIERS AND LICENSORS EXPRESSLY DISCLAIM ANY AND ALL WARRANTIES AND REPRESENTATIONS OF ANY KIND WITH REGARD TO ANY SUBJECT MATTER OF THIS AGREEMENT, INCLUDING, WITHOUT LIMITATION, ANY WARRANTY OF NON-INFRINGEMENT, TITLE, FITNESS FOR A PARTICULAR PURPOSE, FUNCTIONALITY OR MERCHANTABILITY, WHETHER EXPRESS, IMPLIED OR STATUTORY. NO ORAL OR WRITTEN INFORMATION OR ADVICE GIVEN BY WEBROOT, ITS EMPLOYEES, DISTRIBUTORS, DEALERS, OR AGENTS SHALL INCREASE THE SCOPE OF THE ABOVE WARRANTIES OR CREATE ANY NEW WARRANTIES.

9. **LIMITATION OF REMEDIES.** REGARDLESS OF WHETHER ANY REMEDY SET FORTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE OR OTHERWISE, IN NO EVENT WILL WEBROOT OR ITS SUPPLIERS BE LIABLE TO YOU OR TO ANY THIRD PARTY FOR ANY LOST PROFITS, LOST DATA, INTERRUPTION OF BUSINESS, OR OTHER SPECIAL, INDIRECT, INCIDENTAL OR CONSEQUENTIAL DAMAGES OF ANY KIND ARISING OUT OF THE USE OR INABILITY TO USE THE SOFTWARE OR ANY DATA SUPPLIED THEREWITH, EVEN IF WEBROOT HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH LOSS OR DAMAGES AND WHETHER OR NOT SUCH LOSS OR DAMAGES ARE FORESEEABLE. IN NO EVENT SHALL THE LIABILITY OF WEBROOT EXCEED THE TOTAL AMOUNT RECEIVED BY WEBROOT FROM YOU UNDER THIS AGREEMENT.
10. **FOR SPY SWEEPER® SOFTWARE ONLY: YOUR ACKNOWLEDGMENTS.** You acknowledge that Your use of the Spy Sweeper Software may remove or disable other programs from Your computer, including software that may or may not be “spyware,” and You agree that Webroot shall not be responsible for such removal or disabling or the results of such removal or disabling. You are solely responsible for selecting which programs the Spy Sweeper Software removes from your computer. While Webroot uses reasonable efforts to properly identify those products that constitute or include “spyware” and update its list of such products, Webroot cannot guarantee that its list is complete or completely accurate. Because new and/or modified “spyware” programs are regularly introduced, You should make sure You receive Updates to the Spy Sweeper software to detect those new products Webroot adds when we provide Updates to the Spy Sweeper Software.
11. **AUTHORITY AND INDEMNITY.** If You have entered into this Agreement on behalf of (or to facilitate the use of the Software by) a Company of which You are an employee or agent, You represent and warrant that You have the full corporate right, power and authority to enter into this Agreement on behalf of the Company, that this Agreement has been duly authorized by the Company and that this Agreement will constitute the legal, valid and binding obligation of the Company, enforceable against the Company in accordance with its terms. You hereby agree to indemnify and hold Webroot harmless from any and all claims, damages, losses and expenses (including, without limitation, attorneys’ fees) arising from any breach of this Section 11.
12. **U. S. GOVERNMENT END USERS.** The Software is a “commercial item” as that term is defined at 48 C.F.R. 2.101, consisting of “commercial computer software” and “commercial computer software documentation” as such terms are used in 48 C.F.R. 12.212. Consistent with 48 C.F.R. 12.212 and 48 C.F.R. 227.7202-1 through 227.7202-4, all U.S. Government end users acquire the Software with only those rights set forth therein.
13. **EXPORT LAW.** The Software and related technology are subject to U.S. export control laws and may be subject to export or import regulations in other countries. You agree to strictly comply with all such laws and regulations and acknowledge that You have the responsibility to obtain such licenses to export, re-export or import as may be required.
14. **HIGH RISK ACTIVITY.** You acknowledge and agree that the Software is not intended for use with any high risk or strict liability activity, including, without limitation, air or space travel, technical building or structural design, power plant design or operation, life support or emergency medical operations or uses, and that Webroot makes no warranty and shall have no liability arising from any use of the Software in any high risk or strict liability activities.



15. **GENERAL.** This Agreement will be governed by the laws of the State of Colorado in the United States of America, without regard to or application of any conflicts of law rules or principles. The federal and state courts for Denver or Boulder County shall have exclusive jurisdiction over any disputes, claims or controversies arising out of or relating to this Agreement, and You hereby irrevocably waive any objection to the jurisdiction of such courts over any such dispute, claim or controversy. If any provision of this Agreement is held to be unenforceable, that provision will be enforced to the extent permissible by law and the remaining provisions will remain in full force. This Agreement is the complete and exclusive statement of the agreement between us which supersedes any proposal or prior agreement, oral or written, and any other communications between You and Webroot in relation to the subject matter of this Agreement.

If You have any questions regarding this Agreement or the Software, please contact the party that supplied the Software to You.

|  |
|--|
| THE SOFTWARE IS PROTECTED BY UNITED STATES COPYRIGHT LAW AND INTERNATIONAL TREATY. UNAUTHORIZED REPRODUCTION OR DISTRIBUTION IS SUBJECT TO CIVIL AND CRIMINAL PENALTIES. |
|--|

© Copyright 2003–2004, Webroot. All rights reserved. Protected by copyright and licenses restricting use, copying, distribution and decompilation. Webroot and Spy Sweeper are trademarks of Webroot.

# Glossary

---

|                     |   |
|---------------------|---|
| <b>adware</b>       | Adware is advertising-supported software that displays pop-up advertisements whenever the program is open. The software is usually available via free downloads from the Internet, and it is the advertisements that create revenue for the company. Although seemingly harmless (aside from intrusiveness and annoyance of pop-up ads), adware can install components onto your computer that track personal information (including your age, gender, location, buying preferences, surfing habits, etc.). Most advertising supported software doesn't inform you that it installs adware on your system, other than via buried reference in a license agreement. In many cases, the software will not function without the adware component. Some adware can install itself on your computer even if you decline the offer. |
| <b>definitions</b>  | A definition is the set of fingerprints that characterize a piece of spyware. Webroot regularly updates the definitions of known spyware that Spy Sweeper uses.   |
| <b>fingerprints</b> | Fingerprints are the unique patterns of files, cookies, and registry entries that spyware installs. Spy Sweeper compares these patterns to its internal database so that Spy Sweeper can detect spyware on your computer.   |

|   |  |
|---|--|
| <p><b>other (as used in the Category field)</b></p> | <p>“Other” represents a category of suspicious and/or annoying programs that can find their way onto your computer without your express knowledge. These programs often come bundled with third-party programs or can be installed as “drive-by downloads.” Some of these programs have spyware capabilities, while others may serve as an annoyance or negatively affect your system resources. There are many terms for these types of programs including scumware, annoyanceaware, parasites, malware, etc.</p> <p>Programs detected on your system that fall under this category are not necessarily considered spyware. These are programs that can fall into several categories: for example, some computer owners believe some of these programs take up unnecessary space and system resources; some computer users do not want to be targeted for advertising or promotions that some of these programs might deliver; some computer users may have forgotten that they downloaded the application and now may no longer want to have it; some of these programs may have been installed by someone else, like a child or roommate, who shares access to your computer, but that you do not want installed.</p> <p>On the other hand, some computer owners find benefit in having some of these programs installed on their systems. In addition, sometimes some of these programs are bundled with or linked to other applications and removing the program may also remove or disable the other applications. We created this category to inform you that this software resides on your system and to give you the ability to make the decision as to whether or not you want this software installed. The choice is up to you.</p> |
| <p><b>spyware</b></p>                               | <p>Spyware is any application that makes surreptitious changes to your computer while collecting information about your computer activities. This information is then sent to a third party for malicious purposes, without your knowledge or consent.</p> <p>Spyware arrives bundled with freeware or shareware, through e-mail or instant messenger, as an ActiveX installation, or by someone with access to your computer. Once on your drive, spyware secretly installs itself and goes to work. Unlike traditional personalization or session cookies, spyware is difficult to detect, and difficult (if not impossible) for the average user to remove.</p>   |
| <p><b>system monitors</b></p>                       | <p>System monitors are applications designed to monitor computer activity to various degrees. These programs can capture virtually everything you do on your computer, including recording all keystrokes, e-mails, chat room dialogue, Web sites visited, and programs run. System monitors usually run in the background so that you do not know that you are being monitored. The information gathered by the system monitor is stored on your computer in an encrypted log file for later retrieval. Some programs are capable of e-mailing the log files to another location.</p> <p>Traditionally, system monitors had to be installed by someone with administrative access to your computer, such as a system administrator or someone who shares your computer. However, there has been a recent wave of system monitoring tools disguised as e-mail attachments or “freeware” software products.</p>   |
| <p><b>traces</b></p>                                | <p>Traces are places where Spy Sweeper finds spyware fingerprints. Traces can be a file, cookie, or registry entry.</p>  |

|                         |  |
|-------------------------|--|
| <b>tracking cookies</b> | Tracking cookies are one type of spyware. These are pieces of information that are generated by a Web server and stored on your computer for future access. Cookies were originally implemented to allow you to customize your Web experience, and continue to serve a useful purpose in enabling a personalized Web experience. However, some Web sites now issue tracking cookies, which allow multiple Web sites to store and access cookies that may contain personal information (including surfing habits, user names and passwords, areas of interest, etc.), and then simultaneously share the information it contains with other Web sites. This sharing of information allows marketing firms to create a user profile based on your personal information and sell it to other firms. Tracking cookies are almost always installed and accessed without your knowledge or consent. |
| <b>Trojan horses</b>    | Trojans are one type of spyware. These are malicious programs that appear as harmless or desirable applications. Trojans are designed to cause loss or theft of computer data, and to destroy your system. Some trojans, called RATs (Remote Administration Tools), allow an attacker to gain unrestricted access of your computer whenever you are online. The attacker can perform activities such as file transfers, adding/deleting files or programs, and controlling the mouse and keyboard. Trojans are generally distributed as e-mail attachments or bundled with another software program.   |



# Index

---

## A

Associated Traces Found field 21

## C

Category field 22  
closing Spy Sweeper 16  
conventions, typographic 1  
customer support 1

## D

definitions  
    updating 13  
Delete Selected button 25  
deleting items permanently 24

## E

exiting Spy Sweeper 16

## F

Figure 15  
Files/Folders Inspected field 21, 23  
Fingerprint Type field 22

## H

home page  
    monitoring changes to 29  
Hosts file  
    monitoring changes to 29

## I

installing Spy Sweeper 2  
Internet Explorer  
    monitoring changes to the home page 29

## L

list of items found 21  
Location field 21

## M

Memory Items Inspected field 21, 23  
memory, monitoring 29  
memory, sweeping 17  
monitoring  
    Hosts file 29  
    Internet Explorer home page 29  
    memory 29  
    startup programs 29  
    tracking cookies 29

Windows system changes 29

## O

opening Spy Sweeper 14  
options, setting for sweeps 17

## P

Pause button 20

## Q

Quarantine folder location 20  
quarantined items, handling 24  
quarantining items 20

## R

Registry Items Inspected field 21, 23  
registry, sweeping 17  
removing items 20  
Restore Selected button 26  
restoring items 25  
results, viewing 23  
running  
    sweeps 20  
    sweeps automatically 28

## S

Save to File button 24  
scanning for threats 20  
scheduling sweeps 28  
Select Drives to Sweep drop-down list 18  
setting sweep options 17  
setting up  
    continuous monitoring 29  
shields  
    setting up 29  
shutting down Spy Sweeper 16  
Skip Files Larger Than option 18  
Software Fingerprints Loaded field 21  
Software Found field 21, 23  
Spy Sweeper  
    exiting 16  
    installing 2  
    running sweeps 20  
    setting sweep options 17  
    starting 14  
    understanding the main window 14  
    updating the definitions 13  
    updating the program 12

- spyware
  - understanding 2
- starting Spy Sweeper 14
- startup programs
  - monitoring 29
- stopping Spy Sweeper 16
- stopping sweeps 21
- support 1
- Sweep All Folders on Selected Drives option 19
- Sweep Memory option 18
- Sweep Only Known Software Folders option 19
- sweep options
  - setting 17
- Sweep Registry option 18
- sweeps
  - running 20
  - running automatically 28
  - scheduling 28
  - starting 20
  - stopping 21
  - viewing results 23
- T**
- technical support 1
- threats

- deleting permanently 24
- handling quarantined 24
- quarantining 20
- removing 20
- restoring 25
- sweeping for 20
- Traces Found field 21, 23
- Traces Quarantined field 23
- Traces Quarantined Since Installation field 23
- tracking cookies
  - monitoring 29
- typographic conventions 1

## **U**

- updating
  - the Spy Sweeper definitions 13
  - the Spy Sweeper program 12

## **V**

- viewing
  - sweep results 23

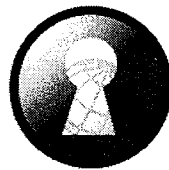
## **W**

- Windows system
  - monitoring changes to 29

**Exhibit 2: *System Administrator Guide*, “Quick Start Guide,” and “Release Notes”  
for Webroot Enterprise Version 2.0**



# Webroot Enterprise System Administrator Guide



**webroot**<sup>®</sup>  
SOFTWARE, INC.

Webroot Software, Inc.  
PO Box 19816  
Boulder, CO 80308  
[www.webroot.com](http://www.webroot.com)

Webroot Enterprise System Administrator Guide

Copyright © 2004 Webroot Software, Inc.

Webroot is a registered trademark of and Admin Console, Client Service, CommAgent, Update Service, Webroot Spy Sweeper Enterprise, Webroot Enterprise, Webroot Enterprise Server, and Webroot Update Server are trademarks of Webroot Software, Inc.

Other product and company names may be trademarks of their respective owners.

# Contents

---

|   |           |
|---|-----------|
| <b>1: Planning Your Installation</b>                              | <b>1</b>  |
| About This Guide .....  | 1         |
| Conventions .....   | 1         |
| Technical Support .....   | 2         |
| System Requirements .....   | 2         |
| Understanding Webroot Enterprise .....                            | 3         |
| Planning for Webroot Enterprise Deployment .....                  | 5         |
| How Webroot Enterprise Updates Work .....                         | 7         |
| Key Steps to Installing and Setting Up Webroot Enterprise .....   | 8         |
| <b>2: Installing Webroot Enterprise</b>                           | <b>9</b>  |
| Setting up a SQL Database .....                                   | 9         |
| Installing Webroot Enterprise Server on Your Company Server ..... | 11        |
| Setting Up Client Workstations .....                              | 20        |
| Client Installation Options .....                                 | 22        |
| Example Logon Script .....  | 22        |
| Uninstalling Spy Sweeper from Client Workstations .....           | 23        |
| Installing and Assigning Distributor Servers .....                | 23        |
| Installing Distributor Servers .....                              | 24        |
| Assigning Distributor Servers .....                               | 24        |
| Changing the Distributor Server Port .....                        | 25        |
| Understanding the Admin Console Window .....                      | 26        |
| <b>3: Setting Up the Webroot Enterprise Server</b>                | <b>27</b> |
| Accessing the Admin Console and Viewing News .....                | 27        |
| Editing the Server Settings .....                                 | 27        |
| Setting Up Notification .....                                     | 30        |
| Setting Up Notification E-mail Addresses .....                    | 30        |
| Setting Up Notification Messages .....                            | 31        |
| Setting Up Error Notification .....                               | 31        |
| Managing Clients .....  | 32        |
| Managing Groups .....   | 32        |
| Creating and Exporting Client Reports .....                       | 33        |
| Polling Client Workstations Now .....                             | 34        |
| Deleting Client Workstations .....                                | 34        |
| Filtering Information .....                                       | 35        |
| <b>4: Managing Spy Sweeper</b>                                    | <b>37</b> |
| Managing Spyware .....  | 37        |
| Setting Up Automatic Spyware Handling .....                       | 37        |
| Setting Up Continuous Monitoring: Active Shields .....            | 39        |
| Configuring Sweeps .....  | 41        |
| Configuring Sweep Settings .....                                  | 41        |
| Setting Up Sweep Alerts .....                                     | 43        |

|   |           |
|---|-----------|
| Running Sweeps .....  | 44        |
| Running a Sweep Now .....                                       | 44        |
| Scheduling Sweeps .....   | 45        |
| Viewing and Stopping Sweeps .....                               | 46        |
| Updating Spy Sweeper .....                                      | 46        |
| Installing Updates Manually .....                               | 46        |
| Installing Updates Automatically .....                          | 47        |
| Setting Up Update Notification .....                            | 48        |
| Setting up Updating for Mobile End Users .....                  | 48        |
| Viewing a Summary of Detected Spyware .....                     | 49        |
| Unlocking Functions at a Client Workstation .....               | 49        |
| <b>5: Monitoring Status</b>                                     | <b>51</b> |
| Viewing Update History and Installed Applications .....         | 51        |
| Viewing Update History .....                                    | 51        |
| Viewing Applications Installed by Workstation .....             | 51        |
| Viewing Client Status .....                                     | 52        |
| Viewing Errors .....  | 52        |
| Generating Reports .....  | 53        |
| <b>A: Webroot Enterprise Port Requirements</b>                  | <b>55</b> |
| <b>B: Migrating an Existing Installation from DBISAM to SQL</b> | <b>57</b> |
| <b>Index</b>  | <b>59</b> |

# 1: Planning Your Installation

---

Webroot Enterprise™ lets you install and manage Webroot® products throughout your company. You can set up groups with different settings, install updates automatically or manually, view the status of all products, and much more.

Webroot Enterprise gives you companywide management and control to ensure that your company's computer resources are protected from a variety of threats.

## About This Guide




---

This *Guide* tells you how to set up and use Webroot Enterprise to install and manage Webroot products throughout the company. It assumes that you have detailed knowledge of the Windows operating systems in use in your company and your network.

The information in this *Guide* is also available from the help button.

## Conventions

This *Guide* uses several typographical conventions to help explain how to use Webroot Enterprise.

| Convention   | Definition   |
|--|--|
| <b>Bold</b>  | Words in <b>bold</b> show items to select or click, such as menu items or buttons.   |
| Tree navigation  | The Guide uses parent node > child node notation for tree navigation. For example, <b>Admin Tasks &gt; Settings</b> . This means to expand to the Admin Tasks node in the tree and select the Settings node. |
|  <b>Note</b>    | This symbol means the following information is a note that gives you important information that may affect how you use Webroot Enterprise.   |
|  <b>Caution</b> | This symbol means the following information is a caution that warns you about actions that may affect your ability to use some programs on your computer.  |
|                 | This symbol means that the following information is a procedure.   |

# Technical Support

---

Technical support is available by phone and e-mail:

- Call 800-870-8102
- Send your questions to: [esupport@webroot.com](mailto:esupport@webroot.com). We will respond within one business day.

## System Requirements

---

Following are the system requirements for Webroot Enterprise.

*Table 1: Company server system requirements*

|                         |  |
|-------------------------|--|
| <b>Operating system</b> | Windows NT 4.0 SP5 or higher, Windows 2000, Windows XP (see note below), Windows Server 2003                       |
| <b>CPU</b>              | 200 MHz minimum; 350 MHz or better recommended   |
| <b>Memory</b>           | 512 MB recommended   |
| <b>Disk space</b>       | 30 MB free space for operation. Additional free space needed for database growth. We recommend 1 GB of free space. |

*Table 2: Distributor server system requirements*

|                         |  |
|-------------------------|--|
| <b>Operating system</b> | Windows NT 4.0 SP5 or higher, Windows 2000 SP4 or higher, Windows XP (see note below), Windows Server 2003 |
| <b>CPU</b>              | 200 MHz minimum; 350 MHz or better recommended   |
| <b>Memory</b>           | 512 MB recommended   |
| <b>Disk space</b>       | 60 MB free space for operation.  |

*Table 3: Client workstation system requirements*

|                          |   |
|--------------------------|---|
| <b>Operating system</b>  | Windows 98, 98SE, ME, NT 4.0, 2000, or XP                             |
| <b>CPU</b>               | 150 MHz or better recommended   |
| <b>Memory</b>            | 32 MB RAM minimum; 128 MB RAM or better recommended                   |
| <b>Disk space</b>        | 15 MB free space  |
| <b>Internet Explorer</b> | Version 6.0 with Service Pack 1 required for Windows 98, 98SE, and ME |



### Note

Due to modifications that Microsoft made in Service Pack 2 for Windows XP that limit simultaneous TCP/IP connections, we do not recommend using the Poll Now or Sweep Now functions for more than five client workstations at a time. If you do, you may see temporary system lag and an Event ID error 4226 entry in your Windows system log. If you are managing large numbers of clients with frequent polling intervals from a server with Windows XP and SP2, you may also see the 4226 error when more than five clients poll in simultaneously.

---

# Understanding Webroot Enterprise

Webroot Enterprise offers a total enterprise solution for your companywide spyware management using a client/server architecture. Figure 1 shows a base configuration and how Webroot Enterprise works.

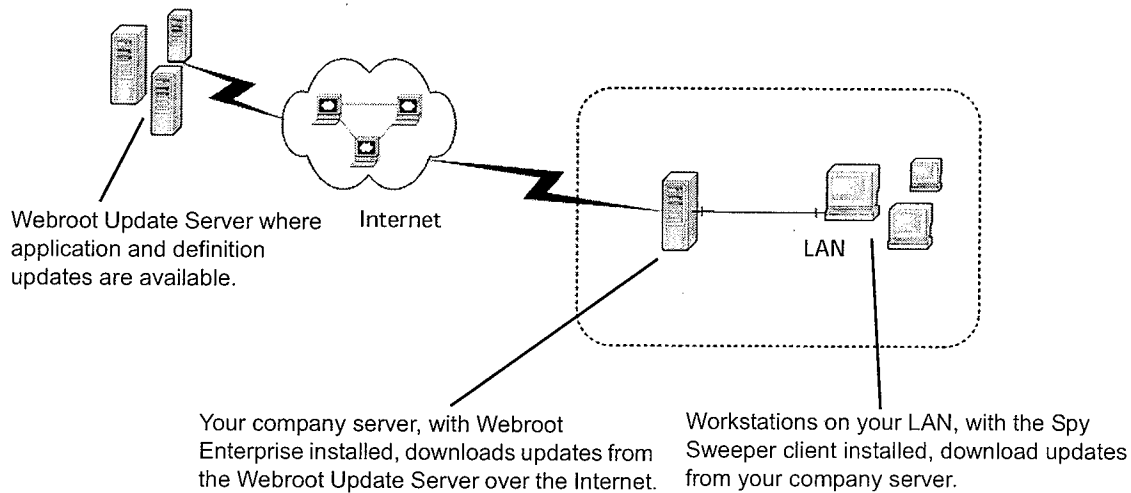


Figure 1: Webroot Enterprise base architecture

The Webroot Enterprise product includes three types of components that you install on your computers:

- On a company server, you install Webroot Enterprise Server™, which is described in Table 4.
  - If you want to use more than one company server, consider using additional distributor servers, as described in “Planning for Webroot Enterprise Deployment” on page 5, or contact technical support for assistance.
- On each end user’s computer, you install the client workstation components, which are described in Table 5.
- On each distributor server, you install the distributor service, which is described in Table 6.

If you have a complex internal network, run firewall programs at the desktop or server level, or use proxy servers internally, you should review “Appendix A. Webroot Enterprise Port Requirements” on page 55.

Table 4: Webroot Enterprise Server components

| Component       | File name                | Description  | Installation/Network Access Requirement  |
|-----------------|--------------------------|--|--|
| Client Service™ | WebrootClientService.exe | Controls the communication between the client workstations and your company server.  | <ul style="list-style-type: none"> <li>Installed during the installation of Webroot Enterprise Server.</li> <li>Requires local network access.</li> </ul>  |
| Update Service™ | WebrootUpdateService.exe | Controls the updates from the Webroot Update Server™ to your company server.   | <ul style="list-style-type: none"> <li>Installed during the installation of Webroot Enterprise Server.</li> <li>Requires local network and Internet access.</li> <li>Requires use of port 443 on your server.</li> </ul> |
| Admin Console™  | WebrootAdminConsole.exe  | Provides a graphical user interface (GUI) to let you set up and manage the Webroot applications across the company. Most of this <i>Guide</i> describes how to use this component. | <ul style="list-style-type: none"> <li>Installed during the installation of Webroot Enterprise Server.</li> <li>Does not require any network access.</li> </ul>  |

Table 5: Webroot Enterprise client workstation components

| Component                        | File name      | Description   | Installation/Network Access Requirement  |
|----------------------------------|----------------|---|--|
| Communication Agent (CommAgent™) | CommAgent.exe  | <ul style="list-style-type: none"> <li>Communicates periodically with the Client Service on your company server to see if any new or updated applications are available.</li> <li>Runs as a system service on each client workstation.</li> </ul> | <ul style="list-style-type: none"> <li>Installed when you set up client workstations.</li> <li>Requires local network access.</li> </ul> |
| Spy Sweeper                      | SpySweeper.exe | <ul style="list-style-type: none"> <li>Detects spyware and provides access to options for workstations users.</li> <li>Runs as a system service on each client workstation.</li> </ul>  | <ul style="list-style-type: none"> <li>Installed when you set up client workstations.</li> </ul>   |

Table 6: Webroot Enterprise distributor server components

| Component           | File name                    | Description   | Installation/Network Access Requirement  |
|---------------------|------------------------------|---|--|
| Distributor service | WebrootUpdateDistributor.exe | <ul style="list-style-type: none"> <li>Communicates periodically with the Client Service on your company server to receive updates and with CommAgents to distribute updates.</li> <li>Runs as a system service on the server.</li> </ul> | <ul style="list-style-type: none"> <li>Installed when you set up distributor servers.</li> <li>Requires local network access.</li> </ul> |



# Planning for Webroot Enterprise Deployment

If you plan to deploy Webroot Enterprise to 500 or fewer client workstations, you can use the base configuration shown in Figure 1. If you are deploying to more than 500 client workstations, you should review the information in this section to determine the best configuration and settings to use.

Table 7 provides general configuration and database recommendations based on the number of client workstations.

*Table 7: Configuration and database recommendations*

| Number of client workstations | Company server specifications   | Database  | Number of distributor servers                             | Poll no more frequently than                              |
|-------------------------------|---|---|---|---|
| Up to 500                     | Single 350 MHz processor with 512 MB RAM                                    | DBISAM  | 0   | One hour  |
| 500 to 10,000                 | Single 1 GHz processor, 512 MB RAM  | DBISAM  | 0 to 2  | Two hours   |
| 10,000 to 40,000              | Single 1 GHz processor, 1 GB RAM  | MS SQL Server   | 2 to 3  | Four hours  |
| 40,000 to 75,000              | Dual 1 GHz processors, 2 GB RAM   | MS SQL Server   | 3 to 6  | Four hours  |
| Over 75,000                   | Deploy multiple company servers<br>Contact technical support for assistance | Base on number of client workstations each server handles | Base on number of client workstations each server handles | Base on number of client workstations each server handles |

You may want to install additional distributor servers or company servers for two reasons:

- You have multiple sites and want to minimize bandwidth usage on WAN segments between the sites. The normal communication between the client and the server is only about 1 KB. Spy definition updates are typically 1 MB. A new Spy Sweeper client update can be as large as 5.5 MB.
- You have a large number of clients relative to your server capabilities. Many things can affect the performance of the server.

Deploying distributor servers reduces WAN bandwidth consumed when spy definitions or software updates are delivered. Distributor servers receive copies of Spy Sweeper client and definitions updates. For more information about how updates work, see "How Webroot Enterprise Updates Work" on page 7.

In a configuration that uses distributor servers, the client workstations poll the company server. If updates are available, the company server sends a randomized list of distributor servers to each client workstation. The client workstation requests updates from the first distributor server on the list. The distributor server sends the updates to the client workstation. If the distributor server is not available, the client workstation sends its request to the next distributor server on the list. The company server is always the last server on the list and will send the updates if no distributor server is able to do so.

The figures that follow show some recommended configurations for typical deployments.

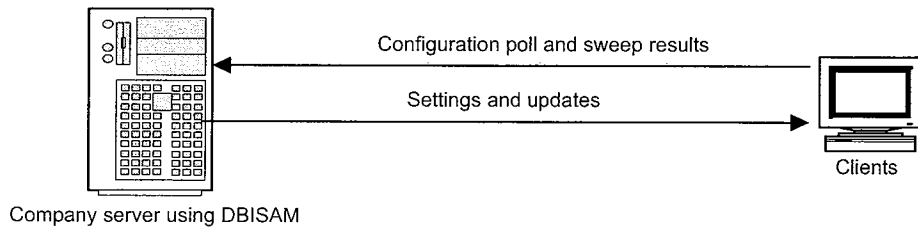


Figure 2: Single site with 500 clients

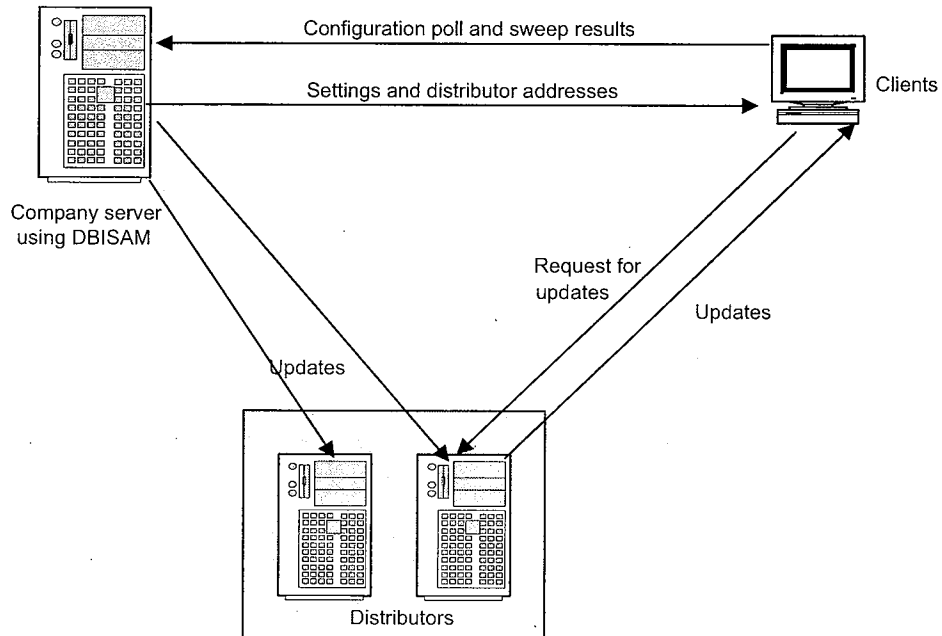


Figure 3: Single site with 10,000 clients

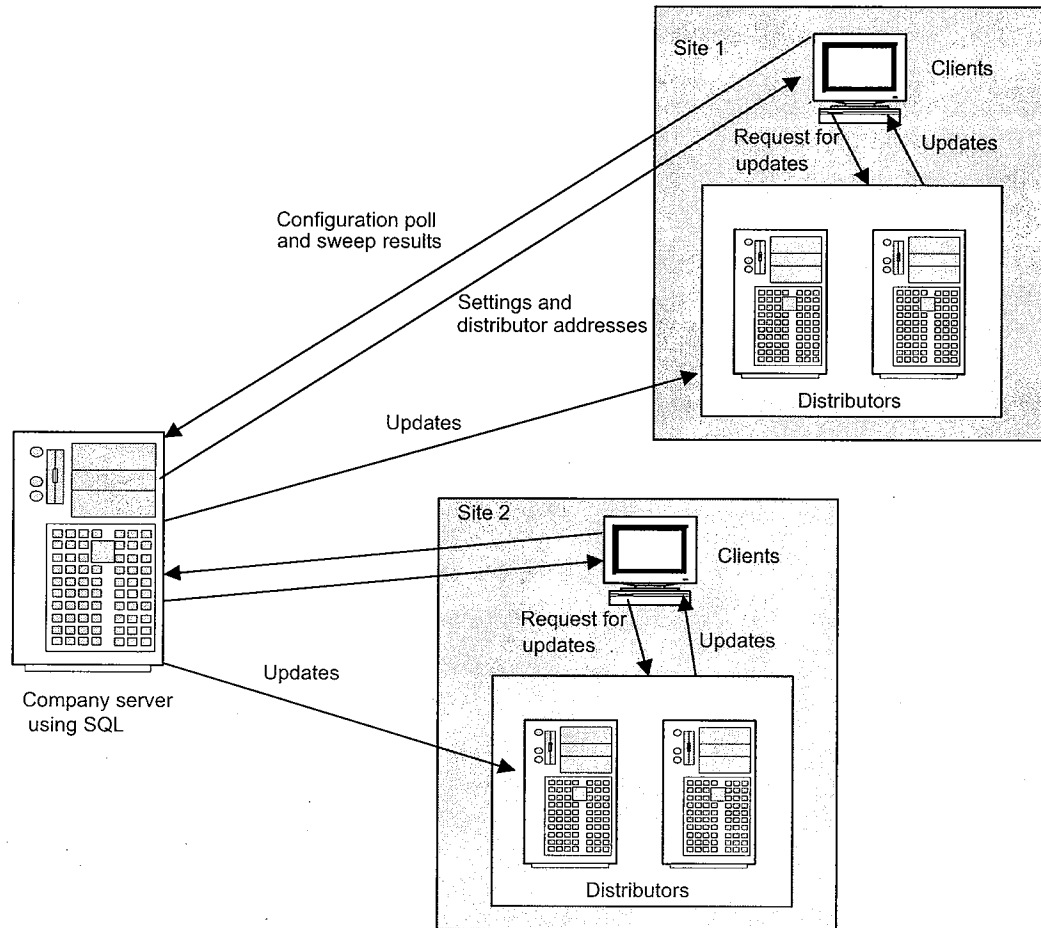


Figure 4: Multiple sites with more than 10,000 total clients

## How Webroot Enterprise Updates Work

Most Webroot Enterprise updates are completely automatic after initial installation and setup. The whole update process works like this:

1. Your company server automatically moves updates to all assigned distributors once they are downloaded from the Webroot Update Server. Your distributor servers synchronize with your company server every minute.
2. The client workstations poll the company server.
3. If updates are available, the company server sends a randomized list of distributor servers containing the update to the client workstation.
  - For client workstations to receive updates, you must assign updates to specific groups or to the company as a whole. From the Admin Console, select **Manage Desktop Applications > Spy Sweeper > Update Spy Sweeper** and go to either **Manual Install** or **Auto Install**. If you set up automatic installation on *after* an update has downloaded, the automatic installation does not apply to that update. For more information, see "Updating Spy Sweeper" on page 46.
4. The client workstation requests updates from the first distributor server on the list.

5. The distributor server sends the updates to the client workstation.
6. If the distributor server is not available, then the client workstation sends its request to the next distributor server on the list. The company server is always the last server on the list, and it will send the updates if no other distributor server is able to do so.

This process spreads the load across all distributor servers to ensure that the servers are not overwhelmed with update requests.

## Key Steps to Installing and Setting Up Webroot Enterprise

---

Once you have determined how you will deploy Spy Sweeper Enterprise in your environment, you are ready to begin the installation and setup. The six major steps in getting started are:

1. Gather information for server installation.
  - For more information, see Table 8 on page 11.
2. Install Webroot Enterprise Server.
  - For more information, see “Installing Webroot Enterprise Server on Your Company Server” on page 11.
3. Check for latest news and updates.
  - For more information, see “Accessing the Admin Console and Viewing News” on page 27 and “Installing Updates Manually” on page 46.
4. Deploy initial clients.
  - For more information, see “Setting Up Client Workstations” on page 20.
5. Set up sweep settings and initial sweeps.
  - For more information, see “Managing Spyware” on page 37, “Configuring Sweeps” on page 41, and “Running Sweeps” on page 44.
6. Broader deployment.

# 2: Installing Webroot Enterprise

---



You must perform the following tasks to install Webroot Enterprise:

1. If you are using Microsoft SQL Server for your database, set up the SQL database. (See page 9.)
  - For information about determining what database to use, see “Planning for Webroot Enterprise Deployment” on page 5.
2. Install Webroot Enterprise Server on your company server. (See page 11.)
3. Set up one or more client workstations. (See page 20.)
4. If you are using distributor servers, install one or more distributors. (See page 23.)

## Setting up a SQL Database

---

If you determined that you will use Microsoft SQL Server for your installation, you must create the database and a system DSN before starting the installation process. You must also have the user name and password available.

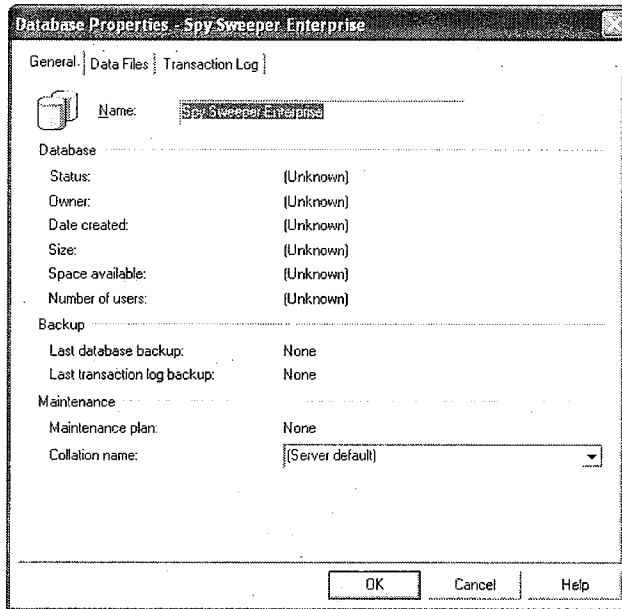
For information about determining whether to use SQL, see “Planning for Webroot Enterprise Deployment” on page 5. If you have an existing Webroot Enterprise installation and need to migrate the database from DBISAM to SQL Server, see “Appendix B, Migrating an Existing Installation from DBISAM to SQL” on page 57.



To set up the SQL database:

1. Open the SQL Enterprise Manager.
2. Browse to the Databases folder.
3. Right-click and select **New Database**.

4. Give the new database a unique name.



5. Browse to the Users pane of the new database.
6. Right-click and select **New Database User**.
7. Create a new user and select the db\_owner role in the Database Role Membership section.



8. Configure your SQL server for SQL Server and Windows authentication and use a SQL user account instead of a Windows account to access a SQL database with Webroot Enterprise.
9. When you install Webroot Enterprise Server, select SQL Server 2000 in the Database Settings window.
  - The Select the SQL Server 2000 drop-down list takes a moment to populate with the list of SQL servers in your environment.
10. Select the SQL server where you just set up the database.

11. Enter the name and login information for the database created above.
  - The installer program attempts to log in to the SQL database with the credentials provided and displays a message if it cannot connect to the database.

## Installing Webroot Enterprise Server on Your Company Server

---

The Webroot Enterprise Server installation process installs all of the executables described in Table 4 on page 4. You must install Webroot Enterprise Server while logged in with Administrative rights.

The WebrootClientService.exe and WebrootUpdateService.exe run as Windows services and should always be started. This permits your company server to download updates from the Webroot Update Server and client workstations to download updates from your company server.

During the installation, you must enter all of the information requested to continue the process. You should be prepared with information listed in Table 8.

*Table 8: Information required for Webroot Enterprise Server installation*

| Field               | Description  |
|---------------------|--|
| Download Folder     | Path to the folder where your company server stores the updates it downloads from the Webroot Update Server. For best performance, use a folder on the same server. It can also be a folder on any drive your company server can access.   |
| Key Code            | Unique code that identifies the rights and privileges associated with your installation, such as the number of licenses you have purchased for each client workstation application.<br><br>Your key code comes in an e-mail message. Be sure to include the brackets.  |
| E-mail Host         | Fully qualified domain name for your e-mail server used for outgoing mail (SMTP server).   |
| From Address        | E-mail address that notification messages will come from. Must be a real e-mail address in the format: tom@webroot.com.  |
| Client Service Port | Port on your company server that the Client Service will use to communicate with your client workstations. The default port is 50000. Be sure that the port you use is not used to communicate with another system.<br><br>After installation you cannot edit this value directly from the Admin Console. If you need to change this setting, contact technical support. |
| Proxy Server        | If you use a proxy server to access the Internet, enter your proxy server name or IP address and port number in one of the following formats: <ul style="list-style-type: none"> <li>• server_name.company.com:80</li> <li>• 10.0.0.1:80</li> </ul> If you do not use a proxy server, leave the field blank.   |
| Proxy Username      | If you use a proxy server that requires authentication, enter your proxy server username.  |

Table 8: Information required for Webroot Enterprise Server installation (Continued)

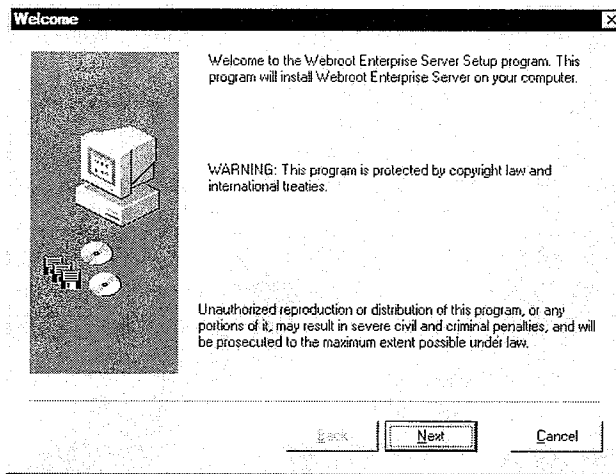
| Field             | Description   |
|-------------------|---|
| Proxy Password    | If you use a proxy server that requires authentication, enter your proxy server password.   |
| Client Service IP | Enter the IP address or host name that the client workstations will use to communicate with your company server. For IP resolution, select the IP address of the network interface card (NIC) visible to client workstations. For host name resolution, enter the fully qualified domain name of your server (requires a properly configured DNS environment).<br><br>After installation you cannot edit this value directly from the Admin Console. If you need to change this setting, contact technical support. |



To install Webroot Enterprise Server:

1. Close all other Windows programs that you have open on your computer.
2. Start the installation program.

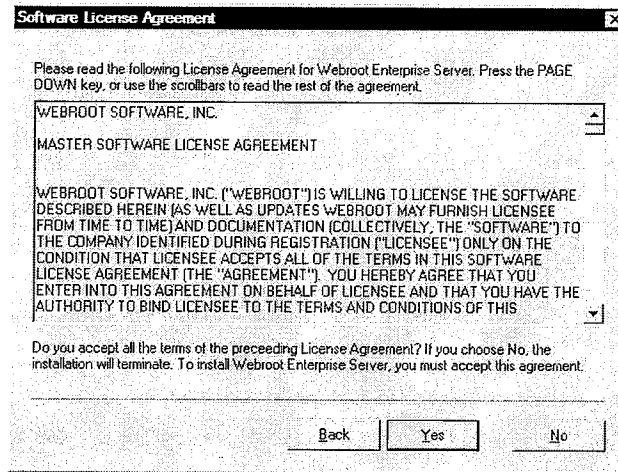
| To install from a CD   | To install from a downloaded file  |
|--|--|
| <ol style="list-style-type: none"> <li>1. Insert the CD into your CD drive. <ul style="list-style-type: none"> <li>• The installation options should display automatically. If they do not, use Windows Explorer to navigate to your CD drive. Then double-click WebrootEnterpriseServerSetup.exe to start the installation.</li> </ul> </li> <li>2. Click <b>Install Webroot Enterprise</b> to start the installation. <ul style="list-style-type: none"> <li>• The Welcome window displays.</li> </ul> </li> </ol> | <ol style="list-style-type: none"> <li>1. Follow the instructions on the Web site to download the WebrootEnterpriseServerSetup.exe file.</li> <li>2. Go to where you downloaded the file. <ul style="list-style-type: none"> <li>• If you downloaded the file to your Windows Desktop, close all open programs, and you will see an icon on your desktop for the file you downloaded.</li> <li>• If you downloaded the file to a different location, use Windows Explorer to navigate to the file.</li> </ul> </li> <li>3. Double-click WebrootEnterpriseServerSetup.exe. <ul style="list-style-type: none"> <li>• The Welcome window displays.</li> </ul> </li> </ol> |





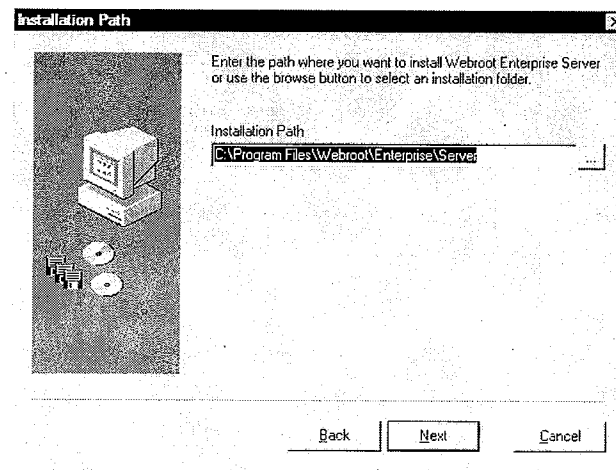
3. Click Next.

- The Software License Agreement window displays.



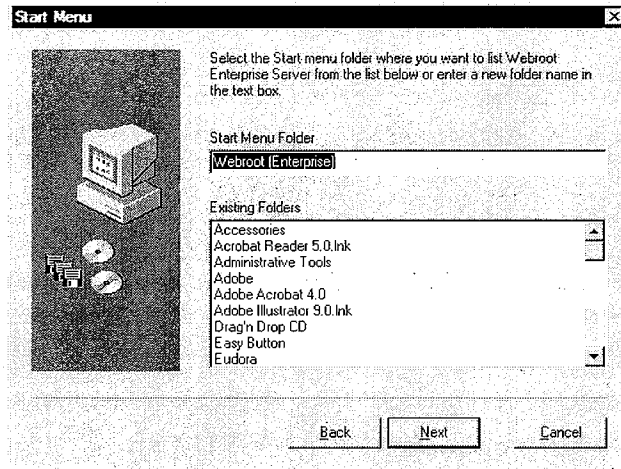
4. Read the license agreement and click Yes if you agree with the content.

- The Installation Path window displays showing you the default installation location.



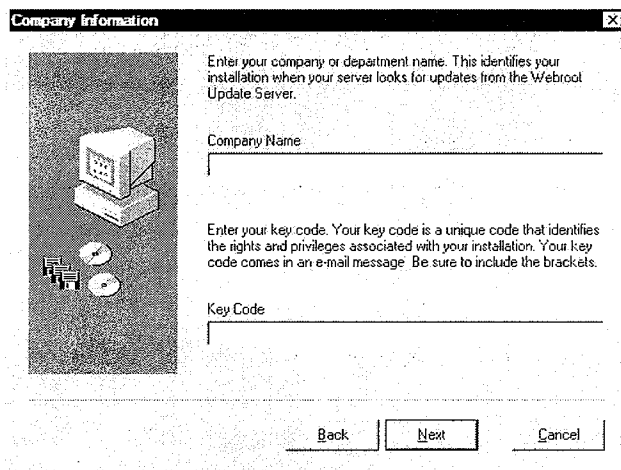
5. Click **Next**.

- If you want to install to a different location, click **browse** and navigate to the new location.
- The Start Menu window displays showing the default Start menu folder.



6. Click **Next**.

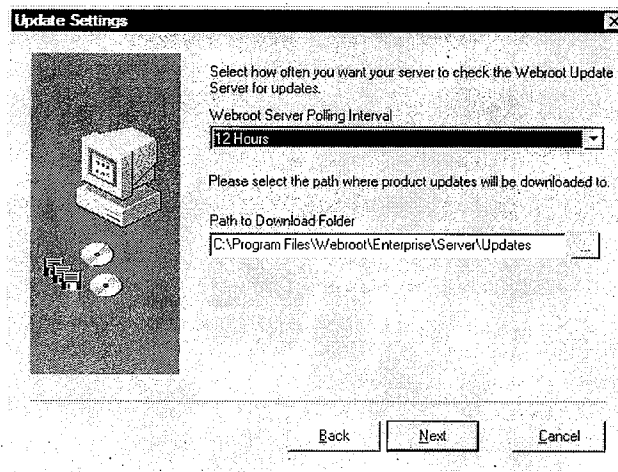
- If you want to use a different Start menu folder, enter a new name or select an existing group.
- The Company Information window displays.



7. Enter the information and click **Next**.

|              |   |
|--------------|---|
| Company Name | Name of your company. This identifies your Webroot Enterprise product when your company server looks for updates from the Webroot Update Server.  |
| Key Code     | Unique code that identifies the rights and privileges associated with your installation, such as the number of licenses you have purchased for each client workstation application.<br><br>Your key code comes in an e-mail message. Be sure to include the braces. |

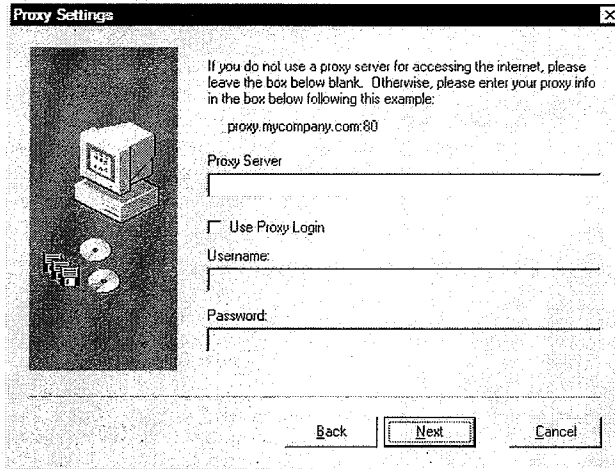
- The Update Settings window displays.



8. Enter or select the information and click **Next**.

|                                 |  |
|---------------------------------|--|
| Webroot Server Polling Interval | Select how often you want your server to check the Webroot Update Server for updates.  |
| Path to Download Folder.        | Path to the folder where your company server stores the updates it downloads from the Webroot Update Server. For best performance, use a folder on the same server. It can also be a folder on any drive your company server can access. |

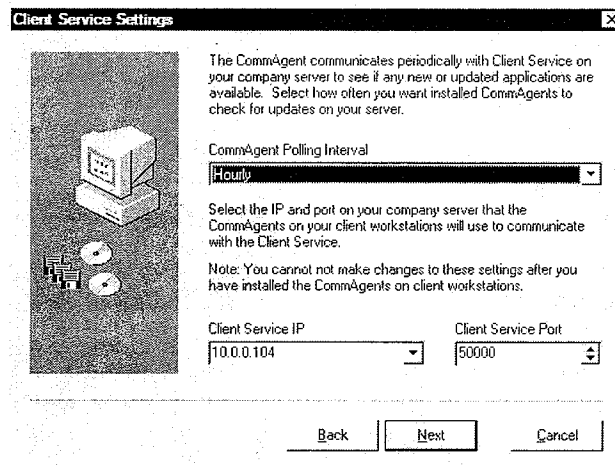
- The Proxy Settings window displays.



9. Enter or select the information and click **Next**.

|                 |  |
|-----------------|--|
| Proxy Server    | If you use a proxy server to access the Internet, enter your proxy server name or IP address and port number in one of the following formats: <ul style="list-style-type: none"> <li>• server_name.company.com:80</li> <li>• 10.0.0.1:80</li> </ul> If you do not use a proxy server, leave the field blank. |
| Use Proxy Login | If you use a proxy server that requires authentication, select this option.  |
| Proxy Username  | If you use a proxy server that requires authentication, enter your proxy server username.  |
| Proxy Password  | If you use a proxy server that requires authentication, enter your proxy server password.  |

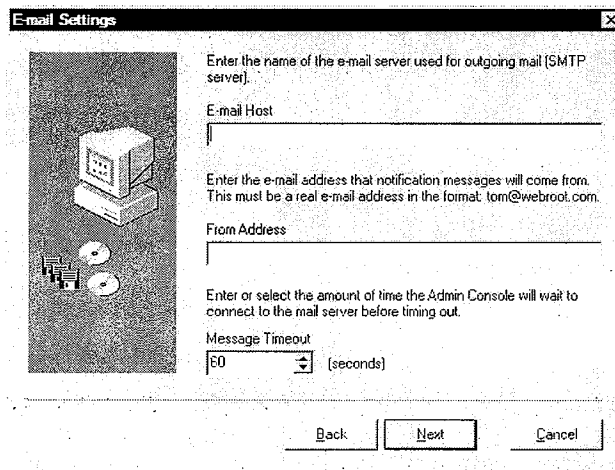
- The Client Service Settings window displays.



10. Enter or select the information and click **Next**.

|                            |   |
|----------------------------|---|
| CommAgent Polling Interval | How often you want installed CommAgents on each client workstation to check for updates on your server.   |
| Client Service IP          | Enter the IP address or host name that the client workstations will use to communicate with your company server. For IP resolution, select the IP address of the network interface card (NIC) visible to client workstations. For host name resolution, enter the fully qualified domain name of your server (requires a properly configured DNS environment).<br><br>After installation you cannot edit this value directly from the Admin Console. If you need to change this setting, contact technical support. |
| Client Service Port        | Port on your company server that the Client Service will use to communicate with your client workstations. The default port is 50000. Be sure that the port you use is not used to communicate with another system.<br><br>After installation you cannot edit this value directly from the Admin Console. If you need to change this setting, contact technical support.  |

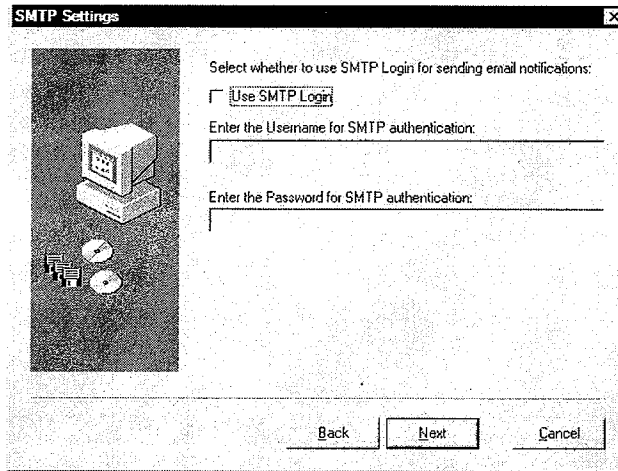
- The E-mail Settings window displays.



11. Enter or select the information and click **Next**.

|                 |   |
|-----------------|---|
| E-mail Host     | Fully qualified domain name for your e-mail server used for outgoing mail (SMTP server). If you do not have this information, enter NA and edit the information from the Admin Console. |
| From Address    | E-mail address that notification messages will come from. Must be a real e-mail address in the format: tom@webroot.com.   |
| Message Timeout | Amount of time the Admin Console will wait to connect to the mail server before timing out.   |

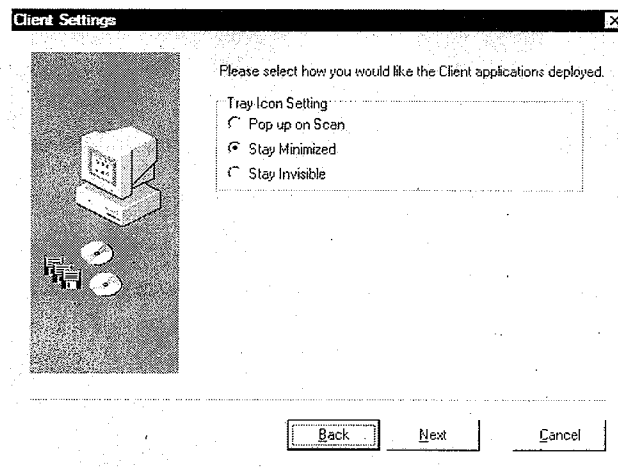
- The SMTP Settings window displays.



12. Enter or select the information and click **Next**.

|                   |   |
|-------------------|---|
| Use SMTP Login    | If you use a secure SMTP e-mail server, select this option and enter the username and password below. |
| Username for SMTP | Name needed to log in to a secure SMTP server.  |
| Password for SMTP | Password needed to log in to a secure SMTP server.  |

- The Client Settings window displays.

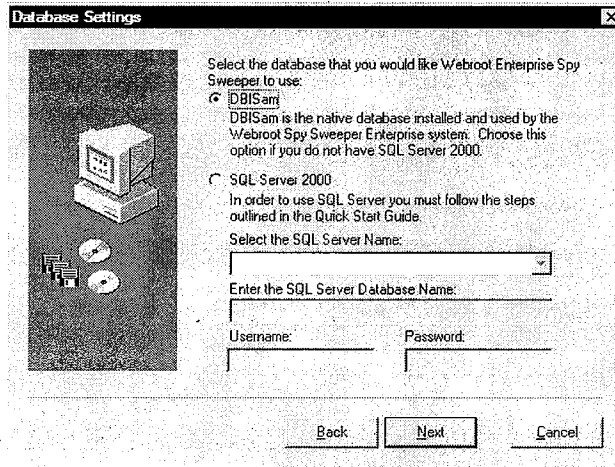


13. Enter or select the information and click **Next**.

|                   |  |
|-------------------|--|
| Tray Icon Setting | Select how you want Spy Sweeper to appear on client workstations. You can change this setting from the Admin Console by selecting <b>Manage Desktop Applications &gt; Spy Sweeper &gt; Configure Spy Sweeper &gt; Sweep Settings</b> . |
| Pop up on Scan    | Displays a system tray icon that end users can double-click to display the Spy Sweeper window and automatically pops up the window whenever a sweep starts, whether scheduled or using Sweep Now.                                      |

|                |  |
|----------------|--|
| Stay Minimized | Default and recommended setting. Displays a system tray icon that end users can double-click to display the Spy Sweeper window, but does <i>not</i> pop up the window whenever a sweep starts. From this interface, end users can start their own sweeps and adjust any allowable settings. When a sweep is running, the tray icon will animate to show that Spy Sweeper is sweeping their system. |
| Stay Invisible | Does not display a system tray icon and does not do anything when a sweep starts. End users have <i>no</i> access to the Spy Sweeper window to use options that are set as editable in the Admin Console.  |

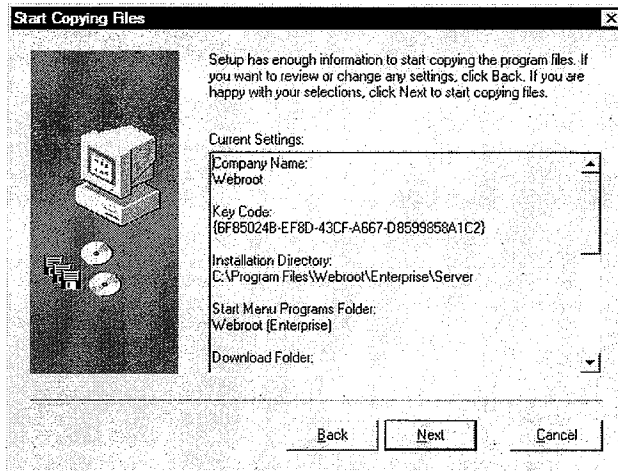
- The Database Settings window displays.



14. Enter or select the information and click **Next**.

|                                |  |
|--------------------------------|--|
| DBISam                         | Select this option only if you have fewer than 10,000 client workstations. You cannot change this selection later.   |
| SQL Server 2000                | Select this option only if you have SQL Server 2000 and you have over 10,000 client workstations. You cannot change this selection later.<br><br>The Select the SQL Server 2000 drop-down list takes a moment to populate with the list of SQL servers in your environment. Select the SQL server where you set up the database. |
| SQL Server Database Name field | Enter the name of your SQL Server database. You must already have the database and a system DSN set up.  |
| User Name and Password fields  | Enter the user name and password for your SQL Server. Be sure they are correct.  |

- The Start Copying window displays showing you the current settings.



15. Click **Next**.

- Webroot Enterprise Server installs and automatically starts the Client Service and Update Service.
- A message displays telling you to set up your client workstations.

16. Click **Finish**.

- Webroot Enterprise Server updates automatically when necessary.

You are now ready to set up one or more client workstations and distributor servers (if needed). For more information, see “Setting Up Client Workstations” on page 20 and “Installing and Assigning Distributor Servers” on page 23.

## Setting Up Client Workstations

---

After you install the Webroot Enterprise Server, you must set up one or more client workstations. This setup installs two components on each client workstation:

- **CommAgent**—communicates periodically with your company server to see if any new or updated applications are available. The CommAgent also updates its settings based on the current server settings in the Admin Console each time it communicates with the company server.
- **Spy Sweeper**—protects your computers from spyware.

You can install these components using any of the following methods:

- Going to each individual workstation and executing one of the following:
  - For Windows 2000 and XP execute the `SpySweeperSetup.msi` file.
    - Make sure that all five of the client installation files (`instnlsi.exe`, `instmsiw.exe`, `SpySweeperSetup.exe`, `SpySweeperSetup.ini`, and `SpySweeperSetup.msi`) are in the same folder whenever `SpySweeperSetup.msi` executes. Typically, these files are in the `C:\Program Files\Webroot\Enterprise\Server\Client` folder of the system where you installed Webroot Enterprise Server.
    - The `SpySweeperSetup.ini` file contains the IP address and port of your company server and is needed for the client to install successfully.



- For Windows 98, 98SE, ME, or NT (with any Service Pack before 6) execute the SpySweeper.exe file.
  - This file installs Windows Installer 2.0, which is required for the client workstation installation, then installs the client components.
  - Make sure that all five of the client installation files (instmsi.exe, instmsiw.exe, SpySweeperSetup.exe, SpySweeperSetup.ini, and SpySweeperSetup.msi) are in the same folder whenever SpySweeper.exe executes. Typically, these files are in the C:\Program Files\Webroot\Enterprise\Server\Client folder of the system where you installed Webroot Enterprise Server.
- Using a logon script to execute one of the above files. Webroot has provided some example logon scripts that you can change to meet your needs. See “Example Logon Script” on page 22.
- Using Group Policies, if you use Active Directory. For more information, refer to <http://support.microsoft.com/default.aspx?kbid=314934> and <http://support.microsoft.com/?kbid=302430>.
- Including the Spy Sweeper client as part of an image installed on workstations.
  - Install Spy Sweeper on the target system you are intending to image. If you will be implementing multiple Admin Consoles, you need to create a separate image for clients managed under each console.
  - Stop the Webroot CommAgent service.
  - Remove the following registry key:  
HKEY\_LOCAL\_MACHINE\SOFTWARE\Webroot\Enterprise\CommAgent\guid
  - Create your image.

The SpySweeperSetup.msi client installation program defaults to visible installation where you see a progress bar and receive feedback when the installation is complete. For information about using different installation options, see “Client Installation Options” on page 22.

The CommAgents contact the Client Service on your company server, as displayed in the Client Service Port field in the Admin Console (**Admin Tasks > Settings**), to look for product updates. If updates are available, the CommAgents access the updates from the location defined in the Download Folder field in the Admin Console. During the first contact, the CommAgent also provides the name and MAC address of the client workstation. This lets you add the workstation to a group.

Once you set up the client workstations and they have polled the company server, you can add the workstations to groups to control settings based on groups. Client workstations poll the company server at random intervals within five minutes of installation. For more information, see “Chapter 3, Setting Up the Webroot Enterprise Server” on page 27.

## Client Installation Options

You can use the following options in your logon script when you set up client workstations:

- If you would like to use a silent installation, add the /q switch in the line that executes SpySweeperSetup.msi. The installation program defaults to visible installation where you see a progress bar and receive feedback when the installation is complete. The syntax is:
  - SpySweeperSetup.msi /q
- You can specify the server IP address and port in the command line instead of relying on the .ini file. The syntax is:
  - SpySweeperSetup.msi SERVERIP=10.10.10.10 SERVERPORT=50000

For a silent installation:

- SpySweeperSetup.msi /q SERVERIP=10.10.10.10 SERVERPORT=50000
- You can also pass the client deployment setting. This setting should go after the /q switch if you are using that:
  - Pop up on scan—RUN\_CLIENT\_AS=0
  - Stay minimized—RUN\_CLIENT\_AS=1
  - Stay invisible—RUN\_CLIENT\_AS=2

The syntax is:

- SpySweeperSetup.msi /q RUN\_CLIENT\_AS=1 SERVERIP=10.10.10.10 SERVERPORT=50000
- You can apply any of these command line arguments to the SpySweeperSetup.exe installer (which is used for installing on systems lacking the 2.0 version of Windows Installer). The syntax is:
  - SpySweeperSetup.exe /q RUN\_CLIENT\_AS=1 SERVERIP=10.10.10.10 SERVERPORT=50000

## Example Logon Script

Below is an example logon script. You have to adjust it for your setup and network environment.

You have to put the script on your domain controllers or logon servers, then assign it so that it executes when a workstation logs in to your network. This script assumes that you have a shared drive on your network that contains the SpySweeperSetup.msi and SpySweeperSetup.ini files.

Typically, these files are in the C:\Program Files\Webroot\Enterprise\Server\Client folder of the system where the Webroot Enterprise Server has been installed. Copy the client files to the network share of your choice, then adjust the script to meet your share path. Also be sure to give all workstations read and execute access to the share.

```
@echo off
REM Check to see if clients are installed on the local machine, if they
REM are then display a confirmation
REM message otherwise install the client package and display a message
REM Check to see if the Enterprise CommAgent is installed, if not go to
REM install otherwise go to check
if exist "C:\Program Files\Webroot\Enterprise\Spy
Sweeper\SpySweeper.exe"
```

```

goto check if not exist "C:\Program Files\Webroot\Enterprise\Spy
Sweeper\SpySweeper.exe"
goto install
REM Check to see if Enterprise Spy Sweeper is installed, if not go to
install otherwise go to loaded
:check if exist "C:\Program Files\Webroot\Enterprise\Spy
Sweeper\SpySweeperTray.exe"
goto loaded if not exist "C:\Program Files\Webroot\Enterprise\Spy
Sweeper\SpySweeperTray.exe"
goto install
REM Display an install message, execute the client setup package from a
shared network drive and then go to end
:install echo Loading Webroot Enterprise Clients...
"C:\Program Files\Webroot\Enterprise\Server\Client\SpySweeperSetup.msi"
goto end
REM If the clients are already installed then display the following
message
:loaded echo Webroot Enterprise Clients are already Installed
:end

```

## Uninstalling Spy Sweeper from Client Workstations

You can uninstall Spy Sweeper from client workstation using Add/Remove Programs. The uninstall process requires access to the SpySweeperSetup.msi file and will look for it in the location from which it was originally run. You need to leave the SpySweeperSetup.msi file in a place that will be available in the future unless you want to prevent users from uninstalling the client.



### Note

The uninstallation process permanently deletes all spyware that was quarantined on the client workstation.

---

## Installing and Assigning Distributor Servers

By default, the Distributor service is installed with Webroot Enterprise Server on your company server. This acts as a single distributor server.

If you need to add distributor servers, you can install the distributor server software on one or more of your servers. For information about determining whether you need distributor servers, see "Planning for Webroot Enterprise Deployment" on page 5.

Installations with 500 or fewer client workstations typically do not need to install additional distributor servers.



You must complete the following tasks to install and use distributor servers:

1. Install the distributor server software. (See page 24.)
2. Assign distributor servers. (See page 24.)

## Installing Distributor Servers

The distributor server installation installs and starts the Distributor service (WebrootUpdateDistributor.exe).



To install distributor servers:

1. Execute the WebrootDistributorSetup.exe file on the server you want to be a distributor server.
  - The file is typically in the C:\Program Files\Webroot\Enterprise\Server\Distributor folder of the system where you installed Webroot Enterprise Server.
2. Follow the on-screen instructions.
  - You can now assign distributor servers.

## Assigning Distributor Servers

After you install the distributor server on your servers, you must assign those servers to groups.

You can assign a distributor server to one or more groups or to the whole company. For example, if you set up four distributor servers and assign them all to the whole company, the system randomly selects the order of distributors it sends back to the client workstations.

For a complete description of the how the update process works, see "How Webroot Enterprise Updates Work" on page 7.

This process spreads the load across the servers to ensure that the servers are not overwhelmed with update requests.



To assign a distributor server:

1. Select **Start > Programs > Webroot (Enterprise) > Admin Console**.
  - The Admin Console window displays, showing the News panel. The News panel includes information of interest to system administrators about spyware.
2. Select **Admin Tasks > Assign Distributors**.
  - The Assign Distributors panel displays, with a list of all existing groups on the left side.
3. Click **Add New Distributor**.
  - The Add Distributor window displays.
4. Enter a name for the distributor server.
  - If you enter the real name of a server on your network, the IP address automatically populates when you tab to the second field.
5. If necessary, enter the IP address of the server.
6. Click **OK**.
  - The server name now displays in the list on the right side of the panel.

7. Drag a server from the list to a group or to the company in the group tree.
  - To remove a server assignment, select the server in the group tree and click **Unassign Distributor**.
  - To update the status of the distributors, click **Refresh**.
  - To remove the selected distributors from their assignments and from the list of distributors, click **Remove Distributors**, then click **Apply Changes**.
8. Click **Apply Changes**.
  - Your company server will automatically send copies of all updates to all distributors. You still need to assign updates manually (from **Spy Sweeper >Update Spy Sweeper >Manual Install**) or set automatic installation rules (from **Spy Sweeper >Update Spy Sweeper >Auto Install**) to determine which updates should be applied to which clients.

## Changing the Distributor Server Port

The default port that a distributor server listens to is port 8080. If you need to change a distributor server to listen on a different port, you can do so.



To change the distributor server port:

1. On the distributor server, create a backup copy of the following file:  
C:\Program Files\Webroot\Enterprise\Distributor\etc\jetty.xml
2. Edit the original jetty.xml file with Notepad or another text editor.
3. Change the jetty.port attribute inside the addListener block from the default port of 8080 to the new port.
4. Restart the Webroot Update Distributor service.
  - To restart the Webroot Update Distributor service, select **Start > Control Panel > Administrative Tools > Services**. Select the Webroot Update Distributor service and click the **Restart the service** link in the upper-left corner of the window.

# Understanding the Admin Console Window

The Admin Console window lets you set up, manage, and monitor Webroot Enterprise functions and applications. Figure 5 shows the window and describes its parts.

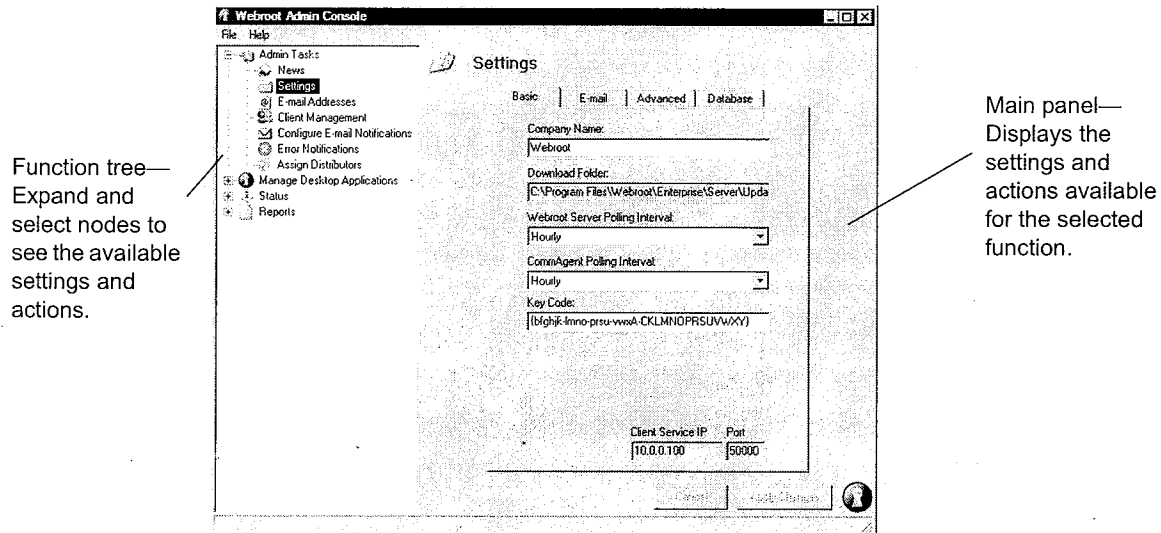


Figure 5: Admin Console window

# 3: Setting Up the Webroot Enterprise Server

---

You can perform the following tasks to complete the setup of the Webroot Enterprise Server:

- Access the Admin Console and view news (see page 27)
- Edit the server settings (see page 27)
- Set up notification (see page 30)
- Manage client workstations (see page 32)
- Assign distributor servers (see page 24)
- Filter information (see page 35)

## Accessing the Admin Console and Viewing News

---

The Admin Console is where you set up, manage, and monitor Webroot Enterprise updates and applications.

Webroot maintains a Webroot Spy Sweeper Enterprise news page that contains information about current version numbers and general spyware news. It also contains links to notes about updates and current documentation.

To access the Admin Console and view news:

1. Select **Start > Programs > Webroot (Enterprise) > Admin Console**.
  - The Admin Console window displays, showing the News panel. The News panel includes information of interest to system administrators about spyware.
2. Select **Admin Tasks > News**.
3. Click **Update News**.

## Editing the Server Settings

---

You entered your server settings during the installation process. These settings provide information to each Spy Sweeper client about the frequency and address for contacting your company server.

Below are important notes about the server settings:

- Client workstations will only get updates and setting changes when the CommAgent polls your company server. Any updates you make here (or elsewhere) will be applied after the polling interval has passed. For example, if your polling interval is every hour and your last client heartbeat was 30 minutes ago, changes you make will be applied 30 minutes from now.

- If you need to be sure that all clients receive updates or setting changes immediately, you can use the **Poll Now** button in the Client Management panel, however, you should use this option selectively to ensure that you do not overwhelm your network and servers.
- You cannot edit the Client Service Port. Contact Webroot Technical Support if you need to change this after installation.
- Updates for the Webroot Enterprise Server, including the Admin Console, download and install automatically whenever your company server contacts the Webroot Update Server.
- Updates for the Spy Sweeper program and definitions download whenever your company server contacts the Webroot Update Server, but they do *not* install automatically. You must either manually install them (see “Installing Updates Manually” on page 46) or set up automatic installation (see “Installing Updates Automatically” on page 47).



To edit the server settings:

1. From the Admin Console function tree, select **Admin Tasks > Settings**.
  - The Settings panel displays, with three tabs of settings you can view and edit.
2. Enter information into each field.

| Field                           | Description   |
|---------------------------------|---|
| Basic tab                       |   |
| Company Name                    | Name of your company. This identifies your Webroot Enterprise product when your server looks for updates from the Webroot Update Server.  |
| Download Folder                 | Path to the folder where your company server stores the updates it downloads from the Webroot Update Server. Typically, this is a folder on your company server. It can also be a folder on any drive your company server can access.                               |
| Webroot Server Polling Interval | How often you want your server to check for updates on the Webroot Update Server. If you select Manual, you must manually check for updates from <b>Status &gt; Update History</b> , then click <b>Check for Updates</b> .  |
| CommAgent Polling Interval      | How often you want installed CommAgents on each client workstation to check for updates on your server. If you change this, each CommAgent will retrieve the new setting the next time it contacts the server.  |
| Key Code                        | Unique code that identifies the rights and privileges associated with your installation, such as the number of licenses you have purchased for each client workstation application.<br><br>Your key code comes in an e-mail message. Be sure to include the braces. |



| Field                       | Description  |
|-----------------------------|--|
| Client Service IP           | <p>Enter the IP address or host name that the client workstations will use to communicate with your company server. For IP resolution, select the IP address of the network interface card (NIC) visible to client workstations. For host name resolution, enter the fully qualified domain name of your server (requires a properly configured DNS environment).</p> <p>After installation you cannot edit this value directly from the Admin Console. If you need to change this setting, contact technical support.</p> |
| Port                        | <p>Port on your company server that the Client Service will use to communicate with your client workstations. The default port is 50000. Be sure that the port you use is not used to communicate with another system.</p> <p>After installation you cannot edit this value directly from the Admin Console. If you need to change this setting, contact technical support.</p>  |
| E-mail tab                  |  |
| E-mail Host                 | Fully qualified domain name for your e-mail server used for outgoing mail (SMTP server).   |
| From Address                | E-mail address that notification messages will come from. Must be a real e-mail address in the format: tom@webroot.com.  |
| Message Timeout             | Amount of time the Admin Console will wait to connect to the mail server before timing out.  |
| Use SMTP Login              | If you use a secure SMTP e-mail server, select this option and enter the Login Name and Login Password below.  |
| Login Name                  | Name needed to log in to a secure SMTP server.   |
| Login Password              | Password needed to log in to a secure SMTP server.   |
| Send Test E-mail            | Select an e-mail address from the drop-down list and click <b>Send Test E-mail</b> . All e-mail addresses entered into <b>Admin Tasks &gt; E-mail Addresses</b> are listed in the drop-down list. You can also enter an e-mail address to test it before adding it.  |
| Advanced tab                |  |
| Proxy Server                | <p>If you use a proxy server to access the Internet, enter your proxy server name or IP address and port number in one of the following formats:</p> <ul style="list-style-type: none"> <li>• server_name.company.com:80</li> <li>• 10.0.0.1:80</li> </ul> <p>If you do not use a proxy server, leave the field blank.</p>   |
| Proxy Username              | If you use a proxy server that requires authentication, enter your proxy server username.  |
| Proxy Password              | If you use a proxy server that requires authentication, enter your proxy server password.  |
| Min Initial Retry (Seconds) | <p>Minimum time a rejected client workstation should wait before trying to connect again.</p> <p>The actual retry time is a randomly generated time between the minimum and maximum. If the client workstation is rejected again, it doubles the retry time. A rejected client continues to double the retry time until it connects successfully or until it reaches the final retry time. It then continues at the final retry interval until it is successful.</p>   |

| Field                       | Description   |
|-----------------------------|---|
| Max Initial Retry (Seconds) | Maximum time a rejected client workstation should wait before trying to connect again. The actual retry time will be between the minimum and maximum, as described above.   |
| Final Retry (Seconds)       | Amount of time between retries after the client has been rejected several times. The rejected client continues to retry to connect at this interval until it is successful. |
| Database tab                | You cannot change the type of database after installation. The information in this tab is read-only.  |

3. Click **Apply Changes**.

## Setting Up Notification

---

You can set up the following for the messages that the Webroot Enterprise Server sends to notify you of various events such as the availability of product updates:

- E-mail addresses to use for notification (see page 30)
- E-mail message content (see page 31)
- Error notification (see page 31)
- Update notification (see page 48)

### Setting Up Notification E-mail Addresses

You can set up e-mail addresses that the Webroot Enterprise Server uses to notify you of various events such as the availability of product updates.



To set up notification e-mail addresses:

1. From the Admin Console function tree, select **Admin Tasks > E-mail Addresses**.
  - The E-mail Addresses panel displays.
2. Click **+** to add a new row to the table.
3. Enter the information into the row.
4. Click **✓** to save the row.
5. Click **Apply Changes**.

## Setting Up Notification Messages

You can set up the messages that Webroot Enterprise Server sends for the following types of events:

- Availability of updates to the Webroot Enterprise Server or client workstation components
- Detected spyware
- Errors that occur on client workstations



To set up notification e-mail messages:

1. From the Admin Console function tree, select **Admin Tasks > Configure E-mail Notifications**.
  - The Configure E-mail Notifications panel displays.
2. Click the tab for the type of message you want to set up.
3. Enter the E-mail Subject you want to use for this type of message.
  - The field is already populated with example text that you can keep or edit.
4. Enter the message text you want for this type of message.
  - The field is already populated with example text that you can keep or edit.
  - For information that will vary, select an option from the Merge Fields drop down list and click **Insert**. Each event will contain information to fill in these merge fields (variables) with content appropriate to the event.
5. Click **Apply Changes**.

## Setting Up Error Notification

You can configure who receives notification of different types of errors that come from your client workstations.



To set up error notification:

1. From the Admin Console function tree, select **Admin Tasks > Error Notifications**.
  - The Error Notifications panel displays with a list of all e-mail addresses you have entered for notification and the alert categories of increasing scope.
2. Drag a name from the list to an alert category.
  - To move an e-mail address from one category to another, drag it from the current category and drop it onto another category.
  - To receive all error messages, move the e-mail address to the Errors, Warnings & Info category.
3. Click **Apply Changes**.

# Managing Clients

---

You can manage client workstations and perform the following functions from the Admin Console:

- Manage groups (see page 32)
- Create and export client reports (see page 33)
- Poll client workstations now (see page 34)
- Delete client workstations (see page 34)

## Managing Groups

You can set up groups to help administer the Webroot product updates and settings. You then add individual workstations to each group. Every workstation where you have installed the Spy Sweeper client is available to add to a group.

You can administer the following by group:

- Which applications to install on client workstations
- Which updates to install on client workstations
- Specific settings for each application

You might use groups to distinguish between different types of users. For example, you could have a group that includes all system administrators and use this group to test new products and product updates before distributing them throughout the company. You can also use groups to distinguish between departments or any other category you choose.

You can also filter the client workstation list to make it easier to create and manage groups. For more information, see "Filtering Information" on page 35.



To set up groups:

1. From the Admin Console function tree, select **Admin Tasks > Client Management**.
  - The Client Management panel displays, with a list of all existing groups on the left side.
  - To see all client workstations that have the Spy Sweeper client installed, click the top (company) node of the group tree.
  - To see fewer client workstations in the list, use the filter options. For more information, see "Filtering Information" on page 35.
2. Click **Add Group**.
  - You can also right-click anywhere in the group tree and select **Add Group**.
  - The New Group window displays.
3. Enter a group name.
4. Click **OK**.
  - The group name now displays in the group tree on the left side of the panel.

5. Drag a workstation from the list to a group in the group tree.
  - To move a workstation from group to another, drag it from the current group and drop it onto another group.
  - To delete a group, move all workstations in the group to another group, select the group you want to delete, and click **Delete Group**.
  - To delete a workstation from a group, select the group, then select the workstation and click **Delete Selected Workstations**. After the workstation contacts the company server the next time, the workstation will return to the list on the right side of the panel when you click the company name.
6. Click **Apply Changes**.

## Creating and Exporting Client Reports

Using the filter on the Client Management panel, you can create various reports. For example, you can filter based on the last heartbeat date, application version, or definition version. If you want to save a report as file, you can export it as a comma separated (CSV) file.



To create and export client reports:

1. From the Admin Console function tree, select **Admin Tasks > Client Management**.
  - The Client Management panel displays with a list of all existing groups on the left side.
  - To see all client workstations that have the Spy Sweeper client installed, click the top (company) node of the group tree.
2. Click the group that includes the workstation you want to report on.
3. Use the filter options to display the information you want in your report.
  - For more information, see “Filtering Information” on page 35.
4. Select the workstations you want to include in the report.
  - You can select more than one workstation by using **Ctrl** or **Shift** as you select workstations.
5. Click **Export Selected Workstations to File**.
  - You can also right-click the selected workstations and select **Export Selected Workstations to File**.
  - The Save Workstations to File window displays.
6. Select where you want to save the file and enter a file name.
7. Click **Save**.

## Polling Client Workstations Now

You can poll one or more client workstations from the Client Management panel. You can use this if you see some client workstations have not polled for a period of time and you want to see if they are still out there. You can also use it if you have changed some settings, such as assigning program or definition updates, and you want client workstation to receive those updates immediately.



### Note

Use this option selectively to ensure that you do not overwhelm your network and servers with a large number of client workstations requesting updates at the same time.

---



To poll client workstations now:

1. From the Admin Console function tree, select **Admin Tasks > Client Management**.
  - The Client Management panel displays with a list of all existing groups on the left side.
  - To see all client workstations that have the Spy Sweeper client installed, click the top (company) node of the group tree.
2. Click the group that includes the client workstation you want to poll.
3. Select the client workstation you want to poll.
  - You can select more than one workstation by using **Ctrl** or **Shift** as you select workstations.
4. Click **Poll Now**.
  - You can also right-click the selected workstations and select **Poll Now**.
  - The poll starts on the selected client workstations. A confirmation message displays, with the number of workstations the system sent the polling message to.
  - To check the status of the polling, click **Refresh** and filter on the heartbeat or by definition updates to see that client workstations have updated.

## Deleting Client Workstations

If you find that a client workstation has not had a heartbeat for a long time or you know that the workstation no longer exists, you can delete the workstation from the database. If the client workstation reconnects to the network and contacts your company server, all functions will work properly.



To delete client workstations:

1. From the Admin Console function tree, select **Admin Tasks > Client Management**.
  - The Client Management panel displays with a list of all existing groups on the left side.
  - To see all client workstations that have the Spy Sweeper client installed, click the top (company) node of the group tree.

2. Click the group that includes the client workstation you want to delete.
3. Select the client workstation you want to delete.
  - You can select more than one workstation by using **Ctrl** or **Shift** as you select workstations.
4. Click **Delete Selected Workstations**.
  - You can also right-click the selected workstations and select **Delete Selected Workstations**.
  - The system removes the workstation from the list.
5. Click **Apply Changes**.
  - The system deletes the workstation from its database.

## Filtering Information

---

On some Admin Console panels, you can filter the information to display only the information that meets your filter criteria. For example, on the Client Management panel, you can limit the number of workstations displayed by filtering on the workstation name, IP address, last heartbeat date, last sweep date, and application version.

You can also group information by one or more column headings.

The filtering options work the same way, regardless of which panel you are working on. You know that the filter options are available when the column headings on the right side of the panel are drop-down lists. For example, in the Client Management panel (**Admin Tasks > Client Management**), you can see that the column headings look like drop-down lists.



To filter information:

1. From a panel that has the filter options, select the drop-down list from one column heading.
  - The drop-down list contains the following options:
    - {All}—Use this to view all rows in the table.
    - {Custom}—Use this to filter based on the information contained in the current column.
    - Each item currently listed in the selected column—Use this to view just one row of the table.
2. Select **{Custom}**.
  - The Custom Filter window displays.
3. From the first drop-down list, select how you want to match your filter criteria.
4. In the field next to drop-down list, enter the information you want to filter on.
  - For example, in the Client Management panel, you can filter based on the current Defs Version field, select equals, then enter the current definition version number.
5. If you want to add more filter criteria, select AND or OR, select how you want to match the second set of criteria, and enter information to filter on.

6. Click **OK**.

- The information in the panel changes to display only those workstations that meet your filter criteria.
- At the bottom of the panel, a gray bar displays that lets you do the following:
  - Close the gray bar—Click the x.
  - Turn off the filter temporarily—Select the check box to toggle the current filter on and off.
  - Edit or save the filter and open other filters—Click **Customize** to see these additional filter options.



To group information:

1. From a panel that has the filter options, drag a table heading to the gray area above the table.
  - For example, in the Client Management panel, click a group, then drag the App Version field to the gray area.
2. Click the plus sign next to the column heading in the table to see the information that matches the heading content.
  - Continuing the example above, click the plus sign next to each occurrence of App Version in the table to see all client workstations in the current group that have the same version of the application.



# 4: Managing Spy Sweeper

---

Spy Sweeper lets you protect your end users' privacy and your company's computers from a variety of spyware including those that monitor all computer activities (system monitors) and those that can steal or destroy data (Trojan horses). It also detects spyware that pops up ads on your computer (adware) and cookies that may contain personal information (tracking cookies).

You can set up and perform the following Spy Sweeper functions from the Admin Console:

- Manage spyware (see page 37)
- Configure sweeps (see page 41)
- Run sweeps (see page 44)
- Update Spy Sweeper (see page 46)
- View a summary of detected spyware (see page 49)

As a system administrator, you can also unlock functions at a client workstation and customize the Spy Sweeper settings for an end user. For more information see "Unlocking Functions at a Client Workstation" on page 49.

## Managing Spyware

---

You can manage spyware for client workstations in the following ways:

- Set up automatic handling of spyware found (see page 37)
- Set up continuous monitoring of certain spyware activities (see page 39)

## Setting Up Automatic Spyware Handling

By default, Spy Sweeper quarantines detected spyware for 30 days. You can change this default behavior for client workstations in the following ways:

- By setting up exceptions for spyware by type
  - You can set up Spy Sweeper to automatically handle detected spyware based on the spyware type. Spy Sweeper can automatically do one of the following for each spyware type:
    - Log only, don't quarantine (default)
    - Quarantine, delete after 2 days
    - Quarantine, delete after 7 days
    - Quarantine, delete after 30 days
    - Don't quarantine, delete right away

- By setting up exceptions for specific spyware to keep or to restore already quarantined spyware
  - To override the default spyware handling for each spyware type, you can set specific spyware to keep. You may want to use this option if your end users have specific spyware on their computers that they need to keep to make another program run properly.
  - Spy Sweeper must detect the spyware on at least one client workstation before you can set Spy Sweeper to keep it.
  - Setting a specific spyware to keep also restores that spyware from quarantine if it has already been detected and quarantined.



**Note**

The settings here override the settings for each spyware type.

---

You can set up automatic spyware handling by group or for the whole company.



**Note**

We recommend creating settings at the company level first, then determining what settings, if any, should be different by group.

---



To set up automatic spyware handling:

1. From the Admin Console function tree, select **Manage Desktop Applications > Spy Sweeper > Manage Spyware > Detected Spyware**.
  - The Detected Spyware panel displays with a list of each spyware type.
2. From the group tree, select the group you want to set up.
  - If you want this setting to apply to the whole company, select the company at the top of the group tree.
3. For each spyware type, select how you want Spy Sweeper to handle it.
  - To see more information about a specific spyware item, select it in the Found Spy List and review the description at the bottom of the panel.
4. For any spyware you want to always keep, move the spyware from the Found Spy List to the Always Keep/Restore from Quarantine list.
  - The Found Spy List includes each spyware instance that Spy Sweeper has found on a workstation in the company.
  - Moving spyware to the Always Keep/Restore from Quarantine list restores any already quarantined instances of the spyware on the next sweep.
5. Click **Apply Changes**.
  - Spy Sweeper will now automatically handle each spyware type based on your selections. It will also always keep the spyware in the Always Keep/Restore from Quarantine list for the selected group when it runs sweeps.

- To change the settings for one group to be the same as the settings for the whole company, select the group in the group tree and click **Apply Company Settings**, then click **Apply Changes**.

## Setting Up Continuous Monitoring: Active Shields

You can set up Spy Sweeper to continuously monitor several common spyware-related activities. We call these settings “shields.” You can set up continuous monitoring options by group or for the whole company.



### Note

We recommend creating settings at the company level first, then determining what settings, if any, should be different by group.



To set up continuous monitoring:

1. From the Admin Console function tree, select **Manage Desktop Applications > Spy Sweeper > Manage Spyware > Active Shields**.
  - The Active Shields panel displays with the continuous monitoring (Active Shields) options.
2. From the group tree, select the group you want to set up.
  - If you want these settings to apply to the whole company, select the company at the top of the group tree.
  - The tabs in the Active Shields panel show the current settings for the selected group or for the company.
3. Select each option you want.

| Option                               | Description  |
|--------------------------------------|--|
| Standard tab                         |  |
| Memory Shield<br>On                  | Sweeps memory frequently looking for spyware.  |
| Startup Shield<br>On                 | Actively watches startup items for any changes. Some spyware will add startup items, so that the spyware will always start. This shield ensures that spyware does not add something to the startup items, but also effectively prevents end users from installing software. Be sure that your users do not need to install new software before selecting this shield.  |
| Messenger<br>Shield On               | (Applies only to Windows NT, 2000, and XP.) This option turns off and actively watches the Microsoft Messenger Service. This service is not an instant messaging program and does not affect your use of instant messaging. This service is often used for sending spam and creating pop-up ads. Turning off the service stops these types of spam and pop-ups.<br><br>If you use this service to broadcast information to your users, do not turn on this shield. |
| Messenger<br>Service Startup<br>Type | If you turn the Messenger Shield off, after having turned it on, this option controls the state of the Messenger Service Startup Type when the Messenger Shield is off.  |

| Option  | Description  |
|---|--|
| Leave the Messenger Service Running when Messenger Shield Is Turned Off | If you turn the Messenger Shield off, after having turned it on, this option controls the status of the Messenger Service when the Messenger Shield is off.  |
| Internet Explorer tab   |  |
| Tracking Cookie Shield On   | Actively watches for tracking cookies as you visit Web sites and removes them. Tracking cookies are cookies that can track your Web activities. These <i>may</i> include cookies that contain user names, passwords, or similar information that you enter on some Web sites.  |
| IE Hijack Shield On   | Actively protects various Internet Explorer functions, such as the search page, error pages, and other default pages that Internet Explorer displays. Some spyware changes (“hijacks”) these pages without letting you know. Whenever spyware tries to change these pages, Spy Sweeper blocks the change.  |
| Hosts File Shield On  | This option actively watches the Hosts file for any changes. Some spyware will add or change the IP address for a Web site in the Hosts file. When you try to go to the added or changed Web site, you will really go to a different Web site, such as an advertising site. This shield ensures that spyware does not change an IP address in the Hosts file.<br><br>If end users are permitted to edit the Hosts file, do not turn this shield on.  |
| Keep Hosts File Read-only   | If you turn the Hosts File Shield off, after having turned it on, this option controls the state of the Hosts file when the Hosts File Shield is off.  |
| IE Home Page Shield On  | Watches for any changes to the home page that you set in Internet Explorer. The home page is the Web site that displays automatically when you start Internet Explorer or when you click the <b>Home</b> button.<br><br>When you enable this shield, the home page you enter will replace the end user’s existing home page. End users will only be able to change their home page through the <b>Options &gt;Active Shields</b> panel in Spy Sweeper. If the Tray Icon Setting ( <b>Manage Desktop Applications &gt; Spy Sweeper &gt; Configure Spy Sweeper &gt; Sweep Settings</b> ) is set to Stay Invisible, end users will not be able to change their home page. |
| Protected Home Page   | Enter the Web address of the Web site you want as your home page in the format:<br>http://www.webroot.com  |

| Option                             | Description  |
|------------------------------------|--|
| Blocked Applications/Web Sites tab |  |
| Blocked Websites Shield On         | <p>Adds a list of suggested sites to block to your Hosts file and sets the IP address for those sites to the IP address for your computer. This blocks banner and other advertising from these sites. When you go to a Web site that has advertising from one of the blocked sites, you may see a small graphic that indicates a broken link to a graphic (typically a red x in a box). This just shows where the blocked ad would display.</p> <p>To add your own sites, enter the Web site address and click <b>Add</b>.</p> |
| Spy Installation Shield On         | <p>Actively watches for known spyware that tries to install itself on your computer. Whenever known spyware tries to install itself, Spy Sweeper stops the installation.</p> <p>You can also add executable file names to the list that will stop the file from executing when a user tries to start a specific program. For example, you could add a file sharing program that you do not want to let company personnel use. To add a program, enter the file name in the text box and click <b>Add</b>.</p>                  |

4. If you want end users to be able to change a setting, select the User Editable option.
5. Click **Apply Changes**.
  - Spy Sweeper will now continuously monitor the settings you selected.
  - To change the settings for one group to be the same as the settings for the whole company, select the group in the group tree and click **Apply Company Settings**, then click **Apply Changes**.

## Configuring Sweeps

---

You can configure the following settings related to spyware sweeps:

- Sweep settings (what to sweep) (see page 41)
- Alerts related to found spyware (see page 43)

## Configuring Sweep Settings

You can configure settings that control how Spy Sweeper sweeps client workstations looking for spyware. You can also set up a password to unlock functions at a client workstation. For more information, see "Unlocking Functions at a Client Workstation" on page 49.

You can configure sweep settings by group or for the whole company.



### Note

We recommend creating settings at the company level first, then determining what settings, if any, should be different by group.

---



To configure sweep settings:

1. From the Admin Console function tree, select **Manage Desktop Applications > Spy Sweeper > Configure Spy Sweeper > Sweep Settings**.
  - The Sweep Settings panel displays with available sweep options.
2. From the group tree, select the group you want to set up.
  - If you want these settings to apply to the whole company, select the company at the top of the group tree.
  - The settings in the Sweep Settings panel show the current settings for the selected group or for the company.
3. Select each option you want.

| Option                               | Description   |
|--------------------------------------|---|
| Drives to Sweep                      | Select the drives you want Spy Sweeper to sweep. Typically, most spyware installs on the C: drive, but you should sweep all hard drives periodically.   |
| Skip Files Larger Than               | If you know that you have very large files that you do not want Spy Sweeper to sweep, select this option and enter a file size in kilobytes. For example, you may want to use this option if you have large graphics or video files on your computer that you created and you know do not contain spyware. This will save time during sweeps. Typically, spyware files are small. |
| Sweep Memory                         | Select this option to have Spy Sweeper sweep your computer's memory for spyware. Typically, you want to sweep memory each time you run a sweep. Spyware commonly loads into memory.   |
| Sweep Registry                       | Select this option to have Spy Sweeper sweep your computer's registry for spyware. Typically, you want to sweep the registry each time you run a sweep. Spyware commonly creates entries in your computer's registry.   |
| Sweep Only Known Spyware Folders     | Select this option to make the sweep run faster. When you use this option, Spy Sweeper only looks in the folders where spyware files are typically found. Using this option performs a less thorough sweep. You should periodically sweep all folders.  |
| Sweep All Folders on Selected Drives | Select this option to have Spy Sweeper look in all folders on the drives you select to sweep. This type of sweep will take longer to run. Using this option performs a more thorough sweep.   |
| Allow Users to Cancel Sweeps         | Select this option to permit end users to stop a sweep, regardless of how the sweep was started.  |

| Option            | Description  |
|-------------------|--|
| Tray Icon Setting | Select how you want Spy Sweeper to appear on client workstations.  |
| Pop up on Scan    | Displays a system tray icon that end users can double-click to display the Spy Sweeper window and automatically pops up the window whenever a sweep starts, whether scheduled or using Sweep Now.  |
| Stay Minimized    | Default and recommended setting. Displays a system tray icon that end users can double-click to display the Spy Sweeper window, but does <i>not</i> pop up the window whenever a sweep starts. From this interface, end users can start their own sweeps and adjust any allowable settings. When a sweep is running, the tray icon will animate to show that Spy Sweeper is sweeping their system. |
| Stay Invisible    | Does not display a system tray icon and does not do anything when a sweep starts. End users have no access to the Spy Sweeper window to use options that are set as editable in the Admin Console.   |
| Password          | Enter a password that lets system administrators access and change Spy Sweeper settings when you are working at a client workstation. For more information, see "Unlocking Functions at a Client Workstation" on page 49.  |

4. If you want end users to be able to change a setting, select the User Editable option.
5. Click **Apply Changes**.
  - Spy Sweeper will use these options when running sweeps.
  - To change the settings for one group to be the same as the settings for the whole company, select the group in the group tree and click **Apply Company Settings**, then click **Apply Changes**.

## Setting Up Sweep Alerts

You set Spy Sweeper to send e-mail alerts to specific people when it detects different types of spyware. Before you can set up e-mail alerts, you must enter one or more notification recipients. For more information, see "Setting Up Notification E-mail Addresses" on page 30.



To set up sweep alerts:

1. From the Admin Console function tree, select **Manage Desktop Applications > Spy Sweeper > Configure Spy Sweeper > Alert Notifications**.
  - The Alert Notifications panel displays with the available alert types and notification recipients.
2. Drag the name of a notification recipient to the alert tree.
  - To move a recipient to different alert type, drag it from the current type and drop it onto another type.
3. Click **Apply Changes**.
  - Spy Sweeper will use these settings to send alerts when it detects spyware.

# Running Sweeps

---

You can run sweeps the following ways:

- Run a sweep now (see page 44)
- Schedule sweeps (see page 45)

You can also view and stop sweeps that are running. For more information, see “Viewing and Stopping Sweeps” on page 46.

## Running a Sweep Now

You can run a sweep on one or more client workstations when you learn about a critical spyware threat. The sweep will use the current sweep settings. If you want to change the settings, make the changes first and wait for the next polling interval to ensure that client workstations receive the new settings. For more information about changing sweep settings, see “Configuring Sweep Settings” on page 41.

The Sweep Now function uses port 50001 to communicate with client workstations. You cannot edit this setting.



### Note

Running a sweep during business hours may slow performance for each affected client workstation.

You can start a sweep now from either the Sweep Now panel or the Client Management panel.



To run a sweep now:

| From the Sweep Now panel   | From the Client Management panel  |
|--|---|
| <ol style="list-style-type: none"><li>1. From the Admin Console function tree, select <b>Manage Desktop Applications &gt; Spy Sweeper &gt; Manage Spyware &gt; Sweep Now</b>.<ul style="list-style-type: none"><li>• The Sweep Now panel displays.</li></ul></li><li>2. Select the group or client workstation where you want to run the sweep.<ul style="list-style-type: none"><li>• If you want to run the sweep on all client workstations in the company, select the company at the top of the group tree.</li></ul></li><li>3. Click <b>Sweep Now</b>.<ul style="list-style-type: none"><li>• To cancel a sweep that is running, select the group or client workstation where you want to stop the sweep and click <b>Cancel Sweeps in Progress</b>.</li></ul></li></ol> | <ol style="list-style-type: none"><li>1. From the Admin Console function tree, select <b>Admin Tasks &gt; Client Management</b>.<ul style="list-style-type: none"><li>• The Client Management panel displays with a list of all existing groups on the left side.</li></ul></li><li>2. Select the group or client workstation where you want to run the sweep.<ul style="list-style-type: none"><li>• You can select more than one client workstation by using <b>Ctrl</b> or <b>Shift</b> as you select workstations.</li><li>• If you want to run the sweep on all client workstations in the company, select the company at the top of the group tree.</li></ul></li><li>3. Right-click the client workstations you want and select <b>Sweep Now</b>.<ul style="list-style-type: none"><li>• The sweep starts on the selected client workstations.</li><li>• To check the status of the sweeps, go to <b>Manage Desktop Applications &gt; Manage Spyware &gt; Sweep Now</b> and click the group that the workstations belong to.</li></ul></li></ol> |



## Scheduling Sweeps

You can schedule sweeps to run on one or more specific days at a specific time.

You can schedule sweeps by group or for the whole company. Below are some things to consider when setting up scheduled sweeps:

- Avoid scheduling sweeps at the same time as anti-virus scans.
- Schedule different groups to sweep at different times to reduce load on the company server when clients report their results.
- You can schedule Windows NT, 2000, XP, and 2003 clients to sweep during off-hours as long as the system remains powered on (even with the user logged out). For Windows 98, 98SE, and ME systems, the user will need to be logged in to execute a scheduled sweep. You need to let users know when their sweep is scheduled to make sure they leave their computer in the proper state for the sweep to run.
- Spy Sweeper will sometimes indicate that other processes on the system are using the hard disk by flashing a red message. Spy Sweeper intelligently throttles its disk usage to allow users to access the disk but will continue through the sweep even if there are repeated interruptions.



To run schedule sweeps:

1. From the Admin Console function tree, select **Manage Desktop Applications > Spy Sweeper > Run Sweeps > Schedule Sweeps**.
  - The Schedule Sweeps panel displays.
2. Select the group or client workstation where you want to schedule the sweep.
  - If you want these settings to apply to the whole company, select the company at the top of the group tree.
  - The settings in the Schedule Sweeps panel show the current settings for the selected group or for the company.
3. If you want end users to be able to change these settings, select the User Editable option.



### Note

We do not recommend making the schedule options user editable.

4. Select the day of the week and the time you want to run the sweep.
  - The time uses military time (24-hour clock).
5. If you want to sweep only known spyware folders at Windows startup or shutdown, select the option you want at the bottom of the panel.
  - These options only scan known spyware folders, so the sweep runs quickly. Using one of these options helps to ensure that sweeps are run periodically, even if the computer is turned off when regular sweeps are scheduled.
6. Click **Apply Changes**.
  - To change the settings for one group to be the same as the settings for the whole company, select the group in the group tree and click **Apply Company Settings**, then click **Apply Changes**.

## Viewing and Stopping Sweeps

You can view sweeps that are running. You can also stop sweeps, regardless of how you or an end user started the sweep.



To view and stop sweeps:

1. From the Admin Console function tree, select **Manage Desktop Applications > Spy Sweeper > Manage Spyware > Sweep Now**.
  - The Sweep Now panel displays, with information about sweeps that are running.
2. Select a group to see which workstations in that group are currently running sweeps.
3. To cancel a sweep that is running, select the group or client workstation where you want to stop the sweep and click **Cancel Sweeps in Progress**.

## Updating Spy Sweeper

---

Updates for the Spy Sweeper program and definitions download whenever your company server contacts the Webroot Update Server, but they do *not* install automatically. You must either manually install them or set up automatic installation.

You can set up and do the following related to the distribution of Spy Sweeper updates:

- Install updates manually (see page 46)
- Install updates automatically (see page 47)
- Set up notification (see page 48)
- Set up updating for mobile end users (see page 48)

## Installing Updates Manually

You can install updates manually whenever you receive notification of an update. For information about setting up notification, see “Setting Up Update Notification” on page 48.

You may want to use manual updates for major and minor updates as well as bug fixes and new products. This gives you the chance to install these updates on a few client workstations to see how they work before deploying them to many users.

You can manually install updates by group or for the whole company.



### Note

We recommend creating settings at the company level first, then determining what settings, if any, should be different by group.

---



To install updates manually:

1. From the Admin Console function tree, select **Manage Desktop Applications > Spy Sweeper > Update Spy Sweeper > Manual Install**.
  - The Manual Install panel displays with the available updates and group tree.

2. Drag an update to a group in the group tree.
  - To install the update on all client workstations in the company, drag the update to the company name at the top of the group tree.
3. Repeat step 2 for each update and group you want to install.
4. Click **Apply Changes**.
  - The next time each client workstation contacts the company server, it will install the update.

## Installing Updates Automatically

You can setup Spy Sweeper to automatically install updates when your company receives them from the Webroot Update Server. The automatic settings only apply to updates received *after* you change these settings. You must manually install any updates that you received before you set up the automatic installation.

We suggest that definitions be set to automatically install. You want to keep your definitions as up to date as possible and automatically installing them assures that all users will have the most recent definitions.



### Note

We recommend setting *only* definitions to install automatically. Install other update types manually.

---

You can set up automatic update installation by group or for the whole company.

---



### Note

We recommend creating settings at the company level first, then determining what settings, if any, should be different by group.

---



To install updates automatically:

1. From the Admin Console function tree, select **Manage Desktop Applications > Spy Sweeper > Update Spy Sweeper > Auto Install**.
  - The Auto Install panel displays with the types updates and group tree.
2. Drag an update type to a group in the group tree.
  - To set the update type to automatically install on all client workstations in the company, drag the update type to the company name at the top of the group tree.
3. Repeat step 2 for each update type and group.
4. Click **Apply Changes**.
  - The next time each client workstation contacts the company server, it will install any available updates set to install automatically.

## Setting Up Update Notification

You can set up e-mail notification for Spy Sweeper updates. Whenever an update arrives from the Webroot Update Server, the Admin Console can send an e-mail message to one or more people. Before you can set up notification, you must enter one or more notification recipients. For more information, see “Setting Up Notification E-mail Addresses” on page 30.



To set up notification for Spy Sweeper updates:

1. From the Admin Console function tree, select **Manage Desktop Applications > Spy Sweeper > Update Spy Sweeper > Update Notifications**.
  - The Update Notifications panel displays with a list of the types of updates and available e-mail notification recipients.
2. Drag the name of an e-mail recipient to the update tree.
  - To move a recipient to different update type, delete it from the current type and add it to another type using the buttons.
3. Click **Apply Changes**.

## Setting up Updating for Mobile End Users

If you have end users who use laptops and travel a lot, you can let them receive Spy Sweeper definition updates directly from Webroot.



### Note

Be sure that the Tray Icon Setting is set to Stay Minimized (recommended) or Pop Up on Scan, or end users will not be able to display the Spy Sweeper main window.



To set up updating for mobile end users:

1. From the Admin Console function tree, select **Manage Desktop Applications > Spy Sweeper > Configure Spy Sweeper > Sweep Settings**.
  - The Sweep Settings panel displays with the types updates and group tree.
2. Select the group or client workstation where you want to change the mobile update setting.
  - If you want these settings to apply to the whole company, select the company at the top of the group tree.
3. Select the Enable Mobile Client Support option.
4. Click **Apply Changes**.
  - The next time each client workstation contacts the company server, it will update Spy Sweeper and make visible the **Update Spy Definitions** button on the Spy Sweeper main window. Whenever end users have an Internet connect, they can use the button to retrieve definition updates. The button is not available for use if a user downloaded updated definitions within the last six hours.

## Viewing a Summary of Detected Spyware

---

You can view a summary of the spyware that Spy Sweeper has detected on client workstations throughout the company either by group or by spyware type.



To view a summary of detected spyware:

1. From the Admin Console function tree, select **Status > Product Summaries > Spy Sweeper**.
  - The Spy Sweeper panel displays with the group tree and spyware type tree.
2. Select a group, client workstation, or spyware type to see where spyware was found.

## Unlocking Functions at a Client Workstation

---

As a system administrator, you can unlock functions at a client workstation and customize the Spy Sweeper settings for an end user. Unlocking functions requires a password that you set in the Admin Console. By default, there is no password set up. You must set up the password before you can unlock functions at an end user's client workstation. For information about setting the password, see the Password option in step 3 of "Configuring Sweep Settings" on page 41.

After you set up the password, you can go to an end user's workstation and unlock functions.



### Note

If the Tray Icon Setting in the Admin Console is set to Stay Invisible, you cannot access the Spy Sweeper interface at all from a client workstation. For information about changing this setting, see the Tray Icon Setting option in step 3 of "Configuring Sweep Settings" on page 41.



To unlock functions at a client workstation:

1. At a client workstation, double-click the Spy Sweeper icon in the system tray.
  - The Spy Sweeper window displays.
2. Press **Ctrl+Alt+p**.
  - The Admin Password window displays.
3. Enter the password you set up in the Admin Console.
4. Click **OK**.
  - Now all functions that are not normally available to end users are available. These include Always Keep and Always Remove, as well as other functions that are not set up as user editable in the Admin Console. Refer to the Spy Sweeper online help for more information about using these functions.
5. After you customize the settings as needed, press **Ctrl+Alt+p** to lock the functions again.





# 5: Monitoring Status

---

You can monitor the status of Webroot Enterprise in the following ways:

- View update history and installed applications (see page 51)
- View client status (see page 52)
- View errors (see page 52)
- Generate reports (see page 53)

## Viewing Update History and Installed Applications

---

You can view the following information about updates and installed applications:

- Update history—List of updates downloaded from the Webroot Update Server. (see page 51)
- Installed applications—List of applications installed by client workstation. (see page 51)

### Viewing Update History

You can view a history of when Webroot Enterprise Server and Spy Sweeper client updates were downloaded from the Webroot Update Server.



To view the update history:

- From the Admin Console function tree, select **Status > Update History**.
- The Update History panel displays with a list of all of the updates downloaded to date.

### Viewing Applications Installed by Workstation

You can view information about the applications installed and the version for each client workstation.



To view applications installed:

1. From the Admin Console function tree, select **Admin Tasks > Client Management**.
  - The Client Management panel displays with a list of all existing groups on the left side.
  - To see all client workstations that have the Spy Sweeper client installed, click the top (company) node of the group tree.

2. Select the group or client workstation whose application version you want to see.
  - You can select more than one client workstation by using **Ctrl** or **Shift** as you select workstations.
3. Use the filter or grouping option to organize the list by application update.
  - For more information, see “Filtering Information” on page 35.

## Viewing Client Status

---

You can view a list of each client workstation that has the Spy Sweeper client installed on it and when it last contacted the company server. The information also includes when Spy Sweeper last ran a sweep on the client workstation.



To view the client status:

- From the Admin Console function tree, select **Admin Tasks > Client Management**.
  - The Client Management panel displays with a list when each client workstation last contacted the company server.
  - To download any available updates, click **Check for Updates**.

## Viewing Errors

---

You can view any errors that an application generates on a client workstation. You can then report the error to Webroot.

You should review the error list periodically to determine if any applications have caused errors.



To view errors:

1. From the Admin Console function tree, select **Status > Errors**.
  - The Errors panel displays with a list errors.
2. Contact your Webroot Enterprise Support for assistance with the resolving the error.



# Generating Reports

---

You can generate the following types of reports:

- Error—Includes all errors from Spy Sweeper.
- Spyware—Includes details of the spyware found.



To generate reports:

1. From the Admin Console function tree, select **Reports** and the type of report you want.
2. From the group tree, select the group you want.
  - If you want the report to include the whole company, select the company name at the top of the group tree.
3. Select the date range you want the report to include.
4. Click **Preview/Print** to preview the report.
  - To save the report to any of several file formats, click **Print**, then select the Print to File option, Type, and Where to save the file.



# A: Webroot Enterprise Port Requirements

A number of communication ports must be opened for proper communications between all network components within the Webroot Enterprise architecture. Table 9 describes the port requirements for a Webroot Enterprise installation.

The aim of this information is not to document how to open all of these ports for a particular firewall, but rather to describe what ports must be open and on what systems within your Webroot Enterprise architecture.

Table 9: Webroot Enterprise communications ports

| Port  | Component  | Description  | Installation/network access requirement  |
|-------|--|--|--|
| 443   | WebrootUpdateService.exe<br>Required on Distributor Servers                    | <ul style="list-style-type: none"> <li>• HTTP protocol over SSL.</li> <li>• Communicates periodically with Webroot to retrieve updates and move them to distributor servers.</li> <li>• Runs as a system service on the server.</li> </ul> | <ul style="list-style-type: none"> <li>• Installed when you set up distributor servers.</li> <li>• Requires local network access.</li> </ul>                                   |
| 8080  | WebrootUpdateDistributor.exe<br>Required on Distributor Servers                | <ul style="list-style-type: none"> <li>• Alternate HTTP. =</li> <li>• Responds to CommAgent on client workstations to distribute updates.</li> <li>• Runs as a system service on the server.</li> </ul>                                    | <ul style="list-style-type: none"> <li>• Installed when you set up distributor servers.</li> <li>• Requires local network access.</li> </ul>                                   |
| 50000 | WebrootClientService.exe<br>Required on company server and client workstations | <ul style="list-style-type: none"> <li>• Controls the communication between the client workstations and your company server.</li> </ul>  | <ul style="list-style-type: none"> <li>• Installed during the installation of Webroot Enterprise Server.</li> <li>• Requires local network access.</li> </ul>                  |
| 50001 | Sweep Now Function<br>Required on company server and client workstations       | <ul style="list-style-type: none"> <li>• Function initiated from the Admin Console that initiates a Spy Sweeper sweep of the selected client workstations.</li> </ul>  | <ul style="list-style-type: none"> <li>• Not an installed component, but a function called from within the Admin Console.</li> <li>• Requires local network access.</li> </ul> |
| 50002 | Poll Now Function<br>Required on company server and client workstations        | <ul style="list-style-type: none"> <li>• Function initiated from the Admin Console that initiates a poll of the selected client workstations to update their heartbeat and status to the server.</li> </ul>                                | <ul style="list-style-type: none"> <li>• Not an installed component, but a function called from within the Admin Console.</li> <li>• Requires local network access.</li> </ul> |



# B: Migrating an Existing Installation from DBISAM to SQL

---

If you have an existing Webroot Enterprise installation and need to migrate the database from DBISAM to SQL Server, you can do so.



## Note

You only need to migrate to SQL if you expect to install more than 10,000 clients.

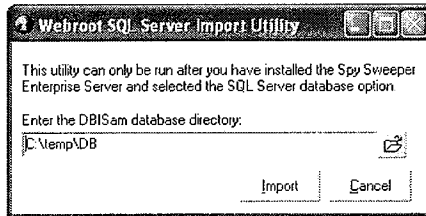
---



To migrate from DBISAM to SQL:

1. From your Webroot Enterprise company server, start the Admin Console and select **Help** > **About** to be sure that your installation has updated to version 2.0
  - You can only migrate to SQL if you have version 2.0 installed.
2. Stop the following Webroot Enterprise services:
  - Webroot Client Service
  - Webroot Update Service
3. Copy the DB folder to a temporary location.
  - If you installed the Webroot Enterprise Server to the default location, the DB folder is in the following location:
    - : C:\Program Files\Webroot\Enterprise\Server\
4. Uninstall the following Webroot Enterprise programs, in this order, using Add/Remove Programs:
  - Webroot Spy Sweeper Enterprise Client, if installed on the company server
  - Webroot Enterprise Server
  - Webroot Spy Sweeper Enterprise Distribution Server
5. Set up the SQL database.
  - For more information, see “Setting up a SQL Database” on page 9.
6. Install a new Webroot Enterprise Server, making sure you select the SQL Server 2000 option during the installation.
  - The full installation file for Webroot Enterprise Server 2.0 is available from the Supplemental Downloads page at: <http://www.webroot.com/entcenter>.
  - For more information, see “Installing Webroot Enterprise Server on Your Company Server” on page 11.

7. Start the import utility to bring the DBISAM database files into the SQL database.



- If you installed the Webroot Enterprise Server to the default location, the import utility is in the following location:
  - C:\Program Files\Webroot\Enterprise\Server\SSEImport.exe
- Depending on the size of the database being imported, the process can take from a few seconds to several minutes.
- On completion of the import, a confirmation message displays.

# Index

---

## A

- Active Shields, setting up 39
- Add Group button 32
- Admin Console
  - configuring server settings 27
  - defined 4
  - installing 4
  - starting 27
  - understanding 3
  - understanding the main window 26
  - updating 28
- Advanced tab 29
- alerts, setting up for sweeps 43
- Always Keep list 38
- applications
  - viewing errors from client workstations 52
  - viewing installed by group 51
  - viewing update history of 51
- assigning distributor servers 23, 24

## B

- Basic tab 28
- Blocked Websites Shield On option 41

## C

- canceling sweeps 46
- changing
  - the port for distributors servers 25
- Check for Updates button 28
- client components
  - example logon script 22
  - installation options 22
- client components, installing 20
- Client Service
  - defined 4
  - installing 4
- Client Service IP field 12, 17, 29
- Client Service Port field 11, 17
- client workstations
  - adding to groups 32
  - creating reports about 33
  - deleting 34
  - example logon script 22
  - options for setting up 22
  - polling now 34
  - removing from groups 32
  - setting up 20

- uninstalling Spy Sweeper from 23
- unlocking Spy Sweeper functions at 49
- viewing application errors from 52
- CommAgent Polling Interval field 17, 28
- CommAgents
  - defined 4
  - installation options 22
  - installing 4, 20
  - viewing heartbeat status of 52
  - viewing update history of 51
- Company Name field 15, 28
- configuration examples 5
- configuring sweeps 41
- continuous monitoring, setting up 39
- conventions, typographic 1
- creating
  - reports about client workstations 33
- customer support 2

## D

- database
  - migrating from DBISAM to SQL 57
  - setting up SQL 9
- Database tab 30
- database, recommendations about selecting type 5
- DBISAM option 19
- DBISAM, migrating from 57
- definitions
  - updating 46
  - updating automatically 47
  - updating for mobile end users 48
  - updating manually 46
- Delete Group button 33
- Delete Selected Workstations button 35
- Deleted Selected Workstations button 33
- deleting
  - client workstations 34
- distributor servers
  - assigning 23, 24
  - changing the default port for 25
  - how they work 5
  - installing 23, 24
  - recommendations about number to use 5
  - removing 24
  - unassigning 24
  - updating process 7
- distributors

- defined 4
  - installing 4
  - Download Folder field 11, 28
  - Drives to Sweep drop-down list 42
- E**
- E-mail Host field 11, 17, 29
  - E-mail tab 29
  - Enable Mobile Client Support option 48
  - errors
    - viewing for applications on client workstations 52
  - example logon script 22
  - Export Selected Workstations to File button 33
  - exporting reports about client workstations 33
- F**
- file, saving reports to 53
  - filtering information 35
  - Final Retry field 30
  - firewalls
    - configuring ports required for Webroot Enterprise 55
  - From Address field 11, 17, 29
- G**
- generating reports 53
  - grouping information 35
  - groups
    - deleting 32
    - renaming 32
    - setting up 32
    - viewing applications installed 51
- H**
- handling
    - spyware 37
    - spyware automatically 37
    - spyware automatically by type 37
  - heartbeat status, viewing for CommAgents 52
  - Hosts File Shield On options 40
- I**
- IE Hijack Shield On option 40
  - information, filtering 35
  - installing
    - client components 20
    - CommAgents 20
    - distributor servers 23, 24
    - example logon script 22
    - key steps for 8
    - options for client components 22
    - options for CommAgents 22
    - options for Spy Sweeper 22
    - Spy Sweeper 20
    - Webroot Enterprise 9
    - Webroot Enterprise Server 11
    - Internet Explorer Home Page Shield On option 40
- K**
- Keep Hosts File Read-only option 40
  - keeping spyware 38
  - Key Code field 11, 15, 28
- L**
- Leave the Messenger Service Running when Messenger Shield Is Turned Off 40
  - Login Name field 29
  - Login Password field 29
  - logon script example 22
- M**
- managing
    - Spy Sweeper 37
    - spyware 37
    - spyware automatically 37
    - spyware automatically by type 37
  - Max Initial Retry field 30
  - Memory Shield On option 39
  - Message Timeout field 17, 29
  - messages for notification, setting up 31
  - Messenger Service Startup Type option 39
  - Messenger Shield On option 39
  - migrating
    - from DBISAM to SQL 57
  - Min Initial Retry field 29
  - monitoring
    - status 51
- N**
- News, viewing 27
  - notification
    - setting up 30
    - setting up e-mail addresses for 30
    - setting up for errors 31
    - setting up for Spy Sweeper updates 48
    - setting up messages for 31
- P**
- Password field 43
  - Password for SMTP field 18
  - Path to Download Folder field 15
  - planning for Webroot Enterprise deployment 5
  - Poll Now button 34
  - polling
    - client workstations now 34
    - recommendations about setting frequency 5
  - Pop up on Scan option 18, 43
  - Port field 29
  - ports



- changing for distributor servers 25
- Webroot Enterprise requirements for 55
- Protected Home Page field 40
- Proxy Password field 12, 16, 29
- Proxy Server field 11, 16, 29
- Proxy Username field 11, 16, 29

## Q

- quarantined spyware, what happens during uninstallation 23

## R

- Refresh button 34
- removing distributor servers 24
- reports
  - creating related to client workstations 33
  - saving to a file 53
- reports, generating 53
- restoring spyware 38
- running
  - a sweep now 44
  - sweeps 44
  - sweeps on a schedule 45

## S

- saving reports to a file 53
- scheduling sweeps 45
- Send Test E-mail button 29
- server settings, configuring in the Admin Console 27
- setting
  - a SQL database 9
- setting sweep settings 41
- setting up
  - client workstations 20
  - continuous monitoring 39
  - error notification 31
  - groups 32
  - key steps for 8
  - notification 30
  - notification e-mail addresses 30
  - notification messages 31
  - options for client workstations 22
  - sweep alerts 43
- shields, setting up 39
- Skip Files Larger Than option 42
- sorting information 35
- Spy Installation Shield On option 41
- Spy Sweeper
  - defined 4
  - example logon script 22
  - installation options 22
  - installing 4, 20
  - managing 37
  - setting up notification about updates 48

- unlocking functions at a client workstation 49
- updating 46
  - updating automatically 47
  - updating definitions for mobile end users 48
  - updating manually 46
  - viewing a summary of detected spyware 49
  - viewing date of last sweep 52

## spyware

- handling automatically by type 37
- managing 37
  - managing automatically 37
  - restoring 38
  - setting up to always keep 38
  - viewing a summary of detected 49

## SQL

- migrating to 57
  - setting up database 9
- SQL Server 2000 option 19
- SQL Server Database Name field 19
- starting the Admin Console 27
- Startup Shield On option 39
- status
  - monitoring 51
- Stay Invisible option 19, 43
- Stay Minimized option 19, 43
- stopping sweeps 46
- support 2
- Sweep All Folders on Selected Drives option 42
- Sweep Memory option 42
- Sweep Now button 44
- Sweep Only Known Spyware Folders option 42
- Sweep Registry option 42
- sweeps
  - configuring 41
  - running 44
  - running now 44
  - scheduling 45
  - setting up alerts for 43
  - settings for 41
  - stopping 46
  - viewing those running 46
- sweeps, viewing last date of 52
- system requirements 2

## T

- technical support 2
- Tracking Cookie Shield On option 40
- Tray Icon Setting field 18
- Tray Icon Setting option 43
- typographic conventions 1

## U

- unassigning distributor servers 24
- uninstalling, Spy Sweeper 23

- unlocking, Spy Sweeper functions at a client workstation 49
- Update News button 27
- Update Service
  - defined 4
  - installing 4
- updates, viewing history of 51
- updating
  - definitions 46
  - definitions automatically 47
  - definitions for mobile end users 48
  - definitions manually 46
  - overview of for Webroot Enterprise 7
  - Spy Sweeper 46
  - Spy Sweeper automatically 47
  - Spy Sweeper manually 46
  - the Admin Console 28
  - Webroot Enterprise Server 28
- Use Proxy Login option 16
- Use SMTP Login option 18, 29
- User Editable option 41, 43
- Username and Password fields 19
- Username for STMP field 18

## V

- viewing
  - a summary of detected spyware 49

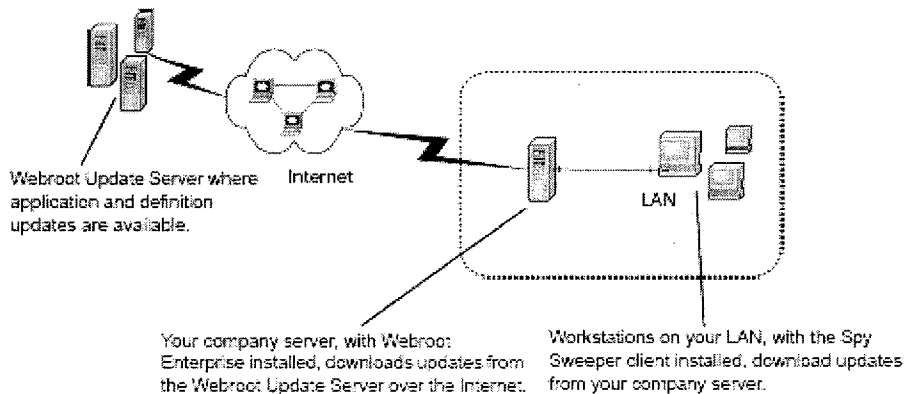
- applications installed by group 51
- heartbeat status of CommAgents 52
- News 27
- sweeps 46
- update history 51

## W

- Webroot Enterprise
  - architecture 3, 5
  - installing 9
  - key steps to installing and setting up 8
  - planning deployment of 5
  - port requirements 55
  - understanding 3
  - updating process described 7
- Webroot Enterprise Server
  - installing 11
  - updating 28
  - viewing update history of 51
- Webroot Server Polling Interval field 15, 28
- workstations
  - adding to groups 32
  - creating reports about 33
  - deleting 34
  - moving to a different group 32
  - polling now 34
  - removing from groups 32

## Webroot Spy Sweeper Enterprise Version 2.0 Quick Start Guide

This guide covers installation and initial configuration of Webroot Spy Sweeper Enterprise. Spy Sweeper Enterprise uses a client-server architecture as shown in the illustration. To successfully install the system, you will need to first install the server and then deploy the clients following the steps below.



### Planning Your Deployment

If you will be supporting more than 500 clients, please read the “Planning Your Installation” section of the System Administrator’s Guide (SAG) to determine appropriate installation and configuration options.

Once you have determined how you will deploy Spy Sweeper Enterprise in your environment, you are ready to begin setup. The six major steps in getting started are:

1. Gather information for server installation
2. Install server
3. Check for latest news and updates
4. Deploy initial clients
5. Setup initial sweeps and settings
6. Broader deployment

#### 1) Gather information for server installation

Before starting the server installation, please have the following information available:

- Your key code
- If you use a proxy server to access the internet, the proxy server name or IP address and port. If your proxy server requires authentication, please have a valid username and password.
- If you have multiple Network Interface Cards installed in your server, the IP address of one that clients on your internal network can contact or the fully qualified domain name of your server if all clients can access it by name.
- Name of your SMTP mail server (fully qualified domain name) and valid email account (for sending notification emails). If your SMTP server requires authentication, a valid username and password.

NOTE: You might want to use Microsoft SQL Server as your database if:

- You are supporting a large number of clients (see SAG for sizing guidelines)
- SQL Server is a standard or easier for you to support
- You want to perform custom queries or run reports against the database

If you will be using Microsoft SQL Server for your installation, you will need to create a database that uses SQL Server Authentication prior to running the installer. You will need the name of the database, the name of the server on which SQL Server is running, and the SQL Server authentication username and password. Detailed guidelines for using SQL Server are provided in the SAG.

## 2) Install server

Refer to System Administrator Guide for detailed installation instructions.

- While logged in with administrative privileges, run WebrootEnterpriseServerSetup.exe on the server you specify as the Webroot Spy Sweeper Enterprise Server.
- Key install notes:
  - Company Information
    - Please include the braces { } in your key code
  - Update Settings
    - Webroot releases updates approximately once per week, therefore polling the Webroot Server more than every 12 hours is typically not necessary.
    - Use an updates folder on the Webroot Enterprise Server
  - Proxy Settings
    - If unsure whether you have a proxy server, leave the proxy fields blank. This information may be edited from the Admin Console.
    - The proxy server field on the Update Service Settings page will pre-populate with a value if the installer detected proxy settings on your machine. Please confirm the format of Machine Name:Port or IP Address:Port before continuing.
  - Client Service Settings
    - Spy Sweeper Enterprise Clients will poll the server at the frequency you determine to receive new configuration information.
    - If you see multiple IP addresses in the Client Service IP box, please select one that can communicate with your internal network.
    - Type a fully qualified domain name (e.g. server.mycompany.com) in the Client Service IP box if you prefer to have the clients contact the server by name.
  - E-mail Settings
    - Use the mail server and e-mail address information from Step One.
    - If you don't know this information, type "NA" in the e-mail field to edit this from the Admin Console.
  - SMTP Settings
    - If you're unsure whether your mail server requires authentication, leave these fields blank. This information may be edited at a later time from the Admin Console.
  - Client Settings
    - This determines what end users will see on their screen. "Stay Minimized" is the recommended, default setting for deploying your test clients. In this mode, end users can display the client interface from the Spy Sweeper Enterprise tray icon. From this interface, they can start their own sweeps and adjust any allowable settings, as determined by the system administrator. When a sweep is running, the tray icon will animate to show that Spy Sweeper is checking their system.

- “Pop up on Scan” mode is similar to “Stay Minimized” with the exception that the entire Spy Sweeper Enterprise client pops up on their screen and shows the detailed sweep in progress.
- “Stay Invisible” mode is typically used to prevent all end user interaction with the client. In this mode, there is no tray icon and end users cannot see or change any settings (even if you make the settings editable in the Admin Console).
- Database
  - Detailed guides for selecting the right database are in the Sys Admin Guide. DBISAM (the default) is not recommended for implementations larger than 10,000 clients.

### 3) Check for News and Updates

After the Spy Sweeper Enterprise server installation, open the Admin Console to display the News page. Click *Update News* in the lower right corner to receive the most recent product information from Webroot.

Check for updates by clicking *Check for Updates* in the lower right corner of the Status -> Update History screen.

If updates are available, they will download automatically. You will see updates that can be assigned to clients in the Manage Desktop Applications -> Spy Sweeper -> Update Spy Sweeper -> Manual Install screen. Because clients haven't been deployed yet, you will not have any groups to assign updates. If an automatic update installation policy is defined in the Auto Install screen, that policy only applies to updates downloaded AFTER the policy is in place (all previous downloads need to be assigned through the Manual Install screen).

The Webroot Enterprise server that you have installed communicates across the internet to the Webroot Update server on port 443. If this port is blocked or if you have not configured proxy settings, you may need to contact support to troubleshoot.

### 4) Deploy initial clients

For a smooth installation, pick 5 to 10 client systems to represent your network environment for initial deployment. This step ensures there are no issues with client-server communication and gathers important information for broader deployment.

To protect the server on which you've deployed the Admin Console, you'll need to install the Spy Sweeper Enterprise Client on the same machine (the Admin Console does not perform any anti-spyware functions by itself). If you plan on protecting the server, install the client on this computer as part of the initial deployment.

To install the client on the server, run *SpySweeperSetup.msi* located in the following directory on the server: `C:\Program Files\Webroot\Enterprise\Server\Client`

Before installing any clients, access the Manage Desktop Applications -> Spy Sweeper -> Manage Spyware -> Detected Spyware screen and set all of the dispositions to “Log only, don't quarantine”. This prevents accidentally quarantining something during your initial steps. To make your initial test sweeps run quickly, you can also click *Sweep only Known Spyware folders* on the Manage Desktop Applications -> Spy Sweeper -> Configure Spy Sweeper -> Sweep Settings screen.

Client installation files are in the Client folder under Server (`C:\Program Files\Webroot\Enterprise\Server\Client` if you accepted the default during installation). The two most important files are *SpySweeperSetup.msi* and *SpySweeperSetup.ini*.

SpySweeperSetup.ini contains important information for SpySweeperSetup.msi to run correctly. Always keep the two files in the same folder to ensure the .msi executes properly.

If you have systems without Microsoft Windows Installer 2.0 (typically Windows 98, 98SE, ME, and Windows NT pre-Service Pack 6), you will need to use the SpySweeperSetup.exe install program found in the same folder. It is important to keep all five of the files in the Client folder together if you are using this installer.

For the initial deployment, it is recommended to share the C:\Program Files\Webroot\Enterprise\Server\Client folder and execute the installer from each of the target systems because updated SpySweeperSetup.msi files are automatically placed in this folder.

Spy Sweeper Client uninstall process requires access to the SpySweeperSetup.msi file and will look for it in the location from which it was originally run. You will need to leave the SpySweeperSetup.msi file in a place that will be available in the future unless you want to prevent users from uninstalling the client.

Refer to the final section of this document for more detailed information on client deployment.

Once clients are deployed, you will begin to see entries in the Admin Tasks -> Client Management screen. You can click *Refresh* on this screen to see recent updates. Clients delay for a random interval of up to five minutes after being installed before they poll the server.

Clients communicate to the server on the port you specified during the installation process (this defaults to 50000). If clients are blocked from outward communication, if there is a proxy server between the client and your Webroot Enterprise server, or if the computer on which you've installed the Webroot Enterprise server is blocking communication on this port, clients may not be able successfully communicate with the server. This will result in the client never appearing in the Admin Console.

For the Sweep Now function, the server communicates with the clients on port 50001. If this port is blocked on either end or if there is a proxy server between the client and your Webroot Enterprise server, you may see a Pending status on the Sweep Now screen and will be unable to send a sweep command or see that status of sweeps.

#### 5) Initial sweeps and settings

From the Manage Desktop Applications -> Spy Sweeper -> Manage Spyware -> Sweep Now select your test systems and initiate the sweep. Alternatively, start sweeps from clients directly or by scheduling a sweep from the Admin Console.

The client sweep results return to the server. From the Admin Console, go to the Manage Desktop Applications -> Spy Sweeper -> Manage Spyware -> Detected Spyware screen and review *Found Spy List*. If your company uses any of the programs listed, move them to the "Always Keep / Restore from Quarantine" column. To create your Found Spies list, you should run thorough scans (select "Sweep all folders on selected drive" on the Manage Desktop Applications -> Spy Sweeper -> Configure Spy Sweeper -> Sweep Settings screen) of several machines with the detected spyware dispositions set at "Log only, don't quarantine". Cydoor p2p, Cdilla, and Backweb are the programs that most frequently have some valid use in an enterprise.

To finish, set the dispositions on the Manage Desktop Applications -> Spy Sweeper -> Manage Spyware -> Detected Spyware screen to one of the quarantine options, sweep again, and verify that the systems are still operating as expected. This validates that no programs needed have been quarantined.

## 6) Broader deployment

The basic steps for completing deployment are:

- Install additional distributor servers and/or Enterprise Servers if necessary (see Planning Your Installation in the SAG)
- Deploy Spy Sweeper Enterprise clients company-wide
- Create groups and adjust settings

There are four options for deploying the client broadly:

- Execute the install from each workstation (e.g. by placing SpySweeperSetup.msi and SpySweeperSetup.ini in a shared folder and requesting each end user double-click SpySweeperSetup.msi)
  - If you choose this option, users must have local administration authority on their systems
- Execute the install from a logon script
  - If you want the install to be silent, use a "/q" switch in the line that executes SpySweeperSetup.msi
  - You can specify the server IP address and port in the command line instead of relying on the .ini file  
The command line syntax is:  
SpySweeperSetup.msi SERVERIP=10.10.10.10 SERVERPORT=50000  
For a silent install:  
SpySweeperSetup.msi /q SERVERIP=10.10.10.10  
SERVERPORT=50000
  - You can also pass the client deployment setting (invisible, stay minimized, pop up) in the command line. The command line argument is RUN\_CLIENT\_AS=0 (pop up on scan) RUN\_CLIENT\_AS=1 (stay minimized) RUN\_CLIENT\_AS=2 (stay invisible). This setting should go after the "/q" switch if you are using that:  
The command line syntax is:  
SpySweeperSetup.msi /q RUN\_CLIENT\_AS=1 SERVERIP=10.10.10.10  
SERVERPORT=50000
  - Finally, you can apply any of these command line arguments to the SpySweeperSetup.exe installer (which is used for installing on systems lacking the 2.0 version of Windows Installer)  
The command line syntax is:  
SpySweeperSetup.exe /q RUN\_CLIENT\_AS=1 SERVERIP=10.10.10.10  
SERVERPORT=50000
  - Example login script syntax is provided in the SAG
- Assign the software through a Group Policy Object in Active Directory
  - NOTE: Group Policy software installation is only supported as assignment by computer (versus assigning or publishing to users).
  - This link provides an overview of Group Policy Software installation  
<http://support.microsoft.com/default.aspx?kbid=314934>
  - The link below provides detail on deploying to only a selected Group through Group Policy assignment  
<http://support.microsoft.com/?kbid=302430>
- Include the Spy Sweeper Client as part of an image installed on systems
  - Install the Spy Sweeper Client on the target system you are intending to image – if you will be implementing multiple Admin Consoles, you'll need to create a separate image for clients managed under each console
  - Stop the Webroot CommAgent service
  - Remove the following registry key:  
HKEY\_LOCAL\_MACHINE\SOFTWARE\Webroot\Enterprise\CommAgent\guid
  - Create your image

Once clients poll, put them into groups on the Admin Tasks -> Client Management screen. Then go through the Manage Desktop Applications -> Spy Sweeper panel to adjust any Enterprise or Group settings.

Consider the following items when enabling Active Shields:

- Spy Installation shield
  - This shield operates at a low level to detect spies attempting to install and prevents the installation. If you detect issues with other software running on your systems when this shield is activated, please notify Webroot support.
- Home page shield
  - The URL you specify will replace the user's existing home page
  - If you have deployed the client in "Invisible" mode, users will not be able to change their home page. This can only be done through the Spy Sweeper Enterprise client once this shield is turned on.
- Tracking Cookies, Memory and Spy Installation shields
  - These shields stop spies and cookies on the system, but do not create report entries (you will see results when a sweep is run and the spies are logged, quarantined, or deleted).
- Hosts file shield
  - This prevents any changes to the hosts file. If users are allowed to edit this file, do not turn on the shield.
- Blocked Sites shield
  - This creates hosts file entries that prevent access to the web sites you specify. The pre-populated list includes sites that have distributed spyware or potentially unwanted programs.
- IE Hijack shield
  - Users should not notice effects of this shield unless they are attempting to modify internal pages on Internet Explorer, which is not common
- Startup shield
  - This shield prevents changes or additions to startup items which effectively prevents users from installing software (as well as stopping spies). If users are allowed to install software, you should typically not turn on this shield.
- Messenger shield
  - This shield disables Windows Messenger service. If you use this service to broadcast to your users, do not turn on the shield. If you turn this shield on and subsequently turn it off, you will need to turn on this service on the target systems as a separate action. Spy Sweeper does not automatically turn on this service after the shield has been disabled as it can be a security issue that administrators should consider carefully.

Three items to consider when creating your sweep schedules:

- Avoid scheduling sweeps at the same time as anti-virus scans.
- Schedule different groups to sweep at different times to reduce load on the server when clients report their results.
- You can schedule Windows NT, 2000, XP, and 2003 clients to sweep during off-hours as long as the system remains powered-on (even with the user logged out). For Windows 98, 98SE, and ME systems, the user must be logged in to execute a scheduled sweep.

On the Sweep Settings page, setting to "Sweep only Known Spyware folders" will produce the fastest scans of systems. If you set clients to "invisible" mode, end-users will not be able to modify any user-editable settings and will not be able to put the client in admin mode even if they have the password.





The Auto Install feature is best used for spy definitions. We recommend installing bug fixes and product updates with the Manual Install feature, to control when the updates are delivered to clients.



### **Support Contact Information**

Email [esupport@webroot.com](mailto:esupport@webroot.com) We will respond within one business day.  
Call 800-870-8102

Information in this document is subject to change without notice.

Copyright 2004 Webroot Software, Inc. All rights reserved.

Trademarks used in this text: "Webroot" is a trademark of Webroot Software, Inc.;  
"Microsoft" and "Windows NT" are registered trademarks of Microsoft Corporation.

Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. Webroot Software, Inc. disclaims any proprietary interest in trademarks and trade names other than its own.

## **Webroot Spy Sweeper Enterprise**

### Version 2.0 Release Notes

#### New Features

- Distributed update delivery
  - Spy definition and software updates downloaded to your Webroot Enterprise Server are automatically moved to a new update distributor server
  - You can define additional distributor servers and assign them to groups to balance load or deploy updates to clients from local distribution points
- Improved spy detection algorithms
  - Client detects and removes the newest and most dangerous spies
- Mobile client definition updating
  - Administrator can enable end-users to check for spy definition updates directly from Webroot when they are off the corporate network
- Client Management screen
  - Search, sort, and filter clients based on group, last heartbeat, software version, spy definition version, last sweep time and more
  - Send Sweep Now and Poll Now commands to one or more clients
  - Delete clients or groups
  - Export lists of clients to Microsoft Excel (.xls) format
- Faster screen displays in the Admin Console
  - With large numbers of clients, screen displays are now tremendously faster
- Microsoft SQL Server support
  - In addition to the embedded database that ships with the software, Microsoft SQL Server is now a supported option for server database
- "Poll Now" command
  - From the Admin Console, tell clients to poll immediately to get new configuration settings or retrieve software or spy definition updates
- Sweep on startup and scheduling sweep times in hours and minutes
  - Sweep on startup does a quick sweep that gives good coverage
  - Scheduling sweeps to the minute-level allows precise control of schedules
- Admin-definable application and site blocking lists
  - Administrators can enter any .exe or any URL to block
  - Spy Sweeper's shields will automatically enforce these rules
- Faster sweep times
  - Full system sweeps are approximately 20% faster
- Automated server throttling and polling randomization
  - Intelligently moderate and spread client load on server
- Allow users to cancel sweeps
  - Administrators can allow users to cancel sweeps that are in-progress whether these sweeps started from a schedule or a Sweep Now from the Admin Console

### **Key Fixes**

- Cases where clients polled but did not get assigned updates have been fixed.
- Issue where NT4 and Windows 98 clients crashed on shutdown has been resolved.
- SpysweeperTray.exe1 rollback errors on client install no longer occur
- Fixed issues where tray icon does not appear
- Resolved issue with crash on shutdown while sweeping
- Fixed THTTPHandler.Get.HTTPSendRequest error on manual check for updates
- Fixed handle leak with cookie shield
- The read-only flag on the hosts file getting set incorrectly has been fixed
- Access Violations in Update Service and Spy Sweeper Service have been corrected
- Fixed issue where users could get command window with system privileges
- Admin password for client is now stored in an encrypted format
- Issues with using domain name instead of server IP address have been corrected

### **Implementation Notes and Known Issues**

- The minimum memory requirement for the Enterprise Server has increased from 256MB to 512MB.
- Poll Now requires port 50002 to be open to the client. The Update Distributor (including the one on your Enterprise Server) requires port 8080 to be open to deliver updates to clients.
- Sweep Now and Poll Now are intended for use with less than twenty clients. These functions open connections to all the clients and can cause significant network traffic if too many are contacted simultaneously.
- The Common Ad Sites shield has been replaced with the Blocked Sites shield. The Blocked Sites shield allows you to prevent access to specific sites (versus a general list of advertising sites). Webroot pre-populates this list with some sites observed to provide spyware or potentially unwanted software downloads. If this list did not get set during an upgrade from 1.5.1 to 2.0, you can enter the following sites:
  - [iefeadsl.com](http://iefeadsl.com)
  - [008k.com](http://008k.com)
  - [356563.net](http://356563.net)
  - [75tz.com](http://75tz.com)
  - [kitasearch.com](http://kitasearch.com)
  - [lookfor.com](http://lookfor.com)
  - [look-today.com](http://look-today.com)
  - [new.8ad.com](http://new.8ad.com)
  - [rf104.com](http://rf104.com)
  - [search-to-find.com](http://search-to-find.com)
  - [www.05p.com](http://www.05p.com)
  - [www.6o9.com](http://www.6o9.com)
  - [www.ga31.com](http://www.ga31.com)
  - [www.v61.com](http://www.v61.com)
- Spy Sweeper automatically terminates Internet Explorer at the end of a sweep to successfully quarantine or delete some spies. If end users typically work with IE, schedule sweeps for non- working times. For Windows NT and later clients, Spy Sweeper runs as service and can sweep when no user is logged in (as long as the system is on).
- The Admin Console calculates the number of licenses in use by counting the number of clients that have polled in the last day. Licenses in Use will show the total count of clients that polled on the previous day.

- Making settings user-editable means the client will reject all changes in the setting. If you want to set a default but with user ability to override follow these steps:
  - Set the default you want
  - Allow the clients to poll – or perform a Poll Now from the Client Management screen
  - Click the “User Editable” checkbox for that feature
- Editing only the hour or minutes of a scheduled sweep time does not enable the Apply Changes button. Click on the scroll box to enable the button.
- Installations using Microsoft SQL Server as the database need to download at least one spy definition before spies will show up in the Found Spies list.
- If you want to switch to Microsoft SQL Server from DBISAM, detailed instructions are provided in the System Administrator Guide.
- Time cannot be specified in filters in the Client Management screen.
- Although you can delete groups created from domain and workgroup names in the Client Management screen, they will be re-created when clients poll in again.
- The cursor disappears when dragging workstations onto groups in the Client Management screen.
- If an update is blocked from being distributed to a client (e.g. if all distributor services are shut down), the client will not receive settings information as well.
- Some auto-install rules may be cleared after upgrading from 1.5.1 to 2.0
- Sweep scheduling now uses 24-hour clock times (PM times have 12 added to them – e.g. 14:00 is the same as 2:00PM)
- On new installation, the Spy Sweeper Enterprise client will wait a random time from 1 to 300 seconds before polling. After this first poll, the client will wait a random delay from 1 second up to the full polling interval specified in the Admin Tasks -> Settings page for CommAgent Polling Interval. This spreads the load of client polling more evenly for large installations.
- The Configure Groups, Client Status, and Applications screens have all been replaced by the new Client Management screen.

## Requirements

### *Administrative Server system requirements:*

- Operating System: Windows NT 4.0 SP5 or higher, Windows 2000, Windows XP, Windows Server 2003
- CPU: 200 MHz minimum; 350 MHz or higher recommended
- Memory: 512 MB recommended
- Disk: 30 MB free disk space for operation. Additional free disk space will be needed for database growth. We recommend 1 GB of free disk.

### *Distributor Server system requirements:*

- Operating System: Windows NT 4.0 SP5 or higher, Windows 2000, Windows XP, Windows Server 2003
- CPU: 200 MHz minimum; 350 MHz or higher recommended
- Memory: 256 MB recommended
- Disk: 30 MB free disk space for operation. Additional free disk space will be needed for database growth. We recommend 1 GB of free disk.

### *Client requirements:*

- Operating System: Windows 98, 98SE, ME (with Internet Explorer 6.0 with Service Pack 1), 2000, XP, 2003, or NT 4.0
- CPU: 150 MHz or higher recommended
- Memory: 32 MB RAM minimum; 128 MB RAM or better recommended
- Disk: 15 MB free disk space

## Uninstall Notes

A user with administrative privileges should uninstall Webroot Spy Sweeper Enterprise to ensure complete removal.

Use Add or Remove Programs to remove the Enterprise Server, Update Distributor and/or Client.

Important: To remove the client, the SpySweeperSetup.msi file must be available in the location from where it was originally run. To prevent end users from uninstalling, simply move SpySweeperSetup.msi to a different location.

Information in this document is subject to change without notice.

Copyright 2004 Webroot Software, Inc. All rights reserved.

Trademarks used in this text: "Webroot" is a trademark of Webroot Software, Inc.; "Microsoft" and "Windows NT" are registered trademarks of Microsoft Corporation.

Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. Webroot Software, Inc. disclaims any proprietary interest in trademarks and trade names other than its own.

**Exhibit 3: Screenshots Comparing Webroot Spy Sweeper Versions 3.2 and 3.5**





**Exhibit 4: Screenshots Comparing Webroot Enterprise Versions 1.5 and 2.0**

Source View - 2.0 Release 3687 [Branch]

File Edit View Activities Repository Branch Tools Window Help

Branches: 2.0 Release 3687

- Download Wizard for Citibank
- Download Wizard for MSN
- Enterprise Products 1.5
- Enterprise Products 2.0
- 2.0 Release 3687
- 2.0 Release 3700
- 2.0 Release 3719
- Enterprise SS Client 2.5 OLD
- Phase 01
- Phase Test
- Phish Net v1.2 (Beta)
- Phish Net v1.3
- PopUp Washer 2.5
- PhidCenter (Alpha)
- Shared Code 1.0
- Shared Code 1.5
- Shared Code 2.0
- Shed v1.0
- Shed v1.7
- Spam Shredder 1.7
- Spam Shredder 1.9

Repositories:

- Webroot/Easyrite
- AdminConsole
- Build
- ClientService
- Components
- DBRepair
- dbu
- Documentation
- exe
- LegacyCode
- Shard
- SysWrapper
- Sub
- TP
- UpdateInfoServer
- Utilities

Files: All Files

| Filename               | Timestamp           | Status  | Type | Ver |
|------------------------|---------------------|---------|------|-----|
| winroot.pas            | 9/13/2004 2:37 PM   | unknown | Text | 1   |
| VolumeItems.pas        | 10/11/2004 3:48 PM  | unknown | Text | 1   |
| VolumeItems.pas        | 10/9/2004 9:38 PM   | unknown | Text | 1   |
| VolumeItems.pas        | 10/9/2004 9:27 PM   | unknown | Text | 1   |
| OSV.pas                | 11/9/2004 8:10 PM   | unknown | Text | 1   |
| LoadfiledataThread.pas | 11/12/2004 5:59 PM  | unknown | Text | 1   |
| FileStack.pas          | 10/12/2004 3:20 PM  | unknown | Text | 1   |
| FileItems.pas          | 10/11/2004 3:45 PM  | unknown | Text | 1   |
| FileItem.pas           | 11/9/2004 8:28 PM   | unknown | Text | 1   |
| FileItem.pas           | 11/10/2004 12:05 AM | unknown | Text | 1   |
| DirectoryItems.pas     | 10/11/2004 3:46 PM  | unknown | Text | 1   |
| DirectoryItem.pas      | 10/9/2004 9:54 PM   | unknown | Text | 1   |
| CustomBucket.pas       | 12/7/2004 9:07 PM   | unknown | Text | 1   |

Source View - 1.51 (Release) [Branch]

File Edit View Activities Repository Branch Tools Window Help

Branches: 1.51 (release)

- Desktop Wizard for Citibank
- Download Wizard for MSN
- Enterprise Products 1.5
- 1.51 (release)
- 1.52 (release)
- Enterprise Products 2.0
- Phase 01
- Phase Test
- Phish Net v1.2 (Beta)
- Phish Net v1.3
- PopUp Washer 2.5
- PhidCenter (Alpha)
- Shared Code 1.0
- Shared Code 1.5

Repositories:

- Webroot/Easyrite
- AdminConsole
- ClientService
- Components
- DBRepair
- dbu
- Documentation
- exe
- LegacyCode
- No FileFileScan
- Shard
- SysWrapper
- Encryption
- Sds
- Sis
- UpdateInfoService
- Utilities

Files: All Files

| Filename    | Timestamp          | Status  | Type   | Version |
|-------------|--------------------|---------|--------|---------|
| Window...   | 8/17/2004 7:53 AM  | unknown | Text   | 1       |
| TrayIcon... | 6/9/2004 10:25 AM  | unknown | Text   | 1       |
| TrayIcon... | 5/21/2004 9:52 PM  | unknown | Binary | 1       |
| etTypes...  | 9/26/2004 8:13 PM  | unknown | Text   | 1       |
| etCard...   | 9/21/2004 8:40 PM  | unknown | Text   | 1       |
| etRegist... | 6/9/2004 10:25 AM  | unknown | Text   | 1       |
| etGlobal... | 9/29/2004 10:38 AM | unknown | Text   | 1       |
| etFullIt... | 8/23/2004 7:38 AM  | unknown | Text   | 1       |
| etComp...   | 5/21/2004 9:52 PM  | unknown | Text   | 1       |
| etClass...  | 9/23/2004 5:58 PM  | unknown | Text   | 1       |
| etSWAbso... | 7/25/2004 1:08 PM  | unknown | Text   | 1       |
| etSWSee...  | 9/29/2004 10:13 AM | unknown | Text   | 1       |
| etSWIne...  | 9/29/2004 8:15 AM  | unknown | Text   | 1       |

```

FastFileProcessor = class
private
    FDirectoryItems: TDirectoryItems;
    FRecursive: boolean;
    FInitialDir: string;
    FCancelProcessing: boolean;
    private FTickCount: cardinal;
    FOnEnumerateFile: TEnumerateFileEvent;
    FOnEnumerateDirectory: TEnumerateDirectoryEvent;
    FOnError: TOnErrorEvent;
private
    procedure SetInitialDir( _value: string );
    function GetInitialDir( const _fileName: string; var _buffer; _size: cardinal; _startingCn: integer ): boolean;
    function GetInitialDir( const _fileName: string; _size: cardinal; _startingCn: integer; _filePath: string );
    procedure ProcessFiles;
protected
    // OnEnumerateFile checks if an OnEnumerateFile event method is assigned
    procedure OnEnumerateFile( const _fileName: string; _size: cardinal; var _process: boolean ); virtual;
    // OnEnumerateDirectory checks if an OnEnumerateDirectory event method is
    // assigned and calls it within a try/finally
    procedure OnEnumerateDirectory( const _dirName: string; _size: cardinal; var _process: boolean ); virtual;
    // OnProcessFiles checks if an OnProcessFiles event method is assigned
    // and if so calls it within a try/finally
    procedure OnProcessFiles( const _dirName: string; _size: cardinal; var _process: boolean ); virtual;
    // OnError checks if an OnError event method is assigned
    // and if so calls it within a try/finally
    procedure OnError( _errorCode: integer; const _errorMessage: string ); virtual;
public
    constructor Create( _errorCode: integer; const _errorMessage: string ); virtual;
    destructor Destroy; override;
    // Near setting this InitialDir as well as the recursive property and the
    // enumeration/process events call ProcessFilesAndDir to have
    // the class enumerate every directory and file it can find in InitialDir
    // (and sub directories, if Recursive is true) and process the found files
    // corresponding events.
    // When ProcessFilesAndDir is called the generated will spawn a file read
    // thread which first sorts the found files according to their locations
    // on the disk for quicker access (less disk head movement) and then starts
    // calculation and puts the read files on a stack. The thread class
    // runs in parallel and removes the items from the stack and passes them on to the
    // OnProcessFiles event where you can calculate the short CRC (without need
    // for the disk continuously) and at full speed (no interruption at all)
    // except when the OS allows itself or other apps to access the disk.
    // When all files that have been enumerated so far have been processed,
    // the code will continue to enumerate more files before it will go back
    // to processing them again. This loop will be repeated as many times as
    // needed until all files in the InitialDir have been enumerated and
    // processed.
    // This iterative process is required because this algorithm relies on the
    // OS caching the location of the files since that the disk has to
    // find out that the file it is working on is at the very end of the disk.
    // Items which will reduce memory consumption by quite a bit.
    // procedure ProcessFilesAndDir;
public
    property Recursive: boolean read FRecursive write FRecursive;
    // Set InitialDir to the directory you want to scan.
    // Since enumerating and processing thousands of files can take minutes
    // you can stop the enumeration or processing action by setting
    // CancelProcessing to true. (from within one of the events)
    // property CancelProcessing: boolean read FCancelProcessing write FCancelProcessing;
    // OnEnumerateFile occurs when you call EnumerateFilesAndDir and a
    // property OnEnumerateFile: TEnumerateFileEvent read FOnEnumerateFile write FOnEnumerateFile;
    // OnEnumerateDirectory occurs when you call EnumerateFilesAndDir
    // and a directory is found.
    // OnProcessFiles occurs when you call ProcessFilesAndDir
    // and the first few bytes are loaded for short CRC calculation
    // property OnProcessFiles: TProcessFilesEvent read FOnProcessFiles write FOnProcessFiles;
    // OnError occurs when you call ProcessFilesAndDir and a
    // notification about this incident via this error event. An ErrorCode will be
    // -1 if the error is an exception, otherwise it will be the result of
    // an GetLastException.
    // property OnError: TOnErrorEvent read FOnError write FOnError;
end;

```

**Exhibit 5: Program Version and Build Numbers with Corresponding Release Dates for  
Webroot Spy Sweeper**

Quick Search

- [Browse](#)
  - [Pages](#)
  - [News](#)
  - [Labels](#)
  - [Attachments](#)
  - [Bookmarks](#)
  - [Mail](#)
  - [Advanced](#)
  - [Activity](#)
  - [People Directory](#)
- [Michael Burtscher](#)
  - [Preferences](#)
  - [History](#)
  - [Labels](#)
  - [Watches](#)
  - [Drafts](#)
  - [Log Out](#)

1. [Dashboard](#)
2. > [QA - Quality Assurance Release Page](#)
3. > ...
4. > [Home](#)
5. > [Releases - Consumer](#)
6. > [SpySweeper Builds](#)

- [Welcome Michael Burtscher](#)
- [History](#)
- [Preferences](#)
- [Log Out](#)

- [Edit](#)
- [Add](#)
  - [Page](#)
  - [News](#)
  - [Bookmark](#)
  - [Comment](#)
  - [Attachment](#)
- [Tools](#)
  - [Attachments \(57\)](#)
  - [History](#)
  - [Favourite](#)
  - [Watch](#)
  - [Info](#)
  - [View Wiki Markup](#)
  - [Export to PDF](#)
  - [Export to Word](#)
  - [Copy](#)
  - [Move](#)

## Spysweeper Builds

Added by [Jake Wilson](#), last edited by [Jake Wilson](#) on Oct 13, 2008 ([view change](#))

| Products             | Type               | Version   | Spy AV Def | AV Eng | SDK Version | Languages | Date Released to site | Dupli- cation Date | Release Type       | Customer              | Release Notice                 | Comments  |
|----------------------|--------------------|-----------|------------|--------|-------------|-----------|-----------------------|--------------------|--------------------|-----------------------|--------------------------------|---|
| Spysweeper, AV, WISE | Online, GMC D      | 6.0.2.22  | 1304       |        | 4.2.0.125   | EN        | 10/15/08              | ?                  | online             | all en except BB      | <a href="#">release notice</a> |   |
| Spysweeper, AV, WISE | BETA Refresh, GMCD | 6.0.1.35  | 1295       |        | 4.2.0.118   | EN        | 9/30/08               | 9/30/08            | Beta Refresh, GMCD | Zomax, Beta customers | <a href="#">release notice</a> |   |
| Spysweeper, AV, WISE | BETA               | 6.0.0.179 | 1138       |        | 4.2.0.98    | EN        | 9/9/08                |                    | Beta               | Beta                  | <a href="#">release notice</a> |   |
| Spysweeper, AV, BBA  | FULL               | 5.8.1.55  | 1250       |        | 4.0.1.302   | all       | 8/18/08               |                    | online, BBA, GMCD  | ALL, BB               | <a href="#">release notice</a> | \\docms\POSTQA-APPROVED\Spysweeper\5.8\5.8.1.55\Release |
| Spysweeper, AV, WISE | Online             | 5.8.1.51  | 1250       |        | 4.0.1.298   | EN, GBR   | 7/31/08               |                    | Online, GMCD       | New, Tech Bench       | <a href="#">release notice</a> | \\docms\POSTQA-   |



Beta (5.5)

RELEASED\SpySweeper\5.5\_BETA  
[5.5.1.3172\Release]

| Product                              | Version          | Build                              | Region                          | Release Date                   | Customer      | Notes  |
|--------------------------------------|------------------|------------------------------------|---------------------------------|--------------------------------|---------------|--|
| FULL, TRIAL, and SNOR                | 866, NL-872      | 5.3.2.2361                         | ES, FR, NL, IT, DE, GBR, JA, EN | 3/7/2007                       | All Customers | ONLINE release. Version Guard. Auto Updates, Manual Updates.   |
|                                      | 866              | 5.3.2.2609                         | GBR                             | 3/8/2007                       |               | Release Notice   |
| Full, Trial, and SNOR                | 866              | 5.3.2.2361                         | GBR                             | 3/8/2007                       | Tribeka       | The build can be found at [DCO:\Dcooms\POSTQA-RELEASED\Webroot Released Applications\Spy Sweeper\5.3\5.3.2.2361\GMCD_GB ROnly] |
| Full (30 day trial)                  | 866              | 5.3.2.2361                         | EN, FR, ES                      | 3/9/2007                       | Sony          | The build can be found at [DCO:\Dcooms\POSTQA-RELEASED\Webroot Released Applications\Spy Sweeper\5.3\Sony\5.3.2.2361]          |
| Full                                 | 872              | 5.3.2.2367                         | JA                              | 4/10/2007                      | POC           | Build can be found at [DCO:\DCCOCMS\POSTQA-RELEASED\Webroot Software\Webroot Released Applications\Spy Sweeper\5.3\5.3.2.2367] |
| Spy Sweeper Moonraker Domestic (5.0) | 1009             | 5.0.x.1009                         | EN                              | 5/15/2006                      |               | Beta 1   |
|                                      | 1133, 1250, 1286 | 5.0.x.1133, 5.0.x.1250, 5.0.x.1286 | EN                              | 6/6/2005, 6/14/2006, 7/10/2006 |               | Beta 2, Beta 3, GA   |
| Full, Trial, SNOR                    | 1607             | 5.0.x.1607                         | EN                              | 8/9/2006                       |               | Patch 1  |
| Trial                                | 1608             | 5.0.7.1608                         | EN                              | 10/30/2006                     |               | OEM Build for Circuit City   |

Spy





|  |                   |           |                                     |            |            |  |
|--|-------------------|-----------|-------------------------------------|------------|------------|--|
| Spy Sweeper L2K International (4.5)      | Full, Trial       | 4.5.x.709 | EN                                  | 1/25/2006  |            | Full Launch Maintenance Release                                  |
|  | SNoRNoSh          | 4.5.x.709 | EN                                  | 1/20/2006  |            | Scan No Remove No Shields Version                                |
|  | SNoR              | 4.5.x.711 | EN                                  | 1/20/2006  |            | Scan No Remove with Shields Updated                              |
|  | SNoRNoSh          | 4.5.x.711 | EN                                  | 2/7/2006   |            | Scan No Remove No Shields Version Updated                        |
|  | Full, Trial, SNoR | 4.5.x.730 | EN                                  | 7/10/2006  |            | EOL build  |
|  | Full, Trial       | 4.5.x.560 | ES,DE,FR,N<br>L,IT, GBR             | 10/11/2005 | Beta       | Beta 2   |
|  | Full, Trial       | 4.5.x.594 | JPN                                 | 10/18/2006 | Beta       | Beta 1 update  |
|  | Full, Trial       | 4.5.x.604 | ES,DE,FR,N<br>L,IT, GBR             | 10/24/2005 |            | Soft Launch  |
|  | Full, Trial       | 4.5.x.607 | ES,DE,FR,N<br>L,IT, GBR             | 10/28/2005 | 10.31.2005 | Hard Launch  |
|  | Full, Trial       | 4.5.x.632 | JPN                                 | 11/3/2005  |            | JP L2K Retail Release and Vector Trial                           |
| Spy Sweeper US Domestic Goldfinger (4.0) | Full, Trial       | 4.5.x.656 | ES,DE,FR,N<br>L,IT, GBR             | 11/17/2005 | 11.18.2005 | Full Launch Maintenance Release                                  |
|  | Full, Trial       | 4.5.x.683 | ES,DE,FR,N<br>L,IT, GBR,<br>JPN     | 12/15/2005 | 12.20.2005 | Full Launch Maintenance Release and JPN 30, 60 and 90 day trials |
|  | SNoR              | 4.5.x.683 | GBR                                 | 12/16/2006 |            | Scan No Remove I18N  |
|  | SNoR              | 4.5.x.711 | FR, GBR,<br>NL, EN                  | 2/7/2006   |            | Scan No Remove I18N Updated                                      |
|  | Full, Trial, SNoR | 4.5.x.730 | ES,DE,FR,N<br>L,IT, GBR,<br>GBR,JPN | 7/10/2006  |            | EOL  |
|  | Full, Trial       | 4.0.x.359 | English                             | 6/3/2005   | Beta       | Beta 1   |
|  | Full, Trial       | 4.0.x.363 | English                             | 6/10/2005  | Beta       | Beta 2   |
|  | Full, Trial       | 4.0.x.402 | English                             | 7/7/2005   |            | Soft Launch  |
|  | Full, Trial       | 4.0.x.405 | English                             | 7/11/2005  |            | Full Launch  |
|  | Full, Trial       | 4.0.x.359 | GBR                                 | 6/3/2005   | Beta       | Beta 1   |

International  
al (4.0)

4.0.x.374 ES,DE,FR,N 6/15/2005  
L,IT, GBR  
4.0.x.443 JPN 8/9/2006  
4.0.x.458 ES,DE,FR,N 9/13/2005  
L,IT, GBR

Soft Launch

JPN L2K Beta1

Full Launch

Spy  
Sweeper  
Pre-4.0

Full, Free, 2.6.x.45 English 4/28/2004  
Trial  
Full, Free, 3.x.x.129 English 7/22/2004  
Trial  
Full, Trial 3.2.x.150 English 11/14/  
2004  
Full, Trial 3.5.x.186 English 12/6/2004  
3.5.x.191 English 1/17/2005  
3.5.x.189 English 12/9/2004  
3.5.x.194 English 1/25/2005  
3.5.x.198 English 3/2/2005  
3.5.x.199 English 3/17/2005

This was the last 2.6 build produced

This was the last 3.0 build produced

This was the last 3.2 build produced

This release is to be in synch with the  
3.5 International release.

PC Mag Review Build

Defect fixes and changes to the  
EULA

Full Launch

This is the first 3.5 international  
release, we have broken out the  
individual language builds for this  
release.

Defect fixes and changes to the

Spy  
Sweeper  
International  
al 3x

Full, Trial 3.2.x.150 ES,DE,FR,N 12/6/2004  
L,IT  
Full, Trial 3.5.x.191 ES,DE,FR,N 1/17/2005  
L,IT  
3.5.x.194 ES,DE,FR,N 1/25/2005  
L,IT  
3.5.x.198 ES,DE,FR,N 3/2/2005

Labels parameters

## Labels

[Add Labels](#) [Done](#)

Enter labels to add to this page:

|                      |                                    |                                     |
|----------------------|------------------------------------|-------------------------------------|
| <input type="text"/> | <input type="button" value="Add"/> | <input type="button" value="Done"/> |
|----------------------|------------------------------------|-------------------------------------|

Looking for a label? Just start typing.

[Add Comment](#)

- [Powered by Atlassian Confluence 2.9.2, the Enterprise Wiki.](#)
- [Printed by Atlassian Confluence 2.9.2, the Enterprise Wiki.](#)
- [Bug/feature request –](#)
- [Atlassian news –](#)
- [Contact administrators](#)

**Exhibit 6: Brian Kellner E-Mail Message Dated December 19, 2004**

**Croft, Tom**

---

**From:** Brian Kellner  
**Sent:** Sunday, December 19, 2004 11:11 PM  
**To:** Webroot All  
**Cc:** 'patrick.ward@104degreeswest.com'; 'Matt Otepka'; 'lindag@techcomplus.com'  
**Subject:** Spy Sweeper Enterprise Version 2.0 Released!  
**Importance:** High

Thanks to the amazing efforts of the entire team, we were able to release version 2.0 tonight.

This release is a huge milestone for the product in terms of stability, scalability, and industry-leading features (see list below).

Thanks again to the entire product development team and everyone who has supported them.

Regards,  
Brian

**New Features in Spy Sweeper Enterprise 2.0**

- Distributed update delivery
  - Spy definition and software updates downloaded to your Webroot Enterprise Server are automatically moved to a new update distributor server
  - You can define additional distributor servers and assign them to groups to balance load or deploy updates to clients from local distribution points
- Improved spy detection algorithms
  - Client detects and removes the newest and most dangerous spies
- Mobile client definition updating
  - Administrator can enable end-users to check for spy definition updates directly from Webroot when they are off the corporate network
- Client Management screen
  - Search, sort, and filter clients based on group, last heartbeat, software version, spy definition version, last sweep time and more
  - Send Sweep Now and Poll Now commands to one or more clients
  - Delete clients or groups
  - Export lists of clients to Microsoft Excel (.xls) format
- Faster screen displays in the Admin Console
  - With large numbers of clients, screen displays are now tremendously faster
- Microsoft SQL Server support
  - In addition to the embedded database that ships with the software, Microsoft SQL Server is now a supported option for server database
- "Poll Now" command
  - From the Admin Console, tell clients to poll immediately to get new configuration settings or retrieve software or spy definition updates

- Sweep on startup and scheduling sweep times in hours and minutes
  - Sweep on startup does a quick sweep that gives good coverage
  - Scheduling sweeps to the minute-level allows precise control of schedules
- Admin-definable application and site blocking lists
  - Administrators can enter any .exe or any URL to block
  - Spy Sweeper's shields will automatically enforce these rules
- Faster sweep times
  - Full system sweeps are approximately 20% faster
- Automated server throttling and polling randomization
  - Intelligently moderate and spread client load on server
- Allow users to cancel sweeps
  - Administrators can allow users to cancel sweeps that are in-progress whether these sweeps started from a schedule or a Sweep Now from the Admin Console

Brian Kellner, Director of Enterprise Product Mgt



2560 55th Street, Ste 200

Boulder, CO 80301

Email: [bkellner@webroot.com](mailto:bkellner@webroot.com)

Web: [www.webroot.com](http://www.webroot.com)

Tel:303.442.3813 ext218| Fax:303.442.3846|

**Exhibit 7: Sarah Mood E-Mail Message Dated December 2, 2004**

## Croft, Tom

---

**From:** Sarah Mood [IMCEAEX-  
\_O=WEBROOT\_OU=FIRST+20ADMINISTRATIVE+20GROUPOU=WEBROOT\_CN=RECIPIENTS\_CN=SMOOD@we  
**Sent:** Thursday, December 02, 2004 9:06 AM  
**To:** DL Webroot Office  
**Cc:** Terry Fleming; Nick Lewis; William Tubbs; Herbert Weustenenk  
**Subject:** Tell your friends & family about our 3.5 external beta

Thank you to everyone who has downloaded Spy Sweeper 3.5 and provided feedback. At this point in time, we'd like to encourage you to tell your friends and family **that are already running Spy Sweeper** to participate in our limited, external beta which just kicked off.

- To participate, they simply need to click on **Update Program** under the **Options** menu of Spy Sweeper. From there, they can just follow the instructions and complete the installation using their original keycode which will be displayed to them for their convenience.
- Getting feedback over the next 2 days is our primary goal. To submit feedback, your friends and family can click on **Submit Feedback** also under the options menu or simply email us at [spybeta@webroot.com](mailto:spybeta@webroot.com).
- If you would still like to try it out for yourself, reply to my message and I'll get you the latest version.

Thanks for your help.

Sarah

Sarah Mood  
Product Manager  
Webroot Software  
tel 303.442.3813 ext.179  
email [smood@webroot.com](mailto:smood@webroot.com)  
web [www.webroot.com](http://www.webroot.com)  
2560 55th Street Boulder, CO 80301

---

**From:** Sarah Mood  
**Sent:** Tuesday, November 30, 2004 4:39 PM  
**To:** Webroot Office  
**Cc:** Terry Fleming  
**Subject:** Internal testing of Spy Sweeper 3.5 - we need your help!

Everyone –

We need your help testing the next version of Spy Sweeper consumer! We need to get more eyes on this version in order to identify any unknown issues before we make 3.5 commercially available and available to PC Magazine for review later this week. We greatly appreciate you making this a huge priority as soon as you have time to spare – the sooner the better.

This is an internal-only release – please do not distribute to non-Webroot employees.

Please feel free to install this beta on either your company PC and/or home computer.

1. Close your existing Spy Sweeper (shut it down, don't minimize)
2. Go to the intranet and click on 'latest version of Spy Sweeper' – follow the instructions listed to complete the installation. <http://intranet.boulder.webroot.com/>
3. Conduct your normal activity with Spy Sweeper – run a sweep, play with shields, etc.
4. Report any problems, questions, or issues to me and I will make sure they get filtered and addressed by our development and QA teams.



New things to look for in this release: Sweeps that are 30% faster, new IE hijack shield, new report spyware feature under Options, ability to ignore cookies during a scan (also under options) and many behind-the-scene tools to effectively remove the worst spies – CWS included! Please note that if you add a favorite on your own you will not be alerted by the IE Favorites Shield with this release. You will only be alerted if a piece of spyware added a favorite.

\*\*\* More kudos will be sent out later to all of the folks that worked nights, weekends and even holidays to get this release out. Just today we have Jeff Horne, Mike Wilson and of course Brad Stowers to thank in adding even more mechanisms to identify and remove tricky CWS variants.

Thanks for your help in this team effort and let's get the feedback rolling in!

Sarah Mood  
Product Manager  
Webroot Software  
tel 303.442.3813 ext.179  
email [smood@webroot.com](mailto:smood@webroot.com)  
web [www.webroot.com](http://www.webroot.com)  
2560 55th Street Boulder, CO 80301

**Exhibit 8: Brian Kellner E-Mail Message Dated November 24, 2004**

## Croft, Tom

---

**From:** Brian Kellner [IMCEAEX-  
\_O=WEBROOT\_OU=FIRST+20ADMINISTRATIVE+20GROUP\_CN=RECIPIENTS\_CN=BKELLN  
**Sent:** Wednesday, November 24, 2004 7:06 PM  
**To:** DL Webroot Enterprise Group; Colin Smith; Gilles Paulot; Herbert Weustenenk; Nick Lewis; Pasc  
Doerr; Ruben Savazzi; William Tubbs  
**Subject:** Spy Sweeper Enterprise 2.0 Beta Released!  
**Attachments:** BetaParticipants.xls

Thanks to the hard work of the entire team, the beta has been released.

The quality of the product has improved tremendously from everyone's efforts, and I think our customers will really enjoy this beta.

We still have a lot left to do in order to release a great product in the week of Dec 6, but I believe it is possible.

Below is the message sent to our beta testers (the list of testers is attached).

Thanks again and have a great Thanksgiving,  
Brian

The Spy Sweeper Enterprise team is excited to release the beta of Spy Sweeper Enterprise 2.0!

To participate in the beta, click the link below to download the software and evaluation documents.

[http://downloadsrv.webroot.com/download.php?  
dlkey=acdefhiklmngstuvxyABDEGIJKNORSTWXY](http://downloadsrv.webroot.com/download.php?dlkey=acdefhiklmngstuvxyABDEGIJKNORSTWXY)

On behalf of the entire team, please accept my thanks for taking the time to review the software and provide your feedback. To thank you for your time, we will be sending appreciation gifts to everyone who provides feedback by December 2.

Brian Kellner, Director of Enterprise Product Mgt.



2560 55th Street, Ste 200  
Boulder, CO 80301

Email: [bkellner@webroot.com](mailto:bkellner@webroot.com)

Web: [www.webroot.com](http://www.webroot.com)

Tel:303.442.3813 ext218| Fax:303.442.3846|

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

|   |   |                                  |                                       |
|---|---|----------------------------------|---------------------------------------|
| <b>PATENT APPLICATION FEE DETERMINATION RECORD</b><br>Substitute for Form PTO-875 | Application or Docket Number<br><b>11/104,202</b> | Filing Date<br><b>04/12/2005</b> | <input type="checkbox"/> To be Mailed |
|---|---|----------------------------------|---------------------------------------|

| APPLICATION AS FILED – PART I   |   |              | OTHER THAN SMALL ENTITY               |          |    |           |          |
|---|---|--------------|---------------------------------------|----------|----|-----------|----------|
|   | (Column 1)  | (Column 2)   | SMALL ENTITY <input type="checkbox"/> | OR       |    |           |          |
| FOR   | NUMBER FILED  | NUMBER EXTRA | RATE (\$)                             | FEE (\$) | OR | RATE (\$) | FEE (\$) |
| <input type="checkbox"/> BASIC FEE<br><small>(37 CFR 1.16(a), (b), or (c))</small>        | N/A   | N/A          | N/A                                   |          |    | N/A       |          |
| <input type="checkbox"/> SEARCH FEE<br><small>(37 CFR 1.16(k), (l), or (m))</small>       | N/A   | N/A          | N/A                                   |          |    | N/A       |          |
| <input type="checkbox"/> EXAMINATION FEE<br><small>(37 CFR 1.16(o), (p), or (q))</small>  | N/A   | N/A          | N/A                                   |          |    | N/A       |          |
| TOTAL CLAIMS<br><small>(37 CFR 1.16(i))</small>   | minus 20 =  | *            | X \$ =                                |          | OR | X \$ =    |          |
| INDEPENDENT CLAIMS<br><small>(37 CFR 1.16(h))</small>                                     | minus 3 =   | *            | X \$ =                                |          |    | X \$ =    |          |
| <input type="checkbox"/> APPLICATION SIZE FEE<br><small>(37 CFR 1.16(s))</small>          | If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$250 (\$125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s). |              |                                       |          |    |           |          |
| <input type="checkbox"/> MULTIPLE DEPENDENT CLAIM PRESENT <small>(37 CFR 1.16(j))</small> |   |              |                                       |          |    |           |          |
|   |   |              | TOTAL                                 |          |    | TOTAL     |          |

\* If the difference in column 1 is less than zero, enter "0" in column 2.

| APPLICATION AS AMENDED – PART II |   |                                  |                                    |               | OTHER THAN SMALL ENTITY |                     |    |                 |                     |
|----------------------------------|---|----------------------------------|------------------------------------|---------------|-------------------------|---------------------|----|-----------------|---------------------|
|                                  | (Column 1)  | (Column 2)                       | (Column 3)                         |               | SMALL ENTITY            | OR                  |    |                 |                     |
| AMENDMENT                        | 12/03/2008  | CLAIMS REMAINING AFTER AMENDMENT | HIGHEST NUMBER PREVIOUSLY PAID FOR | PRESENT EXTRA | RATE (\$)               | ADDITIONAL FEE (\$) | OR | RATE (\$)       | ADDITIONAL FEE (\$) |
|                                  | Total <small>(37 CFR 1.16(i))</small>   | * 14                             | Minus ** 20                        | = 0           | X \$ =                  |                     | OR | X \$52=         | 0                   |
|                                  | Independent <small>(37 CFR 1.16(h))</small>   | * 3                              | Minus ***3                         | = 0           | X \$ =                  |                     | OR | X \$220=        | 0                   |
|                                  | <input type="checkbox"/> Application Size Fee <small>(37 CFR 1.16(s))</small>                           |                                  |                                    |               |                         |                     |    |                 |                     |
|                                  | <input type="checkbox"/> FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM <small>(37 CFR 1.16(j))</small> |                                  |                                    |               |                         |                     | OR |                 |                     |
|                                  |   |                                  |                                    |               | TOTAL ADD'L FEE         |                     | OR | TOTAL ADD'L FEE | 0                   |

|           | (Column 1)  | (Column 2)                         | (Column 3)    |           |                     |    |           |                     |
|-----------|---|------------------------------------|---------------|-----------|---------------------|----|-----------|---------------------|
| AMENDMENT | CLAIMS REMAINING AFTER AMENDMENT  | HIGHEST NUMBER PREVIOUSLY PAID FOR | PRESENT EXTRA | RATE (\$) | ADDITIONAL FEE (\$) | OR | RATE (\$) | ADDITIONAL FEE (\$) |
|           | Total <small>(37 CFR 1.16(i))</small>   | *                                  | Minus **      | =         | X \$ =              |    | OR        | X \$ =              |
|           | Independent <small>(37 CFR 1.16(h))</small>   | *                                  | Minus ***     | =         | X \$ =              |    | OR        | X \$ =              |
|           | <input type="checkbox"/> Application Size Fee <small>(37 CFR 1.16(s))</small>                           |                                    |               |           |                     |    |           |                     |
|           | <input type="checkbox"/> FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM <small>(37 CFR 1.16(j))</small> |                                    |               |           |                     |    | OR        |                     |
|           |   |                                    |               |           | TOTAL ADD'L FEE     |    | OR        | TOTAL ADD'L FEE     |


\* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.  
 \*\* If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".  
 \*\*\* If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".

The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

Legal Instrument Examiner:  
 /VIOLA ROGERS/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

|  |  |  |
|--|--|--|
| <b>Application Number</b><br> | <b>Application/Control No.</b><br>11/104,202 | <b>Applicant(s)/Patent under Reexamination</b><br>BURTSCHER, MICHAEL |
|  |  |  |

|                             |  |
|-----------------------------|--|
| <b>Document Code - DISQ</b> | <b>Internal Document – DO NOT MAIL</b> |
|-----------------------------|--|

|                            |  |   |
|----------------------------|--|---|
| <b>TERMINAL DISCLAIMER</b> | <input checked="" type="checkbox"/> <b>APPROVED</b>    | <input type="checkbox"/> <b>DISAPPROVED</b> |
| Date Filed : 12/3/08       | <b>This patent is subject to a Terminal Disclaimer</b> |   |

|                                 |
|---------------------------------|
| <b>Approved/Disapproved by:</b> |
| BRIAN                           |



NOTICE OF ALLOWANCE AND FEE(S) DUE

22903 7590 03/23/2009

COOLEY GODWARD KRONISH LLP
ATTN: PATENT GROUP
Suite 1100
777 - 6th Street, NW
WASHINGTON, DC 20001

EXAMINER: CERVETTI, DAVID GARCIA
ART UNIT: 2436 PAPER NUMBER:
DATE MAILED: 03/23/2009

Table with 5 columns: APPLICATION NO., FILING DATE, FIRST NAMED INVENTOR, ATTORNEY DOCKET NO., CONFIRMATION NO.
11/104,202 04/12/2005 Michael Burtscher WEBR-011/00US 1284
TITLE OF INVENTION: SYSTEM AND METHOD FOR DIRECTLY ACCESSING DATA FROM A DATA STORAGE MEDIUM

Table with 7 columns: APPLN. TYPE, SMALL ENTITY, ISSUE FEE DUE, PUBLICATION FEE DUE, PREV. PAID ISSUE FEE, TOTAL FEE(S) DUE, DATE DUE
nonprovisional NO \$1510 \$300 \$0 \$1810 06/23/2009

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the SMALL ENTITY status shown above.

If the SMALL ENTITY is shown as YES, verify your current SMALL ENTITY status:

- A. If the status is the same, pay the TOTAL FEE(S) DUE shown above.
B. If the status above is to be removed, check box 5b on Part B - Fee(s) Transmittal and pay the PUBLICATION FEE (if required) and twice the amount of the ISSUE FEE shown above, or

If the SMALL ENTITY is shown as NO:

- A. Pay TOTAL FEE(S) DUE shown above, or
B. If applicant claimed SMALL ENTITY status before, or is now claiming SMALL ENTITY status, check box 5a on Part B - Fee(s) Transmittal and pay the PUBLICATION FEE (if required) and 1/2 the ISSUE FEE shown above.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Utility patents issuing on applications filed on or after Dec. 12, 1980 may require payment of maintenance fees. It is patentee's responsibility to ensure timely payment of maintenance fees when due.

**PART B - FEE(S) TRANSMITTAL**

**Complete and send this form, together with applicable fee(s), to: Mail Mail Stop ISSUE FEE  
 Commissioner for Patents  
 P.O. Box 1450  
 Alexandria, Virginia 22313-1450  
 or Fax (571)-273-2885**

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

22903 7590 03/23/2009

**COOLEY GODWARD KRONISH LLP**  
 ATTN: PATENT GROUP  
 Suite 1100  
 777 - 6th Street, NW  
 WASHINGTON, DC 20001

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

**Certificate of Mailing or Transmission**

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

|                    |
|--------------------|
| (Depositor's name) |
| (Signature)        |
| (Date)             |

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO.          | CONFIRMATION NO. |
|-----------------|-------------|----------------------|------------------------------|------------------|
| 11/104,202      | 04/12/2005  | Michael Burtscher    | WEBR-011/00US<br>303666-2011 | 1284             |

TITLE OF INVENTION: SYSTEM AND METHOD FOR DIRECTLY ACCESSING DATA FROM A DATA STORAGE MEDIUM

| APPLN. TYPE    | SMALL ENTITY | ISSUE FEE DUE | PUBLICATION FEE DUE | PREV. PAID ISSUE FEE | TOTAL FEE(S) DUE | DATE DUE   |
|----------------|--------------|---------------|---------------------|----------------------|------------------|------------|
| nonprovisional | NO           | \$1510        | \$300               | \$0                  | \$1810           | 06/23/2009 |

| EXAMINER               | ART UNIT | CLASS-SUBCLASS |
|------------------------|----------|----------------|
| CERVETTI, DAVID GARCIA | 2436     | 713-182000     |

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.

"Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list

(1) the names of up to 3 registered patent attorneys or agents OR, alternatively, 1 \_\_\_\_\_

(2) the name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed. 2 \_\_\_\_\_

3 \_\_\_\_\_

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE \_\_\_\_\_ (B) RESIDENCE: (CITY AND STATE OR COUNTRY) \_\_\_\_\_

Please check the appropriate assignee category or categories (will not be printed on the patent) :  Individual  Corporation or other private group entity  Government

4a. The following fee(s) are submitted:

Issue Fee

Publication Fee (No small entity discount permitted)

Advance Order - # of Copies \_\_\_\_\_

4b. Payment of Fee(s); (Please first reapply any previously paid issue fee shown above)

A check is enclosed.

Payment by credit card. Form PTO-2038 is attached.

The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment, to Deposit Account Number \_\_\_\_\_ (enclose an extra copy of this form).

5. Change in Entity Status (from status indicated above)

a. Applicant claims SMALL ENTITY status. See 37 CFR 1.27.  b. Applicant is no longer claiming SMALL ENTITY status. See 37 CFR 1.27(g)(2).

NOTE: The Issue Fee and Publication Fee (if required) will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the United States Patent and Trademark Office.

Authorized Signature \_\_\_\_\_ Date \_\_\_\_\_

Typed or printed name \_\_\_\_\_ Registration No. \_\_\_\_\_

This collection of information is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P. O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

Table with columns: APPLICATION NO., FILING DATE, FIRST NAMED INVENTOR, ATTORNEY DOCKET NO., CONFIRMATION NO.
Rows: 11/104,202 04/12/2005 Michael Burtscher WEBR-011/00US 1284
22903 7590 03/23/2009
COOLEY GODWARD KRONISH LLP
ATTN: PATENT GROUP
Suite 1100
777 - 6th Street, NW
WASHINGTON, DC 20001
EXAMINER: CERVETTI, DAVID GARCIA
ART UNIT: 2436 PAPER NUMBER: DATE MAILED: 03/23/2009

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(application filed on or after May 29, 2000)

The Patent Term Adjustment to date is 828 day(s). If the issue fee is paid on the date that is three months after the mailing date of this notice and the patent issues on the Tuesday before the date that is 28 weeks (six and a half months) after the mailing date of this notice, the Patent Term Adjustment will be 828 day(s).

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (http://pair.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.



**Notice of Allowability**

|  |   |  |
|--|---|--|
| <b>Application No.</b><br>11/104,202     | <b>Applicant(s)</b><br>BURTSCHER, MICHAEL |  |
| <b>Examiner</b><br>David García Cervetti | <b>Art Unit</b><br>2436                   |  |

**-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--**

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

- 1.  This communication is responsive to 12/3/08.
- 2.  The allowed claim(s) is/are 1-5,7-10,12-15 and 17.
- 3.  Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
  - a)  All   b)  Some\*   c)  None   of the:
    - 1.  Certified copies of the priority documents have been received.
    - 2.  Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
    - 3.  Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

\* Certified copies not received: \_\_\_\_\_.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.

**THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.**

- 4.  A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
  - 5.  CORRECTED DRAWINGS ( as "replacement sheets") must be submitted.
    - (a)  including changes required by the Notice of Draftsperson's Patent Drawing Review ( PTO-948) attached
      - 1)  hereto or 2)  to Paper No./Mail Date \_\_\_\_\_.
    - (b)  including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date \_\_\_\_\_.
- Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).**
- 6.  DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

**Attachment(s)**

- 1.  Notice of References Cited (PTO-892)
- 2.  Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3.  Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date \_\_\_\_\_
- 4.  Examiner's Comment Regarding Requirement for Deposit of Biological Material
- 5.  Notice of Informal Patent Application
- 6.  Interview Summary (PTO-413), Paper No./Mail Date \_\_\_\_\_.
- 7.  Examiner's Amendment/Comment
- 8.  Examiner's Statement of Reasons for Allowance
- 9.  Other \_\_\_\_\_.

/David García Cervetti/  
Primary Examiner, Art Unit 2436

### **DETAILED ACTION**

1. Applicant's arguments filed December 3, 2008, have been fully considered.
2. Claims 1-5, 7-10, 12-15, and 17 are pending and have been examined. Claims 6, 11, and 16 have been canceled.

### ***Response to Amendment***

3. The requirement for information is withdrawn due to the affidavits and manuals submitted in response.
4. The objection to the specification is withdrawn.
5. The provisional Double Patenting rejection is withdrawn in view of the Terminal Disclaimer filed on 12/3/08.
6. The rejection of claims 1-3, 7-8, and 12-13 under 35 USC 112, second paragraph, is withdrawn.

### ***Terminal Disclaimer***

7. The terminal disclaimer filed on 12/3/08 disclaiming the terminal portion of any patent granted on this application which would extend beyond the expiration date of US Patent 7,346,611 has been reviewed and is accepted. The terminal disclaimer has been recorded.

### ***Allowable Subject Matter***

8. Claims 1-5, 7-10, 12-15, and 17 are allowed.
9. Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably

Art Unit: 2436

accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

***Conclusion***

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to David García Cervetti whose telephone number is (571)272-5861. The examiner can normally be reached on Monday-Tuesday and Thursday-Friday.

11. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on (571)272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

12. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/David García Cervetti/  
Primary Examiner, Art Unit 2436

|                                   |                                       |   |             |
|-----------------------------------|---------------------------------------|---|-------------|
| <b>Notice of References Cited</b> | Application/Control No.<br>11/104,202 | Applicant(s)/Patent Under Reexamination<br>BURTSCHER, MICHAEL |             |
|                                   | Examiner<br>David García Cervetti     | Art Unit<br>2436  | Page 1 of 2 |

**U.S. PATENT DOCUMENTS**

| * |   | Document Number<br>Country Code-Number-Kind Code | Date<br>MM-YYYY | Name              | Classification |
|---|---|--|-----------------|-------------------|----------------|
| * | A | US-2003/0120947 A1                               | 06-2003         | Moore et al.      | 713/200        |
| * | B | US-2004/0199763 A1                               | 10-2004         | Freund, Gregor P. | 713/154        |
| * | C | US-2005/0155031 A1                               | 07-2005         | Wang et al.       | 717/170        |
| * | D | US-2005/0268112 A1                               | 12-2005         | Wang et al.       | 713/188        |
| * | E | US-2006/0010485 A1                               | 01-2006         | Gorman, Jim       | 726/003        |
| * | F | US-2006/0031940 A1                               | 02-2006         | Rozman et al.     | 726/027        |
| * | G | US-2006/0095967 A1                               | 05-2006         | Durham et al.     | 726/023        |
| * | H | US-2006/0101264 A1                               | 05-2006         | Costea et al.     | 713/165        |
| * | I | US-2006/0101282 A1                               | 05-2006         | Costea et al.     | 713/188        |
| * | J | US-2006/0200863 A1                               | 09-2006         | Ray et al.        | 726/024        |
| * | K | US-7,114,185 B2                                  | 09-2006         | Moore et al.      | 726/24         |
| * | L | US-2006/0272021 A1                               | 11-2006         | Marinescu et al.  | 726/024        |
| * | M | US-7,302,584 B2                                  | 11-2007         | Tarbotton et al.  | 713/188        |

**FOREIGN PATENT DOCUMENTS**

| * |   | Document Number<br>Country Code-Number-Kind Code | Date<br>MM-YYYY | Country | Name | Classification |
|---|---|--|-----------------|---------|------|----------------|
|   | N |  |                 |         |      |                |
|   | O |  |                 |         |      |                |
|   | P |  |                 |         |      |                |
|   | Q |  |                 |         |      |                |
|   | R |  |                 |         |      |                |
|   | S |  |                 |         |      |                |
|   | T |  |                 |         |      |                |

**NON-PATENT DOCUMENTS**

| * |   | Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages) |
|---|---|---|
|   | U |   |
|   | V |   |
|   | W |   |
|   | X |   |

\*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)  
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

|                                   |                                       |   |             |
|-----------------------------------|---------------------------------------|---|-------------|
| <b>Notice of References Cited</b> | Application/Control No.<br>11/104,202 | Applicant(s)/Patent Under Reexamination<br>BURTSCHER, MICHAEL |             |
|                                   | Examiner<br>David García Cervetti     | Art Unit<br>2436  | Page 2 of 2 |

**U.S. PATENT DOCUMENTS**

| * | Document Number<br>Country Code-Number-Kind Code | Date<br>MM-YYYY | Name               | Classification |
|---|--|-----------------|--------------------|----------------|
| * | A US-2007/0283439 A1                             | 12-2007         | Ballard, Clinton L | 726/24         |
| * | B US-7,383,581 B1                                | 06-2008         | Moore et al.       | 726/24         |
|   | C US-  |                 |                    |                |
|   | D US-  |                 |                    |                |
|   | E US-  |                 |                    |                |
|   | F US-  |                 |                    |                |
|   | G US-  |                 |                    |                |
|   | H US-  |                 |                    |                |
|   | I US-  |                 |                    |                |
|   | J US-  |                 |                    |                |
|   | K US-  |                 |                    |                |
|   | L US-  |                 |                    |                |
|   | M US-  |                 |                    |                |

**FOREIGN PATENT DOCUMENTS**

| * | Document Number<br>Country Code-Number-Kind Code | Date<br>MM-YYYY | Country | Name | Classification |
|---|--|-----------------|---------|------|----------------|
|   | N  |                 |         |      |                |
|   | O  |                 |         |      |                |
|   | P  |                 |         |      |                |
|   | Q  |                 |         |      |                |
|   | R  |                 |         |      |                |
|   | S  |                 |         |      |                |
|   | T  |                 |         |      |                |

**NON-PATENT DOCUMENTS**

| * | Document Number<br>Country Code-Number-Kind Code | Date<br>MM-YYYY   | Country | Name | Classification |
|---|--|---|---------|------|----------------|
|   | U  | Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages) |         |      |                |
|   | V  |   |         |      |                |
|   | W  |   |         |      |                |
|   | X  |   |         |      |                |

\*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)  
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

## EAST Search History

| Ref # | Hits | Search Query  | DBs             | Default Operator | Plurals | Time Stamp       |
|-------|------|---|-----------------|------------------|---------|------------------|
| L1    | 515  | (sort\$ order\$) with (file document) with (physical near4 location memory near4 location)  | US-PGPUB; USPAT | OR               | ON      | 2009/03/15 16:37 |
| L2    | 224  | (sort\$ order\$) near7 (file document) near7 (physical near4 location memory near4 location)  | US-PGPUB; USPAT | OR               | ON      | 2009/03/15 16:37 |
| L3    | 7    | (sort\$ order\$) near7 (file document) near7 (physical near4 location memory near4 location) with (scan\$ analyz\$ analysis )   | US-PGPUB; USPAT | OR               | ON      | 2009/03/15 16:39 |
| L4    | 37   | (sort\$ order\$) with (file document) with (physical near4 location memory near4 location) and (scan \$ analyz\$ analysis ) with (virus antivirus anti adj virus pestware spyware trojan spy-ware pest-ware)                  | US-PGPUB; USPAT | OR               | ON      | 2009/03/15 16:47 |
| L5    | 37   | (sort\$ order\$) with (file document) with (physical near4 location memory near4 location) and (scan \$ analyz\$ analysis ) with (virus antivirus anti adj virus pestware spyware trojan spy-ware pest-ware malware mal-ware) | US-PGPUB; USPAT | OR               | ON      | 2009/03/15 16:47 |
| L6    | 9    | ("6542943"   "6748534"   "6886099"   "6928555"   "6963978"   "6973578"   "6980992"   "6993660"   "7020895").PN.   | US-PGPUB; USPAT | OR               | ON      | 2009/03/15 16:49 |
| L7    | 2    | ("6542943"   "6748534"   "6886099"   "6928555"   "6963978"   "6973578"   "6980992"   "6993660"   "7020895").PN. and (sort \$)   | US-PGPUB; USPAT | OR               | ON      | 2009/03/15 16:51 |
| L8    | 1476 | 726/22.ccls.  | US-PGPUB; USPAT | OR               | ON      | 2009/03/15 16:51 |

|     |      |  |                    |    |    |                     |
|-----|------|--|--------------------|----|----|---------------------|
| L9  | 1020 | 726/23.ccls.   | US-PGPUB;<br>USPAT | OR | ON | 2009/03/15<br>16:51 |
| L10 | 858  | 726/24.ccls.   | US-PGPUB;<br>USPAT | OR | ON | 2009/03/15<br>16:51 |
| L11 | 613  | 726/25.ccls.   | US-PGPUB;<br>USPAT | OR | ON | 2009/03/15<br>16:51 |
| L12 | 470  | 713/187.ccls.  | US-PGPUB;<br>USPAT | OR | ON | 2009/03/15<br>16:52 |
| L13 | 554  | 713/188.ccls.  | US-PGPUB;<br>USPAT | OR | ON | 2009/03/15<br>16:52 |
| L14 | 1686 | 713/182.ccls.  | US-PGPUB;<br>USPAT | OR | ON | 2009/03/15<br>17:28 |
| L15 | 894  | 717/127.ccls.  | US-PGPUB;<br>USPAT | OR | ON | 2009/03/15<br>17:33 |
| L16 | 604  | 717/131.ccls.  | US-PGPUB;<br>USPAT | OR | ON | 2009/03/15<br>17:33 |
| L17 | 1    | "20060101282".pn.  | US-PGPUB;<br>USPAT | OR | ON | 2009/03/15<br>17:34 |
| L18 | 1    | "20060101282".pn. and<br>(sort\$ order\$)  | US-PGPUB;<br>USPAT | OR | ON | 2009/03/15<br>17:34 |
| L19 | 1    | "20060230291".pn. and<br>(sort\$ order\$)  | US-PGPUB;<br>USPAT | OR | ON | 2009/03/15<br>17:37 |
| S1  | 50   | ("7346611"  <br>"20060230290"  <br>"20060230291"  <br>"20070124267"  <br>"20060277182"  <br>"20060277183"  <br>"7349931"  <br>"20060074896"  <br>"20060236397"  <br>"20070006311"  <br>"20080028466"  <br>"20070250818"  <br>"20080028462"  <br>"20070250817"  <br>"20060075501"  <br>"20070094496"  <br>"20070203884"  <br>"20060236389"  <br>"20060236396"  <br>"20070074289"  <br>"4757533"   "5144659"  <br>"5289540"   "5307497"  <br>"5881287"   "6105140"  <br>"6233576"   "6272611"  <br>"6317742"   "6993642"  <br>"6993649"   "7024581"  <br>"7318163"   "7395394"  <br>"20030023839"  <br>"20040111250" | US-PGPUB;<br>USPAT | OR | ON | 2008/09/11<br>10:27 |

|    |      |  |                    |    |    |                     |
|----|------|--|--------------------|----|----|---------------------|
|    |      | "20040117610"  <br>"20050039032"  <br>"20060031937"  <br>"20070186070"  <br>"20070226704"  <br>"20070261117"  <br>"20080010310"  <br>"20080028388"  <br>"4761737"   "7053936"  <br>"7120763"   "7203865"  <br>"20030011687"  <br>"20040143736").PN.  |                    |    |    |                     |
| S2 | 50   | ("20060230291"  <br>"20060277182"  <br>"20060277183"  <br>"20070124267"  <br>"7346611"   "7349931"  <br>"20060230290"  <br>"20060236389"  <br>"20060236397"  <br>"20070006311"  <br>"20070073792"  <br>"20060265761"  <br>"20070203884"  <br>"20070074289"  <br>"20070094496"  <br>"20070226704"  <br>"4757533"   "5586301"  <br>"5657470"   "5926652"  <br>"5944821"   "5745701"  <br>"5974547"   "6154751"  <br>"6971018"   "5032979"  <br>"5261089"   "5289540"  <br>"5361359"   "5363446"  <br>"5475625"   "5537540"  <br>"5675833"   "5694583"  <br>"5710941"   "5758174"  <br>"5842002"   "5881287"  <br>"5892902"   "6092198"  <br>"6101607"   "6112312"  <br>"6175924"   "6199166"  <br>"6233576"   "6237023"  <br>"6269456"   "6366988"  <br>"6385645"   "6769075").<br>PN. | US-PGPUB;<br>USPAT | OR | ON | 2008/09/11<br>10:28 |
| S3 | 18   | S1 and S2  | US-PGPUB;<br>USPAT | OR | ON | 2008/09/11<br>10:28 |
| S4 | 1575 | 713/182.ccls.  | US-PGPUB;<br>USPAT | OR | ON | 2008/09/11<br>10:28 |
| S5 | 618  | 713/183.ccls.  | US-PGPUB;<br>USPAT | OR | ON | 2008/09/11<br>10:28 |
| S6 | 518  | 713/188.ccls.  | US-PGPUB;<br>USPAT | OR | ON | 2008/09/11<br>10:28 |




|     |      |  |                    |    |    |                     |
|-----|------|--|--------------------|----|----|---------------------|
| S7  | 756  | 726/24.ccls.   | US-PGPUB;<br>USPAT | OR | ON | 2008/09/11<br>10:29 |
| S8  | 888  | 726/23.ccls.   | US-PGPUB;<br>USPAT | OR | ON | 2008/09/11<br>10:29 |
| S9  | 1286 | 726/22.ccls.   | US-PGPUB;<br>USPAT | OR | ON | 2008/09/11<br>10:29 |
| S10 | 812  | 717/127.ccls.  | US-PGPUB;<br>USPAT | OR | ON | 2008/09/11<br>10:29 |
| S11 | 555  | 717/131.ccls.  | US-PGPUB;<br>USPAT | OR | ON | 2008/09/11<br>10:29 |
| S12 | 1    | "20060085528".pn.  | US-PGPUB;<br>USPAT | OR | ON | 2008/09/11<br>11:39 |
| S13 | 28   | (pestware spyware<br>malware adware<br>scumware spamware)<br>near5 circumvent\$  | US-PGPUB;<br>USPAT | OR | ON | 2008/09/11<br>12:30 |
| S14 | 3    | (pestware spyware<br>malware adware<br>scumware spamware)<br>near5 (analyz\$) near8<br>location  | US-PGPUB;<br>USPAT | OR | ON | 2008/09/11<br>12:34 |
| S15 | 1    | pestpatrol   | US-PGPUB;<br>USPAT | OR | ON | 2008/09/11<br>12:45 |
| S16 | 3    | pestpatrol pest adj patrol   | US-PGPUB;<br>USPAT | OR | ON | 2008/09/11<br>12:48 |
| S17 | 1    | spysweeper spy adj<br>sweeper  | US-PGPUB;<br>USPAT | OR | ON | 2008/09/11<br>12:50 |
| S18 | 9    | ad-aware   | US-PGPUB;<br>USPAT | OR | ON | 2008/09/11<br>12:50 |
| S19 | 50   | ("20060277182"<br>"20060277183"<br>"7346611" "7349931"<br>"20060230290"<br>"20060230291"<br>"20060236389"<br>"20060236397"<br>"20070006311"<br>"20070073792"<br>"20070124267"<br>"20060265761"<br>"20060074896"<br>"20070074289"<br>"20070094496"<br>"20070203884"<br>"20070250817"<br>"20070250928"<br>"20070261117"<br>"20070169198"<br>"20070226704"<br>"20060085528" | US-PGPUB;<br>USPAT | OR | ON | 2008/09/11<br>12:53 |

|     |     |   |                    |    |    |                     |
|-----|-----|---|--------------------|----|----|---------------------|
|     |     | "20060212940"<br>"20060236396"<br>"20070094732"<br>"20070169197"<br>"20070168694"<br>"20080010310"<br>"20080034430"<br>"20080052679"<br>"20070094726"<br>"20070094733"<br>"20070168982"<br>"20070169191"<br>"20070180520"<br>"20070226800"<br>"20070250818"<br>"20070300303"<br>"20080127352"<br>"4757533" "6122629"<br>"6148402" "5586301"<br>"5657470" "5944821"<br>"6154751" "5361359"<br>"5475625" "5740433"<br>"5745701" ).pn. |                    |    |    |                     |
| S20 | 401 | (pestware spyware<br>malware adware<br>scumware spamware).<br>clm.  | US-PGPUB;<br>USPAT | OR | ON | 2008/09/11<br>16:20 |
| S21 | 137 | (pestware spyware<br>malware adware<br>scumware spamware).<br>clm. with file.clm.   | US-PGPUB;<br>USPAT | OR | ON | 2008/09/11<br>16:20 |
| S22 | 26  | (pestware spyware<br>malware adware<br>scumware spamware).<br>clm. with file.clm. and<br>table.clm.   | US-PGPUB;<br>USPAT | OR | ON | 2008/09/11<br>16:21 |
| S23 | 7   | (pestware spyware<br>malware adware<br>scumware spamware).<br>clm. and master adj file<br>adj table.clm.  | US-PGPUB;<br>USPAT | OR | ON | 2008/09/11<br>16:21 |
| S24 | 5   | (pestware spyware<br>malware adware<br>scumware spamware).<br>clm. and master adj file<br>adj table.clm. and scan\$.<br>clm.  | US-PGPUB;<br>USPAT | OR | ON | 2008/09/11<br>16:25 |

3/15/2009 5:38:40 PM

C:\Documents and Settings\dcervetti\My Documents\EAST\Workspaces\11-104-202-09-11-2008.  
wsp

|  |  |  |
|--|--|--|
| <b><i>Index of Claims</i></b><br><br> | <b>Application/Control No.</b><br><br>11104202 | <b>Applicant(s)/Patent Under Reexamination</b><br><br>BURTSCHER, MICHAEL |
|  | <b>Examiner</b><br><br>David García Cervetti   | <b>Art Unit</b><br><br>2436  |

|   |                 |
|---|-----------------|
| ✓ | <b>Rejected</b> |
| = | <b>Allowed</b>  |


|   |                   |
|---|-------------------|
| - | <b>Cancelled</b>  |
| ÷ | <b>Restricted</b> |

|   |                     |
|---|---------------------|
| N | <b>Non-Elected</b>  |
| I | <b>Interference</b> |

|   |                 |
|---|-----------------|
| A | <b>Appeal</b>   |
| O | <b>Objected</b> |

Claims renumbered in the same order as presented by applicant
  CPA
  T.D.
  R.1.47


| CLAIM |          | DATE       |            |  |  |  |  |  |  |
|-------|----------|------------|------------|--|--|--|--|--|--|
| Final | Original | 09/11/2008 | 03/15/2009 |  |  |  |  |  |  |
| 1     | 1        | ✓          | =          |  |  |  |  |  |  |
| 2     | 2        | ✓          | =          |  |  |  |  |  |  |
| 3     | 3        | ✓          | =          |  |  |  |  |  |  |
| 4     | 4        | ✓          | =          |  |  |  |  |  |  |
| 5     | 5        | ✓          | =          |  |  |  |  |  |  |
|       | 6        | ✓          | -          |  |  |  |  |  |  |
| 6     | 7        | ✓          | =          |  |  |  |  |  |  |
| 7     | 8        | ✓          | =          |  |  |  |  |  |  |
| 8     | 9        | ✓          | =          |  |  |  |  |  |  |
| 9     | 10       | ✓          | =          |  |  |  |  |  |  |
|       | 11       | ✓          | -          |  |  |  |  |  |  |
| 10    | 12       | ✓          | =          |  |  |  |  |  |  |
| 11    | 13       | ✓          | =          |  |  |  |  |  |  |
| 12    | 14       | ✓          | =          |  |  |  |  |  |  |
| 13    | 15       | ✓          | =          |  |  |  |  |  |  |
|       | 16       | ✓          | -          |  |  |  |  |  |  |
| 14    | 17       | ✓          | =          |  |  |  |  |  |  |

|   |  |  |
|---|--|--|
| <b>Issue Classification</b><br> | <b>Application/Control No.</b><br>11104202 | <b>Applicant(s)/Patent Under Reexamination</b><br>BURTSCHER, MICHAEL |
|   | <b>Examiner</b><br>David García Cervetti   | <b>Art Unit</b><br>2436  |

| ORIGINAL                  |                                   |          |     |  | INTERNATIONAL CLASSIFICATION |   |   |   |                      |             |  |  |  |  |  |  |  |  |  |
|---------------------------|-----------------------------------|----------|-----|--|------------------------------|---|---|---|----------------------|-------------|--|--|--|--|--|--|--|--|--|
| CLASS                     |                                   | SUBCLASS |     |  | CLAIMED                      |   |   |   |                      | NON-CLAIMED |  |  |  |  |  |  |  |  |  |
| 726                       |                                   | 24       |     |  | G                            | 0 | 6 | F | 11 / 00 (2006.01.01) |             |  |  |  |  |  |  |  |  |  |
| <b>CROSS REFERENCE(S)</b> |                                   |          |     |  |                              |   |   |   |                      |             |  |  |  |  |  |  |  |  |  |
| CLASS                     | SUBCLASS (ONE SUBCLASS PER BLOCK) |          |     |  |                              |   |   |   |                      |             |  |  |  |  |  |  |  |  |  |
| 726                       | 22                                | 23       | 25  |  |                              |   |   |   |                      |             |  |  |  |  |  |  |  |  |  |
| 713                       | 182                               | 187      | 188 |  |                              |   |   |   |                      |             |  |  |  |  |  |  |  |  |  |
| 717                       | 127                               | 131      |     |  |                              |   |   |   |                      |             |  |  |  |  |  |  |  |  |  |
|                           |                                   |          |     |  |                              |   |   |   |                      |             |  |  |  |  |  |  |  |  |  |
|                           |                                   |          |     |  |                              |   |   |   |                      |             |  |  |  |  |  |  |  |  |  |
|                           |                                   |          |     |  |                              |   |   |   |                      |             |  |  |  |  |  |  |  |  |  |
|                           |                                   |          |     |  |                              |   |   |   |                      |             |  |  |  |  |  |  |  |  |  |
|                           |                                   |          |     |  |                              |   |   |   |                      |             |  |  |  |  |  |  |  |  |  |
|                           |                                   |          |     |  |                              |   |   |   |                      |             |  |  |  |  |  |  |  |  |  |
|                           |                                   |          |     |  |                              |   |   |   |                      |             |  |  |  |  |  |  |  |  |  |
|                           |                                   |          |     |  |                              |   |   |   |                      |             |  |  |  |  |  |  |  |  |  |
|                           |                                   |          |     |  |                              |   |   |   |                      |             |  |  |  |  |  |  |  |  |  |
|                           |                                   |          |     |  |                              |   |   |   |                      |             |  |  |  |  |  |  |  |  |  |
|                           |                                   |          |     |  |                              |   |   |   |                      |             |  |  |  |  |  |  |  |  |  |

| <input type="checkbox"/> Claims renumbered in the same order as presented by applicant |          |       |          |       |          |       |          |       |          |       |          |       |          |       |          | <input type="checkbox"/> CPA |          |       |          |       |          |       |          |       |          |       |          |  |  |  |  | <input checked="" type="checkbox"/> T.D. |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | <input type="checkbox"/> R.1.47 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|--|----------|-------|----------|-------|----------|-------|----------|-------|----------|-------|----------|-------|----------|-------|----------|------------------------------|----------|-------|----------|-------|----------|-------|----------|-------|----------|-------|----------|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|---------------------------------|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|
| Final  | Original | Final | Original | Final | Original | Final | Original | Final | Original | Final | Original | Final | Original | Final | Original | Final                        | Original | Final | Original | Final | Original | Final | Original | Final | Original | Final | Original |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |                                 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 1  | 1        | 14    | 17       |       |          |       |          |       |          |       |          |       |          |       |          |                              |          |       |          |       |          |       |          |       |          |       |          |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |                                 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 2  | 2        |       |          |       |          |       |          |       |          |       |          |       |          |       |          |                              |          |       |          |       |          |       |          |       |          |       |          |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |                                 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 3  | 3        |       |          |       |          |       |          |       |          |       |          |       |          |       |          |                              |          |       |          |       |          |       |          |       |          |       |          |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |                                 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 4  | 4        |       |          |       |          |       |          |       |          |       |          |       |          |       |          |                              |          |       |          |       |          |       |          |       |          |       |          |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |                                 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 5  | 5        |       |          |       |          |       |          |       |          |       |          |       |          |       |          |                              |          |       |          |       |          |       |          |       |          |       |          |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |                                 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | 6        |       |          |       |          |       |          |       |          |       |          |       |          |       |          |                              |          |       |          |       |          |       |          |       |          |       |          |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |                                 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 6  | 7        |       |          |       |          |       |          |       |          |       |          |       |          |       |          |                              |          |       |          |       |          |       |          |       |          |       |          |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |                                 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 7  | 8        |       |          |       |          |       |          |       |          |       |          |       |          |       |          |                              |          |       |          |       |          |       |          |       |          |       |          |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |                                 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 8  | 9        |       |          |       |          |       |          |       |          |       |          |       |          |       |          |                              |          |       |          |       |          |       |          |       |          |       |          |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |                                 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 9  | 10       |       |          |       |          |       |          |       |          |       |          |       |          |       |          |                              |          |       |          |       |          |       |          |       |          |       |          |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |                                 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | 11       |       |          |       |          |       |          |       |          |       |          |       |          |       |          |                              |          |       |          |       |          |       |          |       |          |       |          |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |                                 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 10   | 12       |       |          |       |          |       |          |       |          |       |          |       |          |       |          |                              |          |       |          |       |          |       |          |       |          |       |          |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |                                 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 11   | 13       |       |          |       |          |       |          |       |          |       |          |       |          |       |          |                              |          |       |          |       |          |       |          |       |          |       |          |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |                                 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 12   | 14       |       |          |       |          |       |          |       |          |       |          |       |          |       |          |                              |          |       |          |       |          |       |          |       |          |       |          |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |                                 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 13   | 15       |       |          |       |          |       |          |       |          |       |          |       |          |       |          |                              |          |       |          |       |          |       |          |       |          |       |          |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |                                 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | 16       |       |          |       |          |       |          |       |          |       |          |       |          |       |          |                              |          |       |          |       |          |       |          |       |          |       |          |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |                                 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

|  |        |                              |                   |
|--|--------|------------------------------|-------------------|
| NONE   |        | <b>Total Claims Allowed:</b> |                   |
|  |        | 14                           |                   |
| (Assistant Examiner)                                       | (Date) | O.G. Print Claim(s)          | O.G. Print Figure |
| /David García Cervetti/<br>Primary Examiner. Art Unit 2436 |        | 1                            | 1                 |
| (Primary Examiner)   | (Date) |                              |                   |

|  |  |  |
|--|--|--|
| <b>Search Notes</b><br><br> | <b>Application/Control No.</b><br><br>11104202 | <b>Applicant(s)/Patent Under Reexamination</b><br><br>BURTSCHER, MICHAEL |
|  | <b>Examiner</b><br><br>David García Cervetti   | <b>Art Unit</b><br><br>2436  |

| <b>SEARCHED</b> |                 |             |                 |
|-----------------|-----------------|-------------|-----------------|
| <b>Class</b>    | <b>Subclass</b> | <b>Date</b> | <b>Examiner</b> |
| 713             | 182,188         | 3/12/09     | DGC             |
| 726             | 22,23,24        | 3/12/09     | DGC             |
| 717             | 127,131         | 3/12/09     | DGC             |

| <b>SEARCH NOTES</b>   |             |                 |
|---|-------------|-----------------|
| <b>Search Notes</b>   | <b>Date</b> | <b>Examiner</b> |
| Inventor name search, ACM, IEEE, Springer, Altavista, Google, Scholar, ACE, PLUS, EAST history attached | 3/12/09     | DGC             |

| <b>INTERFERENCE SEARCH</b> |                 |             |                 |
|----------------------------|-----------------|-------------|-----------------|
| <b>Class</b>               | <b>Subclass</b> | <b>Date</b> | <b>Examiner</b> |
| 726                        | 22,23,24,25     | 3/12/09     | DGC             |
| 713                        | 182, 187, 188   | 3/12/09     | DGC             |
| 717                        | 127,131         | 3/12/09     | DGC             |

|  |   |
|--|---|
|  | / David García Cervetti/<br>Primary Examiner. Art Unit 2436 |
|--|---|

|   |        |                          |                            |
|---|--------|--------------------------|----------------------------|
| Substitute for form 1449A/PTO<br><br><b>INFORMATION DISCLOSURE<br/>                 STATEMENT BY APPLICANT</b><br><br>(use as many sheets as necessary) |        | <i>Complete if Known</i> |                            |
|   |        | Application Number       | 11/104,202                 |
|   |        | Filing Date              | 04/12/2005                 |
|   |        | First Named Inventor     | Michael BURTSCHER          |
|   |        | Group Art Unit           | 2161                       |
|   |        | Examiner Name            | Not Yet Assigned           |
| Sheet   | 1 of 1 | Attorney Docket Number   | WEBR-01 I/00US 303666-2011 |

| U.S. PATENT DOCUMENTS |                       |   |                                |  |  |
|-----------------------|-----------------------|---|--------------------------------|--|--|
| Examiner Initials*    | Cite No. <sup>1</sup> | Document Number                             | Publication Date<br>MM-DD-YYYY | Name of Patentee or Applicant of<br>Cited Document | Pages, Columns, Lines, Where Relevant<br>Passages or Relevant Figures Appear |
|                       |                       | Number-Kind Code <sup>2</sup> (if<br>known) |                                |  |  |
| /DGC/                 |                       | US-2006/0074896 A1                          | 04/06/2006                     | Thomas   |  |
| /DGC/                 |                       | US-2006/0075501 A1                          | 04/06/2006                     | Thomas   |  |
| /DGC/                 |                       | US-2006/0085528 A1                          | 04/20/2006                     | Thomas   |  |
| /DGC/                 |                       | US-2006/0288416 A1                          | 12/21/2006                     | Costea   |  |
| /DGC/                 |                       | US-5,715,455 A                              | 02/03/1998                     | Macon  |  |
| /DGC/                 |                       | US-6,173,291                                | 01/09/2001                     | Jenevein   |  |
| /DGC/                 |                       | US-7,346,611 <del>3</del> 1,2008            | <del>10/12/2006</del>          | Burtscher  |  |
| /DGC/                 |                       | US-6,667,751                                | 12/23/2003                     | Wynn   |  |

JS  
4122109

|                    |                         |                 |            |
|--------------------|-------------------------|-----------------|------------|
| Examiner Signature | /David Garcia Cervetti/ | Date Considered | 09/15/2006 |
|--------------------|-------------------------|-----------------|------------|

\*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. <sup>1</sup>Unique citation designation number (optional). <sup>2</sup>See attached Kinds of U.S. Patent Documents. <sup>3</sup>Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). <sup>4</sup>For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. <sup>5</sup>Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. <sup>6</sup>Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

**PART B - FEE(S) TRANSMITTAL**

**Complete and send this form, together with applicable fee(s), to: Mail Mail Stop ISSUE FEE  
 Commissioner for Patents  
 P.O. Box 1450  
 Alexandria, Virginia 22313-1450  
 or Fax (571)-273-2885**

**INSTRUCTIONS:** This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

22903 7590 03/23/2009

**COOLEY GODWARD KRONISH LLP**  
 ATTN: PATENT GROUP  
 Suite 1100  
 777 - 6th Street, NW  
 WASHINGTON, DC 20001

**EFS Filing** filed via **EFS**  
 Certificate of Mailing or Transmission  
 I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

|                             |                    |
|-----------------------------|--------------------|
| <b>Sherry Duncan Bitler</b> | (Depositor's name) |
| <i>Sherry Duncan Bitler</i> | (Signature)        |
| 6/15/09                     | (Date)             |

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO.          | CONFIRMATION NO. |
|-----------------|-------------|----------------------|------------------------------|------------------|
| 11/104,202      | 04/12/2005  | Michael Burtscher    | WEBR-011/00US<br>303666-2011 | 1284             |

TITLE OF INVENTION: SYSTEM AND METHOD FOR DIRECTLY ACCESSING DATA FROM A DATA STORAGE MEDIUM

| APPLN. TYPE    | SMALL ENTITY | ISSUE FEE DUE | PUBLICATION FEE DUE | PREV. PAID ISSUE FEE | TOTAL FEE(S) DUE | DATE DUE   |
|----------------|--------------|---------------|---------------------|----------------------|------------------|------------|
| nonprovisional | NO           | \$1510        | \$300               | \$0                  | \$1810           | 06/23/2009 |

| EXAMINER               | ART UNIT | CLASS-SUBCLASS |
|------------------------|----------|----------------|
| CERVETTI, DAVID GARCIA | 2436     | 713-182000     |

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).  
 Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.  
 "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. Use of a Customer Number is required.

2. For printing on the patent front page, list  
 (1) the names of up to 3 registered patent attorneys or agents OR, alternatively,  
 (2) the name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1 Cooley Godward Kronish LLP  
 2 \_\_\_\_\_  
 3 \_\_\_\_\_

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE

(B) RESIDENCE: (CITY and STATE OR COUNTRY)

Webroot Software, Inc.

Boulder, CO

Please check the appropriate assignee category or categories (will not be printed on the patent):  Individual  Corporation or other private group entity  Government

4a. The following fee(s) are submitted:

Issue Fee  
 Publication Fee (No small entity discount permitted)  
 Advance Order - # of Copies \_\_\_\_\_

4b. Payment of Fee(s): (Please first reapply any previously paid issue fee shown above)

A check is enclosed.  
 Payment by credit card. Form PTO-2038 is attached.  
 The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment, to Deposit Account Number 501283 (enclose an extra copy of this form).

5. Change in Entity Status (from status indicated above)

a. Applicant claims SMALL ENTITY status. See 37 CFR 1.27.  b. Applicant is no longer claiming SMALL ENTITY status. See 37 CFR 1.27(g)(2).

NOTE: The Issue Fee and Publication Fee (if required) will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the United States Patent and Trademark Office.

Authorized Signature Thomas M. Croft  
 Typed or printed name Thomas M. Croft

Date 6/15/09  
 Registration No. 44,051

This collection of information is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

## Electronic Patent Application Fee Transmittal

|   |  |
|---|--|
| <b>Application Number:</b>                  | 11104202   |
| <b>Filing Date:</b>                         | 12-Apr-2005  |
| <b>Title of Invention:</b>                  | SYSTEM AND METHOD FOR DIRECTLY ACCESSING DATA FROM A DATA STORAGE MEDIUM |
| <b>First Named Inventor/Applicant Name:</b> | Michael Burtscher  |
| <b>Filer:</b>                               | Thomas M. Croft/Sherry Bitler  |
| <b>Attorney Docket Number:</b>              | WEBR-011/00US 303666-2011  |

Filed as Large Entity

### Utility under 35 USC 111(a) Filing Fees

| Description                              | Fee Code | Quantity | Amount | Sub-Total in USD(\$) |
|--|----------|----------|--------|----------------------|
| <b>Basic Filing:</b>                     |          |          |        |                      |
| <b>Pages:</b>                            |          |          |        |                      |
| <b>Claims:</b>                           |          |          |        |                      |
| <b>Miscellaneous-Filing:</b>             |          |          |        |                      |
| <b>Petition:</b>                         |          |          |        |                      |
| <b>Patent-Appeals-and-Interference:</b>  |          |          |        |                      |
| <b>Post-Allowance-and-Post-Issuance:</b> |          |          |        |                      |
| Utility Appl issue fee                   | 1501     | 1        | 1510   | 1510                 |
| Publ. Fee- early, voluntary, or normal   | 1504     | 1        | 300    | 300                  |



| Description               | Fee Code | Quantity | Amount | Sub-Total in USD(\$) |
|---------------------------|----------|----------|--------|----------------------|
| <b>Extension-of-Time:</b> |          |          |        |                      |
| <b>Miscellaneous:</b>     |          |          |        |                      |
| <b>Total in USD (\$)</b>  |          |          |        | <b>1810</b>          |

## Electronic Acknowledgement Receipt

|   |  |
|---|--|
| <b>EFS ID:</b>                              | 5514785  |
| <b>Application Number:</b>                  | 11104202   |
| <b>International Application Number:</b>    |  |
| <b>Confirmation Number:</b>                 | 1284   |
| <b>Title of Invention:</b>                  | SYSTEM AND METHOD FOR DIRECTLY ACCESSING DATA FROM A DATA STORAGE MEDIUM |
| <b>First Named Inventor/Applicant Name:</b> | Michael Burtscher  |
| <b>Customer Number:</b>                     | 22903  |
| <b>Filer:</b>                               | Thomas M. Croft/Sherry Bitler  |
| <b>Filer Authorized By:</b>                 | Thomas M. Croft  |
| <b>Attorney Docket Number:</b>              | WEBR-011/00US 303666-2011  |
| <b>Receipt Date:</b>                        | 15-JUN-2009  |
| <b>Filing Date:</b>                         | 12-APR-2005  |
| <b>Time Stamp:</b>                          | 20:16:15   |
| <b>Application Type:</b>                    | Utility under 35 USC 111(a)  |

### Payment information:

|  |                 |
|--|-----------------|
| Submitted with Payment                   | yes             |
| Payment Type                             | Deposit Account |
| Payment was successfully received in RAM | \$1810          |
| RAM confirmation Number                  | 5588            |
| Deposit Account                          | 501283          |
| Authorized User                          |                 |

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)

**File Listing:**

| Document Number | Document Description        | File Name            | File Size(Bytes)/<br>Message Digest                              | Multi Part /.zip | Pages (if appl.) |
|-----------------|-----------------------------|----------------------|--|------------------|------------------|
| 1               | Issue Fee Payment (PTO-85B) | WEBR01100USpartB.pdf | 127561<br><small>2d2aff0defd71c11ee846c9246cf2b49cefb965</small> | no               | 1                |

**Warnings:****Information:**

|   |                         |              |  |    |   |
|---|-------------------------|--------------|--|----|---|
| 2 | Fee Worksheet (PTO-875) | fee-info.pdf | 31950<br><small>fce2e6d516c632ad81deff4e86a10911c41419db</small> | no | 2 |
|---|-------------------------|--------------|--|----|---|

**Warnings:****Information:**

|                                     |        |
|-------------------------------------|--------|
| <b>Total Files Size (in bytes):</b> | 159511 |
|-------------------------------------|--------|

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

**New Applications Under 35 U.S.C. 111**

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

**National Stage of an International Application under 35 U.S.C. 371**

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

**New International Application Filed with the USPTO as a Receiving Office**

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

| APPLICATION NO. | ISSUE DATE | PATENT NO. | ATTORNEY DOCKET NO.       | CONFIRMATION NO. |
|-----------------|------------|------------|---------------------------|------------------|
| 11/104,202      | 07/21/2009 | 7565695    | WEBR-011/00US 303666-2011 | 1284             |

22903 7590 07/01/2009  
COOLEY GODWARD KRONISH LLP  
ATTN: PATENT GROUP  
Suite 1100  
777 - 6th Street, NW  
WASHINGTON, DC 20001

## ISSUE NOTIFICATION

The projected patent number and issue date are specified above.

### **Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)** (application filed on or after May 29, 2000)

The Patent Term Adjustment is 828 day(s). Any patent to issue from the above-identified application will include an indication of the adjustment on the front page.

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (<http://pair.uspto.gov>).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at (571)-272-4200.

APPLICANT(s) (Please see PAIR WEB site <http://pair.uspto.gov> for additional applicants):

Michael Burtscher, Longmont, CO;

**UNITED STATES PATENT AND TRADEMARK OFFICE  
CERTIFICATE OF CORRECTION**

**PATENT NO.:** 7565695

Page 1 of 1

**DATED:** June 07, 2010

**INVENTOR(S):** Michael Burtscher

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

Inventors: Michael Burtscher, Longmont, CO (US)  
Tony Nichols, Erie, CO (US)

/David García Cervetti/  
Primary Examiner, Art Unit 2436

UNITED STATES PATENT AND TRADEMARK OFFICE  
**CERTIFICATE OF CORRECTION**

PATENT NO. : 7,565,695 B2  
APPLICATION NO. : 11/104202  
DATED : July 21, 2009  
INVENTOR(S) : Michael Burtscher and Tony Nichols

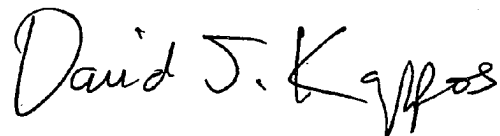
Page 1 of 1

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

Title Page, Item (75) should read:  
Inventors: Michael Burtscher, Longmont, CO (US)  
Tony Nichols, Erie, CO (US)

Signed and Sealed this

Thirteenth Day of July, 2010

A handwritten signature in black ink that reads "David J. Kappos". The signature is written in a cursive, flowing style.

David J. Kappos  
*Director of the United States Patent and Trademark Office*

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

**REQUEST FOR WITHDRAWAL  
AS ATTORNEY OR AGENT  
AND CHANGE OF  
CORRESPONDENCE ADDRESS**

|                        |                |
|------------------------|----------------|
| Application Number     | SEE SCHEDULE A |
| Filing Date            | SEE SCHEDULE A |
| First Named Inventor   | SEE SCHEDULE A |
| Art Unit               | SEE SCHEDULE A |
| Examiner Name          | SEE SCHEDULE A |
| Attorney Docket Number | SEE SCHEDULE A |

**To: Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450**

Please withdraw me as attorney or agent for the above identified patent application, and

- all the practitioners of record;
- the practitioners (with registration numbers) of record listed on the attached paper(s); or
- the practitioners of record associated with Customer Numbers: 58249 and 22903

**NOTE:** The immediately preceding box should only be marked when the practitioners were appointed using the listed Customer Number.

The reason(s) for this request are those described in 37 CFR :

- 10.40(b)(1)       10.40(b)(2)       10.40(b)(3)       10.40(b)(4)
- 10.40(c)(1)(i)       10.40(c)(1)(ii)       10.40(c)(1)(iii)       10.40(c)(1)(iv)
- 10.40(c)(1)(v)       10.40(c)(1)(vi)       10.40(c)(2)       10.40(c)(3)
- 10.40(c)(4)       10.40(c)(5)       10.40(c)(6). Please explain below:

**Certifications**

**Check each box below that is factually correct. WARNING: If a box is left unchecked, the request will likely not be approved.**

1.  I/We have given reasonable notice to the client, prior to the expiration of the response period, that the practitioner(s) intend to withdraw from employment.
2.  I/We have delivered to the client or a duly authorized representative of the client all papers and property (including funds) to which the client is entitled.
3.  I/We have notified the client of any responses that may be due and the time frame within which the client must respond.

Please provide an explanation, if necessary:

SEE ATTACHED LETTER FROM WEBROOT, INC. REQUESTING TRANSFER OF FILES.

[Page 1 of 2]

This collection of information is required by 37 CFR 1.36. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

## REQUEST FOR WITHDRAWAL AS ATTORNEY OR AGENT AND CHANGE OF CORRESPONDENCE ADDRESS

Complete the following section only when the correspondence address will change. Changes of address will only be accepted to an inventor or an assignee that has properly made itself of record pursuant to 37 CFR 3.71.

Change the correspondence address and direct all future correspondence to:

A.  The address of the inventor or assignee associated with Customer Number:

**OR**

B.  Inventor or Assignee name      Webroot, Inc. c/o Sheridan Ross

Address

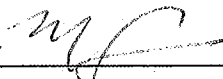
1560 Broadway, Suite 1200

|                |             |                |               |
|----------------|-------------|----------------|---------------|
| City    Denver | State    CO | Zip      80202 | Country    US |
|----------------|-------------|----------------|---------------|

|                           |                                     |
|---------------------------|-------------------------------------|
| Telephone    303-863-9700 | Email    rbrunelli@sheridanross.com |
|---------------------------|-------------------------------------|

I am authorized to sign on behalf of myself and all withdrawing practitioners.

Signature



|                           |                         |
|---------------------------|-------------------------|
| Name      Mark R. Schafer | Registration No. 65,336 |
|---------------------------|-------------------------|

Address    777 6<sup>th</sup> Street NW, Ste. 1100

|                    |             |                |               |
|--------------------|-------------|----------------|---------------|
| City    Washington | State    DC | Zip      20001 | Country    UA |
|--------------------|-------------|----------------|---------------|

|                      |                            |
|----------------------|----------------------------|
| Date      2012-09-20 | Telephone No. 720 566-4044 |
|----------------------|----------------------------|

**NOTE: Withdrawal is effective when approved rather than when received.**

[Page 2 of 2]

This collection of information is required by 37 CFR 1.36. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: **Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

*If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.*



**SCHEDULE A**

| Application No. | Application Date | Inventor  | Group Art Unit | Examiner                  | Cooley Docket No.         | Conf. No. |
|-----------------|------------------|-----------|----------------|---------------------------|---------------------------|-----------|
| 11/031,615      | Jan-07-2005      | THOMAS    | 2163           | LE, Uyen                  | WEBR-001/01US 303666-2010 | 3544      |
| 10/956,573      | Oct-01-2004      | THOMAS    | 2162           | Alam, Shahid              | WEBR-003/00US 303666-2004 | 7086      |
| 10/956,274      | Oct-01-2004      | BERTMAN   | 2135           | Truong, Thanhnga B.       | WEBR-004/00US 303666-2008 | 6861      |
| 10/956,574      | Oct-01-2004      | THOMAS    | 2162           | BULLOCK, Joshua           | WEBR-005/00US 303666-2007 | 7085      |
| 11/104,201      | Apr-12-2005      | BURTSCHER | 2167           | KIM, Chong                | WEBR-010/00US 303666-2014 | 1307      |
| 11/104,202      | Apr-12-2005      | BURTSCHER | 2436           | CERVETTI, David G.        | WEBR-011/00US 303666-2011 | 1284      |
| 11/462,827      | Aug-07-2006      | SCHNEIDER | 2438           | LANE, Gregory A.          | WEBR-023/00US 303666-2024 | 5954      |
| 13/460,655      | Apr-30-2012      | SCHNEIDER | 2431           |                           | WEBR-023/01US 303666-2124 | 9502      |
| 11/145,592      | Jun-06-2005      | NICHOLS   | 2167           | UDDIN, Mohammed           | WEBR-024/00US 303666-2027 | 4495      |
| 11/258,536      | Oct-25-2005      | MOOD      | 2432           | PERUNGAVOOR, Venkatanaray | WEBR-026/00US 303666-2028 | 2648      |
| 11/334,318      | Jan-18-2006      | HORNE     | 4144           | WATSON, Joshua C.         | WEBR-033/00US 303666-2038 | 6611      |
| 11/334,307      | Jan-18-2006      | HORNE     | 2431           | ZIA, Syed                 | WEBR-034/00US 303666-2039 | 6605      |
| 11/334,317      | Jan-18-2006      | HORNE     | 2431           | Avery, Jeremiah L.        | WEBR-035/00US 303666-2040 | 6608      |
| 11/460,032      | Jul-26-2006      | BURTSCHER | 2439           | OLION, Brian L.           | WEBR-037/00US 303666-2042 | 1341      |
| 11/386,595      | Mar-22-2006      | NICHOLS   | 2439           | LE, Canh                  | WEBR-038/00US 303666-2046 | 4954      |
| 11/386,590      | Mar-22-2006      | NICHOLS   | 2195           | WAI, Eric Charles         | WEBR-039/00US 303666-2045 | 4944      |
| 11/386,594      | Mar-22-2006      | NICHOLS   | 2189           | Peikari, Behzad           | WEBR-040/00US 303666-2044 | 4951      |
| 11/408,146      | Apr-20-2006      | BONEY     | 2438           | RAHMAN, Mahfuzur          | WEBR-044/00US 303666-2049 | 8009      |
| 13/490,294      | Jun-06-2012      | BONEY     | 2431           |                           | WEBR-044/01US 303666-2126 | 1064      |
| 11/408,145      | Apr-20-2006      | BONEY     | 2438           | RAHMAN, Mahfuzur          | WEBR-045/00US 303666-2050 | 8007      |
| 13/460,648      | Apr-30-2012      | BONEY     | 2431           |                           | WEBR-045/01US 303666-2125 | 8780      |
| 11/482,903      | Jul-07-2006      | SPROWLS   | 2438           | Truong, Thanhnga B.       | WEBR-057/00US 303666-2069 | 6773      |
| 13/184,925      | Jul-18-2011      | SPROWLS   | 2438           | Truong, Thanhnga B.       | WEBR-057/01US 303666-2121 | 1361      |
| 13/184,931      | Jul-18-2011      | SPROWLS   | 2438           | Truong, Thanhnga B.       | WEBR-057/02US 303666-2122 | 1371      |
| 11/465,680      | Aug-18-2006      | WANG      | 2115           | Connolly, Mark A.         | WEBR-059/00US 303666-2065 | 1654      |
| 12/829,749      | Jul-02-2010      | WANG      | 2115           | Connolly, Mark A.         | WEBR-059/01US 303666-2119 | 9140      |
| 12/830,021      | Jul-02-2010      | WANG      | 2115           | Connolly, Mark A.         | WEBR-059/02US 303666-2120 | 9668      |
| 13/413,391      | Mar-06-2012      | WANG      | 2115           |                           | WEBR-059/03US 303666-2123 | 7167      |
| 11/462,943      | Aug-07-2006      | BURTSCHER | 2438           | LANE, Gregory A.          | WEBR-060/00US 303666-2067 | 6147      |
| 11/462,956      | Aug-07-2006      | BURTSCHER | 2197           | DAS, Chameli              | WEBR-061/00US 303666-2070 | 6168      |
| 11/462,781      | Aug-07-2006      | MCCLOY    | 2442           |                           | WEBR-063/00US 303666-2066 | 5887      |
| 12/236,419      | Sep-23-2008      | ADAMS     | 2491           | SHAW, Brian F             | WEBR-072/00US 303666-2108 | 7849      |

webroot

Webroot

385 Interlocken Crescent Boulevard  
Suite 800  
Broomfield, CO 80021  
Toll-Free: 800.870.8102  
www.webroot.com

---

July 17, 2012

**BY EMAIL**

Wayne O. Stacy, Esq.  
Cooley LLP  
380 Interlocken Crescent  
Suite 900  
Broomfield, CO 80021

**RE: Engagement of Sheridan Ross P.C.**

Dear Wayne:

As you and I discussed recently, Webroot Inc. has elected to consolidate its intellectual property prosecution work with Sheridan Ross P.C. Accordingly, I write to request that you arrange for the items listed below to be forwarded Sheridan Ross as soon as possible:

- Lists of all patent, trademark, and copyright matters your firm has handled – and is currently handling – for Webroot;
- A docket report for each patent, trademark, and copyright matter detailing upcoming deadlines through December 31, 2012;
- Physical files for each patent, trademark, and copyright matter;
- Electronic files for each patent, trademark, and copyright matter, if available; and
- A master list of all items forwarded to Sheridan Ross.

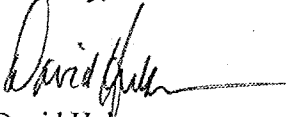
All items should be sent to the attention of Robert Brunelli, 1560 Broadway, Suite 1200, Denver, Colorado 80202; [rbrunelli@sheridanross.com](mailto:rbrunelli@sheridanross.com).

Webroot anticipates that the fees/costs associated with providing the foregoing materials to Sheridan Ross will be minimal, and in no event will exceed \$500 per docket. If you expect fees/costs greater than that amount, please contact me immediately.

Please note that you need not notify foreign associates of Webroot's engagement of Sheridan Ross. Sheridan Ross will handle those notifications.

Thank you for your attention to this matter.

Sincerely,



David Huberman  
General Counsel  
Webroot Inc.

## Electronic Acknowledgement Receipt

|   |  |
|---|--|
| <b>EFS ID:</b>                              | 13799549   |
| <b>Application Number:</b>                  | 11104202   |
| <b>International Application Number:</b>    |  |
| <b>Confirmation Number:</b>                 | 1284   |
| <b>Title of Invention:</b>                  | SYSTEM AND METHOD FOR DIRECTLY ACCESSING DATA FROM A DATA STORAGE MEDIUM |
| <b>First Named Inventor/Applicant Name:</b> | Michael Burtscher  |
| <b>Customer Number:</b>                     | 22903  |
| <b>Filer:</b>                               | Mark Randolph Schafer  |
| <b>Filer Authorized By:</b>                 |  |
| <b>Attorney Docket Number:</b>              | WEBR-011/00US 303666-2011  |
| <b>Receipt Date:</b>                        | 20-SEP-2012  |
| <b>Filing Date:</b>                         | 12-APR-2005  |
| <b>Time Stamp:</b>                          | 17:20:19   |
| <b>Application Type:</b>                    | Utility under 35 USC 111(a)  |

### Payment information:

|                        |    |
|------------------------|----|
| Submitted with Payment | no |
|------------------------|----|

### File Listing:

| Document Number | Document Description | File Name             | File Size(Bytes)/<br>Message Digest                               | Multi Part /.zip | Pages (if appl.) |
|-----------------|----------------------|-----------------------|---|------------------|------------------|
| 1               | Change of Address    | WEBR-Req2Withdraw.pdf | 282148<br><small>8bb7d27bcb066b34eeeca860249160c928194588</small> | no               | 4                |

### Warnings:

### Information:

**This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.**

**New Applications Under 35 U.S.C. 111**

**If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.**

**National Stage of an International Application under 35 U.S.C. 371**

**If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.**

**New International Application Filed with the USPTO as a Receiving Office**

**If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.**

## POWER OF ATTORNEY TO PROSECUTE APPLICATIONS BEFORE THE USPTO

I hereby revoke all previous powers of attorney given in the application identified in the attached statement under 37 CFR 3.73(c).

I hereby appoint:



Practitioners associated with Customer Number:

22442

**OR**



Practitioner(s) named below (if more than ten patent practitioners are to be named, then a customer number must be used):

| Name | Registration Number |
|------|---------------------|
|      |                     |
|      |                     |
|      |                     |
|      |                     |
|      |                     |

| Name | Registration Number |
|------|---------------------|
|      |                     |
|      |                     |
|      |                     |
|      |                     |
|      |                     |

As attorney(s) or agent(s) to represent the undersigned before the United States Patent and Trademark Office (USPTO) in connection with any and all patent applications assigned only to the undersigned according to the USPTO assignment records or assignments documents attached to this form in accordance with 37 CFR 3.73(c).

Please change the correspondence address for the application identified in the attached statement under 37 CFR 3.73(c) to:



The address associated with Customer Number:

22442

**OR**

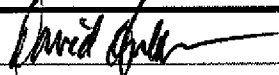
|                          |                         |       |     |  |
|--------------------------|-------------------------|-------|-----|--|
| <input type="checkbox"/> | Firm or Individual Name |       |     |  |
| <input type="checkbox"/> | Address                 |       |     |  |
| <input type="checkbox"/> | City                    | State | Zip |  |
| <input type="checkbox"/> | Country                 |       |     |  |
| <input type="checkbox"/> | Telephone               | Email |     |  |

Assignee Name and Address: **WEBROOT INC.**  
385 Interlocken Crescent, Ste. 800  
Broomfield, Colorado 80021

**A copy of this form, together with a statement under 37 CFR 3.73(c) (Form PTO/AIA/96 or equivalent) is required to be filed in each application in which this form is used. The statement under 37 CFR 3.73(c) may be completed by one of the practitioners appointed in this form, and must identify the application in which this Power of Attorney is to be filed.**

### SIGNATURE of Assignee of Record

The individual whose signature and title is supplied below is authorized to act on behalf of the assignee

|           |   |           |              |
|-----------|---|-----------|--------------|
| Signature |  | Date      | 1 OCT 2012   |
| Name      | David Huberman, Esq.  | Telephone | 720-842-3627 |
| Title     | General Counsel   |           |              |

This collection of information is required by 37 CFR 1.31, 1.32 and 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

## Electronic Acknowledgement Receipt

|   |  |
|---|--|
| <b>EFS ID:</b>                              | 13896150   |
| <b>Application Number:</b>                  | 11104202   |
| <b>International Application Number:</b>    |  |
| <b>Confirmation Number:</b>                 | 1284   |
| <b>Title of Invention:</b>                  | SYSTEM AND METHOD FOR DIRECTLY ACCESSING DATA FROM A DATA STORAGE MEDIUM |
| <b>First Named Inventor/Applicant Name:</b> | Michael Burtscher  |
| <b>Customer Number:</b>                     | 22903  |
| <b>Filer:</b>                               | Bradley M. Knepper/Erica Picard  |
| <b>Filer Authorized By:</b>                 | Bradley M. Knepper   |
| <b>Attorney Docket Number:</b>              | WEBR-011/00US 303666-2011  |
| <b>Receipt Date:</b>                        | 02-OCT-2012  |
| <b>Filing Date:</b>                         | 12-APR-2005  |
| <b>Time Stamp:</b>                          | 18:50:02   |
| <b>Application Type:</b>                    | Utility under 35 USC 111(a)  |

### Payment information:

|                        |    |
|------------------------|----|
| Submitted with Payment | no |
|------------------------|----|

### File Listing:

| Document Number | Document Description                           | File Name     | File Size(Bytes)/<br>Message Digest               | Multi Part /.zip | Pages (if appl.) |
|-----------------|--|---------------|---|------------------|------------------|
| 1               | Assignee showing of ownership per 37 CFR 3.73. | STATEMENT.pdf | 120998<br>d4d0b4c386829eeffe57b7f3a74ddad7bf71bac | no               | 3                |

### Warnings:

### Information:

|   |                   |         |  |    |   |
|---|-------------------|---------|--|----|---|
| 2 | Power of Attorney | POA.pdf | 59485<br>68e3501600681c461a6a1ad6257bc47dc71e26d | no | 1 |
|---|-------------------|---------|--|----|---|

**Warnings:**

**Information:**

|                                     |        |
|-------------------------------------|--------|
| <b>Total Files Size (in bytes):</b> | 180483 |
|-------------------------------------|--------|

**This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.**

**New Applications Under 35 U.S.C. 111**

**If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.**

**National Stage of an International Application under 35 U.S.C. 371**

**If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.**

**New International Application Filed with the USPTO as a Receiving Office**

**If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.**

**STATEMENT UNDER 37 CFR 3.73(c)**

Applicant/Patent Owner: Webroot Inc.

Application No./Patent No.: 7,565,695 Filed/Issue Date: 2009-07-21

Titled: SYSTEM AND METHOD FOR DIRECTLY ACCESSING DATA FROM A DATA STORAGE MEDIUM

Webroot Inc., a Corporation

(Name of Assignee) (Type of Assignee, e.g., corporation, partnership, university, government agency, etc.)

states that, for the patent application/patent identified above, it is (choose **one** of options 1, 2, 3 or 4 below):

- 1.  The assignee of the entire right, title, and interest.
- 2.  An assignee of less than the entire right, title, and interest (check applicable box):
  - The extent (by percentage) of its ownership interest is \_\_\_\_\_%. Additional Statement(s) by the owners holding the balance of the interest must be submitted to account for 100% of the ownership interest.
  - There are unspecified percentages of ownership. The other parties, including inventors, who together own the entire right, title and interest are:

Additional Statement(s) by the owner(s) holding the balance of the interest must be submitted to account for the entire right, title, and interest.

- 3.  The assignee of an undivided interest in the entirety (a complete assignment from one of the joint inventors was made). The other parties, including inventors, who together own the entire right, title, and interest are:

Additional Statement(s) by the owner(s) holding the balance of the interest must be submitted to account for the entire right, title, and interest.

- 4.  The recipient, via a court proceeding or the like (e.g., bankruptcy, probate), of an undivided interest in the entirety (a complete transfer of ownership interest was made). The certified document(s) showing the transfer is attached.

The interest identified in option 1, 2 or 3 above (not option 4) is evidenced by either (choose **one** of options A or B below):

- A.  An assignment from the inventor(s) of the patent application/patent identified above. The assignment was recorded in the United States Patent and Trademark Office at Reel \_\_\_\_\_, Frame \_\_\_\_\_, or for which a copy thereof is attached.
- B.  A chain of title from the inventor(s), of the patent application/patent identified above, to the current assignee as follows:

1. From: Michael Burtscher To: Webroot Software, Inc.

The document was recorded in the United States Patent and Trademark Office at Reel 016471, Frame 0484, or for which a copy thereof is attached.

2. From: Tony Nichols To: Webroot Software, Inc.

The document was recorded in the United States Patent and Trademark Office at Reel 022808, Frame 0389, or for which a copy thereof is attached.



Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

**STATEMENT UNDER 37 CFR 3.73(c)**

3. From: Webroot Software, Inc. To: Webroot Inc.

The document was recorded in the United States Patent and Trademark Office at  
Reel 028953, Frame 0917, or for which a copy thereof is attached.

4. From: \_\_\_\_\_ To: \_\_\_\_\_

The document was recorded in the United States Patent and Trademark Office at  
Reel \_\_\_\_\_, Frame \_\_\_\_\_, or for which a copy thereof is attached.

5. From: \_\_\_\_\_ To: \_\_\_\_\_

The document was recorded in the United States Patent and Trademark Office at  
Reel \_\_\_\_\_, Frame \_\_\_\_\_, or for which a copy thereof is attached.

6. From: \_\_\_\_\_ To: \_\_\_\_\_

The document was recorded in the United States Patent and Trademark Office at  
Reel \_\_\_\_\_, Frame \_\_\_\_\_, or for which a copy thereof is attached.

Additional documents in the chain of title are listed on a supplemental sheet(s).

As required by 37 CFR 3.73(c)(1)(i), the documentary evidence of the chain of title from the original owner to the assignee was, or concurrently is being, submitted for recordation pursuant to 37 CFR 3.11.

[NOTE: A separate copy (i.e., a true copy of the original assignment document(s)) must be submitted to Assignment Division in accordance with 37 CFR Part 3, to record the assignment in the records of the USPTO. See MPEP 302.08]

The undersigned (whose title is supplied below) is authorized to act on behalf of the assignee.

/Bradley M. Knepper/

Signature

Bradley M. Knepper

Printed or Typed Name

2012-10-02

Date

44,189

Title or Registration Number

## Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

| APPLICATION NUMBER | FILING OR 371(C) DATE | FIRST NAMED APPLICANT | ATTY. DOCKET NO./TITLE       |
|--------------------|-----------------------|-----------------------|------------------------------|
| 11/104,202         | 04/12/2005            | Michael Burtscher     | WEBR-011/00US<br>303666-2011 |

**CONFIRMATION NO. 1284**

**POA ACCEPTANCE LETTER**



22442  
Sheridan Ross PC  
1560 Broadway  
Suite 1200  
Denver, CO 80202

Date Mailed: 10/12/2012

**NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY**

This is in response to the Power of Attorney filed 10/11/2012.

The Power of Attorney in this application is accepted. Correspondence in this application will be mailed to the above address as provided by 37 CFR 1.33.

/dolipscomb/

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

| APPLICATION NUMBER | FILING OR 371(C) DATE | FIRST NAMED APPLICANT | ATTY. DOCKET NO./TITLE       |
|--------------------|-----------------------|-----------------------|------------------------------|
| 11/104,202         | 04/12/2005            | Michael Burtscher     | WEBR-011/00US<br>303666-2011 |

**CONFIRMATION NO. 1284**

**POWER OF ATTORNEY NOTICE**



22903  
COOLEY LLP  
ATTN: PATENT GROUP  
Suite 1100  
777 - 6th Street, NW  
WASHINGTON, DC 20001

Date Mailed: 10/12/2012

**NOTICE REGARDING CHANGE OF POWER OF ATTORNEY**

This is in response to the Power of Attorney filed 10/11/2012.

- The Power of Attorney to you in this application has been revoked by the assignee who has intervened as provided by 37 CFR 3.71. Future correspondence will be mailed to the new address of record(37 CFR 1.33).

/dolipscomb/

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

**Power of Attorney to Transact Business with the  
United States Patent and Trademark Office**

I hereby revoke all previous Powers of Attorney given in the application(s) identified in the attached Transmittal for Power of Attorney to One or More Registered Practitioners ("Transmittal Form").

I hereby appoint practitioners associated with the following Customer Number associated with Sprinkle IP Law Group, PC :

109422

as my/our attorney(s) or agent(s) and to transact all business before the United States Patent and Trademark Office (USPTO) in connection with any and all patents and patent applications that are assigned to **Webroot Inc.** (the "assignee's patents/patent applications") in which they shall appear, any and all assignee's patents/patent applications associated with the above-referenced customer number, and any and all patents and patent applications referenced in the attached Transmittal Form.


Please recognize or change the correspondence address for the patents and patent applications referenced in the attached Transmittal Form to the address associated with the above-referenced customer number.

The undersigned is:

- Inventor or Joint Inventor
- Assignee or Person to Whom the Inventor is Under an Obligation to Assign  
\*the undersigned has authority to act on behalf of the Assignee or Person to Whom the Inventor is Under an Obligation to Assign.
- Legal Representative of a Deceased or Legally Incapacitated Inventor
- Person Who Otherwise Shows Sufficient Proprietary Interest (e.g., a petition under 37 CFR 1.46(b)(2) was granted in the application or is currently being filed in this document)

The Transmittal Form may be completed and executed by one of the practitioners associated with the above-referenced customer number.

**SIGNATURE OF APPLICANT**

|   |                               |
|---|-------------------------------|
| <b>Signature:</b>  | <b>Date:</b> January 29, 2020 |
| <b>Name:</b> Gordon A. Davies   |                               |
| <b>Title:</b> Director  |                               |
| <b>Company:</b> Webroot Inc.  |                               |

I am authorized to act on behalf of the assignee.

## Electronic Acknowledgement Receipt

|   |  |
|---|--|
| <b>EFS ID:</b>                              | 39149949   |
| <b>Application Number:</b>                  | 11104202   |
| <b>International Application Number:</b>    |  |
| <b>Confirmation Number:</b>                 | 1284   |
| <b>Title of Invention:</b>                  | SYSTEM AND METHOD FOR DIRECTLY ACCESSING DATA FROM A DATA STORAGE MEDIUM |
| <b>First Named Inventor/Applicant Name:</b> | Michael Burtscher  |
| <b>Customer Number:</b>                     | 22442  |
| <b>Filer:</b>                               | John L. Adair/keunah cheun   |
| <b>Filer Authorized By:</b>                 | John L. Adair  |
| <b>Attorney Docket Number:</b>              | 6890-33  |
| <b>Receipt Date:</b>                        | 14-APR-2020  |
| <b>Filing Date:</b>                         | 12-APR-2005  |
| <b>Time Stamp:</b>                          | 10:54:09   |
| <b>Application Type:</b>                    | Utility under 35 USC 111(a)  |

### Payment information:

|                        |    |
|------------------------|----|
| Submitted with Payment | no |
|------------------------|----|

### File Listing:

| Document Number | Document Description | File Name              | File Size(Bytes)/<br>Message Digest              | Multi Part /.zip | Pages (if appl.) |
|-----------------|----------------------|------------------------|--|------------------|------------------|
| 1               | Power of Attorney    | WEBROOT_POA_012820.pdf | 42303<br>460c019d47e52952aad549f0d335131a49b6cfe | no               | 1                |

### Warnings:

**Information:****Total Files Size (in bytes):**

42303

**This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.**

**New Applications Under 35 U.S.C. 111**

**If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.**

**National Stage of an International Application under 35 U.S.C. 371**

**If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.**

**New International Application Filed with the USPTO as a Receiving Office**

**If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.**



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

| APPLICATION NUMBER | FILING OR 371(C) DATE | FIRST NAMED APPLICANT | ATTY. DOCKET NO./TITLE |
|--------------------|-----------------------|-----------------------|------------------------|
| 11/104,202         | 04/12/2005            | Michael Burtscher     | 6890-33                |

**CONFIRMATION NO. 1284  
IMPROPER CPOA LETTER**

22442  
Sheridan Ross PC  
1560 Broadway  
Suite 1200  
Denver, CO 80202



Date Mailed: 05/12/2020

**NOTICE REGARDING POWER OF ATTORNEY**

This is in response to the power of attorney filed 04/14/2020. The power of attorney in this application is not accepted for the reason(s) listed below:

- The power of attorney is from an assignee and the statement required by 37 CFR 3.73(c) has not been received.

/trwoodson/

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

|   |
|---|
| 109422<br>Sprinkle IP Law Group/OPEN<br>1301 W. 25th Street, Suite 408<br>Austin, TX 78705<br>UNITED STATES |
|---|