

Webroot Spy Sweeper Enterprise Anti-Spyware Effectiveness Testing

Executive summary

Webroot, Inc. commissioned VeriTest, a division of Lionbridge Technologies, Inc., to conduct a test comparing the following Enterprise class anti-spyware applications:

- Webroot Spy Sweeper Enterprise 2.5.1
- Symantec AntiVirus Corporate 10.1.0.394
- Trend Micro Anti-Spyware Enterprise 3.0.0.76

The testing was designed to focus on effectiveness of completely cleaning spyware of user desktops .

For the purposes of this test, spyware was intended to include all varieties, including system monitors, adware and Trojans.

Spyware is software with a wide variety of purposes that varies as designed by spyware creators. This software is often installed on a personal computer without knowledge of the PC user. Spyware, unbeknownst to the PC user may monitor activities on the PC and glean personal information for unscrupulous third parties. Spyware may also present undesired advertising to the PC user, or even provide a means for additional undesired software to be installed.

VeriTest began with a CD-ROM containing 150 individual pieces of spyware comprising system monitors, adware and Trojans to be used in this test¹. Each Enterprise anti-spyware application was installed to its own server, each of which had three client PC's dedicated as agents. All computers in this test were provided Internet access via a proxy server.

A Snapshot was taken which included the File and Operating System configurations on each PC prior to installing spyware. After the Snapshot was taken, five individual spyware applications were installed to each client PC. The PC was then rebooted. Upon reboot, Internet Explorer was opened and a known web page was visited. The Enterprise Agent was then instructed to perform an exhaustive scan with subsequent reboots and rescans if required. When the Enterprise Agent software indicated that there were no further traces of spyware, or the Enterprise Agent demonstrated no progress in removing identified spyware, an analysis of changed file and Operating System configurations was performed.

Analysis of a PC after the cleaning process requires an intimate knowledge of Registry and File System components. A spyware application will often use shared applications or components that are common amongst desired software that a spyware application may also take advantage of. In analyzing the log

¹ The spyware programs utilized for this test were randomly chosen from a database of over 8000 spyware installation programs that was provided by Webroot. These spies consisted of a random mix of adware, system monitors and Trojans. 184 spies were randomly chosen from the database, 150 of which were used in the test.

Key findings

- ❑ Webroot Spy Sweeper Enterprise identified and removed more spyware than competitors.
- ❑ Webroot Spy Sweeper Enterprise removed 91% of adware tested.
- ❑ Webroot Spy Sweeper Enterprise identified and removed 97% of Trojan Horses tested.
- ❑ Webroot Spy Sweeper Enterprise identified and removed 88% of system monitors tested.

files produced during this test, VeriTest Engineers took special care in utilizing their experience to identify Registry and File System modifications that are not unique to the spyware application. These shared and benign components were not counted as spyware traces left behind by the anti-spyware software.

In testing 150 individual spyware applications, Webroot Spy Sweeper Enterprise performed exceptionally well in identification and thorough removal of spyware traces. Though all tested anti-spyware applications were noted to identify spies, Webroot Spy Sweeper Enterprise proved superior to the competitors in effectively identifying and fully removing spyware.

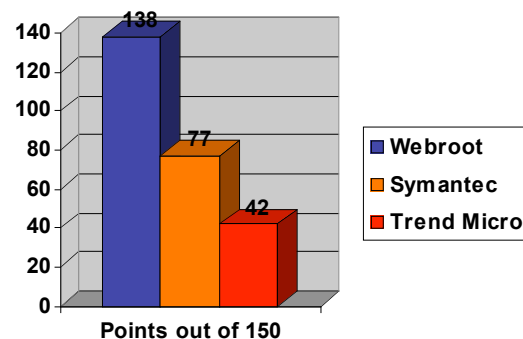
Webroot Spy Sweeper Enterprise took a most important step beyond removing the spyware infection by also removing the file that installed the spyware. Individuals responsible for Enterprise security demand that anti-spyware applications not only remove all spyware infections, but also eliminate the threat of future infections by completely removing the spyware installation file from the PC.

VeriTest Enterprise Anti-Spyware Test Scoring:

Scores were determined by subtracting points from a total of 150 possible, relative to the number of spyware applications tested. 1 point was subtracted for each spyware application noted to have not been effectively cleaned.

Total Score

- Webroot SpySweeper Enterprise: 138
- Symantec AntiVirus Corporate: 77
- Trend Micro Anti-Spyware Enterprise: 42



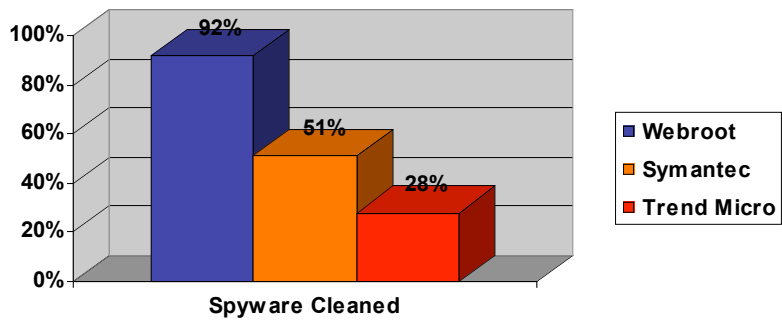
Webroot Spy Sweeper Enterprise proved to provide the most effective product for the identification and removal of spyware applications in this test.

Test Findings

Spyware Identification and Removal Effectiveness Testing

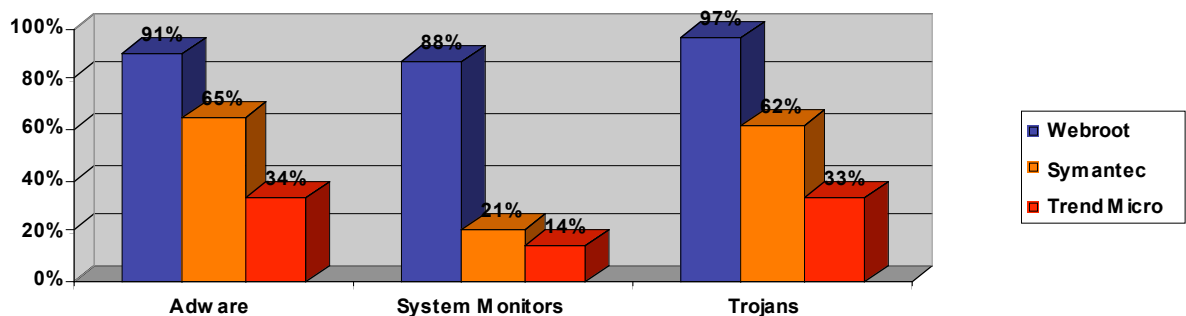
Results

Of the 150 spyware applications tested, Webroot Spy Sweeper Enterprise effectively cleaned 138 Spyware applications. Symantec AntiVirus Corporate cleaned 56 and Trend Micro Anti-Spyware Enterprise cleaned 42. The accurate identification of spyware applications is critical to the security of the PC in the Enterprise. As demonstrated in the graph below, Webroot Spy Sweeper Enterprise demonstrated the greatest ability to identify and remove Spyware.



Spyware Identified and Cleaned by Category

The graph below demonstrates identification and cleaning ability based on spyware category. For the purposes of this test, spyware was grouped into adware, system monitors and Trojans. There was a total of 68 adware, 43 system monitor and 39 Trojan applications tested.



CONCLUSION:

Testing anti-spyware applications for effectiveness is extremely complex. Most businesses conduct rudimentary tests with common spies that produce inconsistent results. VeriTest noted: "In this robust test that spanned two months and included 150 spies, with simultaneous installations of adware, system monitors and Trojan's, Webroot Spy Sweeper Enterprise significantly outperformed Symantec and Trend Micro products by accurately identifying and effectively removing more spyware applications used in this test. Effectively removing 92% of spyware in this test demonstrates excellent early detection and cleaning methodology. Administrators must take in to account the rate at which their anti-spyware solution provider identifies new threats. The aforementioned testing results are evident of a "Right tool for the job" scenario. Webroot has proven to provide the greatest protection against spyware at the time of this testing.

APPENDIX A: Testing Methodology

Each Enterprise product was installed to an individual Windows 2003 Standard Edition server. Each Enterprise product had three client PC's dedicated as Agents of that software. Each Agent PC had a Windows XP Professional Operating System. All PC's and servers were provided unrestricted Internet access via a proxy server. Enterprise applications were allowed to update their products via the Internet at will. On each client PC, an Enterprise Agent was installed along with Install Watch, Regmon, Filemon and HijackThis analysis tools. InstallWatch was used to take a snapshot of File and Operating System states prior to the installation of Spyware. Regmon and Filemon were configured to watch File system and Windows Registry modifications made by each group of five Spyware applications installed. With analysis software in place and a snapshot of the clean PC taken, five Spyware applications were installed. These applications were a random combination of Spyware, Malware, Adware and Trojans. Each client PC had the same batch of five Spyware applications installed in each group. After Spyware installation was complete, Filemon and Regmon analysis data was exported for later review. The PC was then rebooted. The Anti-Spyware software was then instructed to perform a scan for Spyware. Upon completion of the initial Spyware scan the PC was rebooted and an additional scan was performed. If the Anti-Spyware Enterprise Agent or Server reported additional Spyware traces were found, an additional reboot and subsequent scan for Spyware was performed until the Agent reported no further Spyware traces were found or no further progress was noted in the removal of an identified piece of spyware. When an Enterprise Agent reported a PC as clean, or an Enterprise Agent application failed to clean, InstallWatch was then instructed to compare the post infection operating system state with the clean snapshot. The analysis was then exported. HijackThis was then executed and its log was also exported. The InstallWatch analysis was then reviewed. Added file and registry modifications were examined to determine what if any Spyware traces were not cleaned. Filemon and Regmon logs facilitated the identification of what Spyware application made what file or registry change to the PC. The HijackThis log also facilitated ready identification of offending registry modifications such as adding URLs to Internet Explorers Trusted Zones. The new file and system modifications were compared to the Regmon and Filemon log files to conclude what Spyware Application was not thoroughly cleaned. A Spyware application was deemed clean if any Executable, Component, or Hijackthis identified running processes or Registry entries associated with the Spyware installation were not identified within logs. Upon the completion of the Agent scans and the export of InstallWatch, Regmon, Filemon and Hijackthis analysis information, the PC was then restored to a clean state by restoration of a clean hard drive image. Steps in the process used in this cycle are as follows:

1. Take a snapshot with Install Watch.
2. Drag the installers from a CD to the testing machine's desktop.
3. Run Filemon and Regmon with no filters enabled.
4. Copy dlls to the test machine's System32 directory.
5. Run the executables.
6. Visit a well-known clean webpage such as google.com or msn.com
7. After five minutes or a halt in activity in the Regmon and Filemon utilities, save the logs for said utilities.
8. Reboot the test machine.
9. Use the installed product to scan and remove any spies.
10. Repeat Steps 8 and 9 either until no spies are detected or until consecutive scans detect the same spies.
11. Run HijackThis and save the resulting log to an external resource.
12. Analyze or complete the snapshot in Install Watch.
13. Save all logs to an external resource.
 - If it is not possible to complete the Install Watch Snapshot or save the logs to an external source, and create a substitute round of installers.
14. Note on the results spreadsheet any spies that are clearly Not Clean.
15. Restore the test machine back to its setup state.

To complete the analysis, compare the Install Watch, Filemon, and Regmon logs captured during each test group. Use the following procedure for analysis:

1. Search the Filemon and Regmon logs for all exe and dll files that are in the Added Files log.
2. Search the Filemon and Regmon logs for all registry keys that are in the Added Registry log.
3. Search the Regmon log for any registry keys that shown as modified in the HijackThis log.
4. Search the Filemon log for any processes found in memory as shown by the HijackThis log.

Use the table below by which to measure the results of a product's effectiveness against a spy compared to the traces discovered using the process above; if any Dirty condition is met that spy is considered Dirty:

Dirty:	<ul style="list-style-type: none"> • The Installer was not removed from the desktop or the System32 directory. • Any executables or dlls on the test machine not removed that were written by any of the installed spies or executables or dlls written by one of the installed spies.² • A process left in memory on the test machine was written by one of the spies installed or executables or dlls written by one of the installed spies. • Any browser hijack(s) created by one of the installed spies or a file written by one of the installed spies.³
Clean:	<ul style="list-style-type: none"> • If none of the conditions of Dirty have been met the spy is considered Clean.

Example of analysis for one round of installers:

In this example the spies CSRSS SpamRelayer, Goldfer_SpamRelayer, mspm-bot, PC Activity Monitor and Spy Software were installed. Two of these pieces of spyware are commercially available Keyloggers but the other three are Trojan horses with no consistent installation source, making it difficult to test against this type of threat unless the user has a ready database of Installers for all manner and type of threats.

The product being analyzed in this instance is McAfee Enterprise AV with anti-spyware module 8.0.

Following the steps of analysis, the first log to search for executables and dlls is the Added Files Log. One of the first executables found is v8install_spy_software_4_parents.exe, see Figure 1.

² There may be cases when a spy downloads and installs known good software such as utilities, Winpcap for example is downloaded by several Keyloggers. Some spies may download and install Microsoft common controls for use in their GUIs, comctl32.dll and comdlg32.ocx may be used by a piece of Adware for example. Files such as these should not be considered part of a spy.

³ Examples of browser hijacks include;
HKEY_CURRENT_USER\Software\Microsoft\Search Assistant DefaultSearchURL
http://search.2020search.com/9894/search/redir.php?cid=shnv9894PCID=0000000000007858367&s=
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main Start Page "about:blank" http://myhomepage.capitan-trash.com/
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main Default_Page_URL "http://www.dell4me.com/mywaybiz" http://myhomepage.capitan-trash.com/

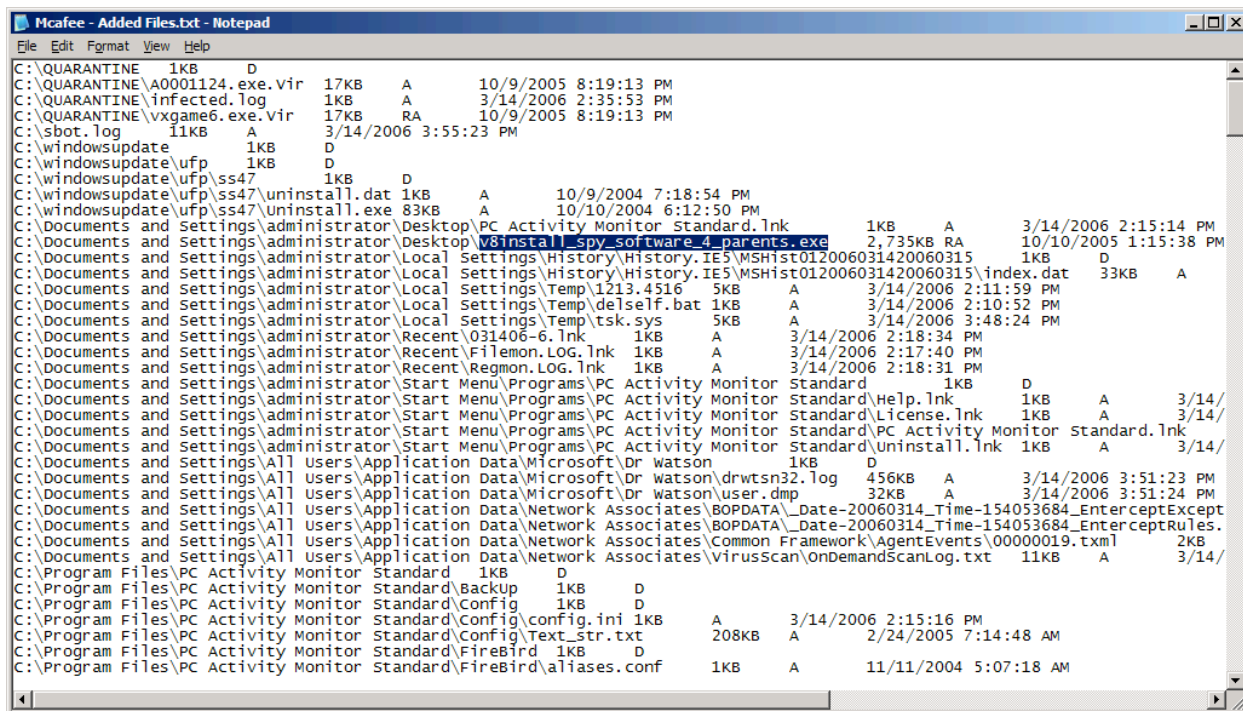


Figure 1 Installer left on machine.

After reviewing the Installer CD, this is the Spy Software installer, see Figure 2. Without knowledge of what installers are present on the box it is impossible to accurately tell if a spy was cleaned or not cleaned by the anti-spyware product.

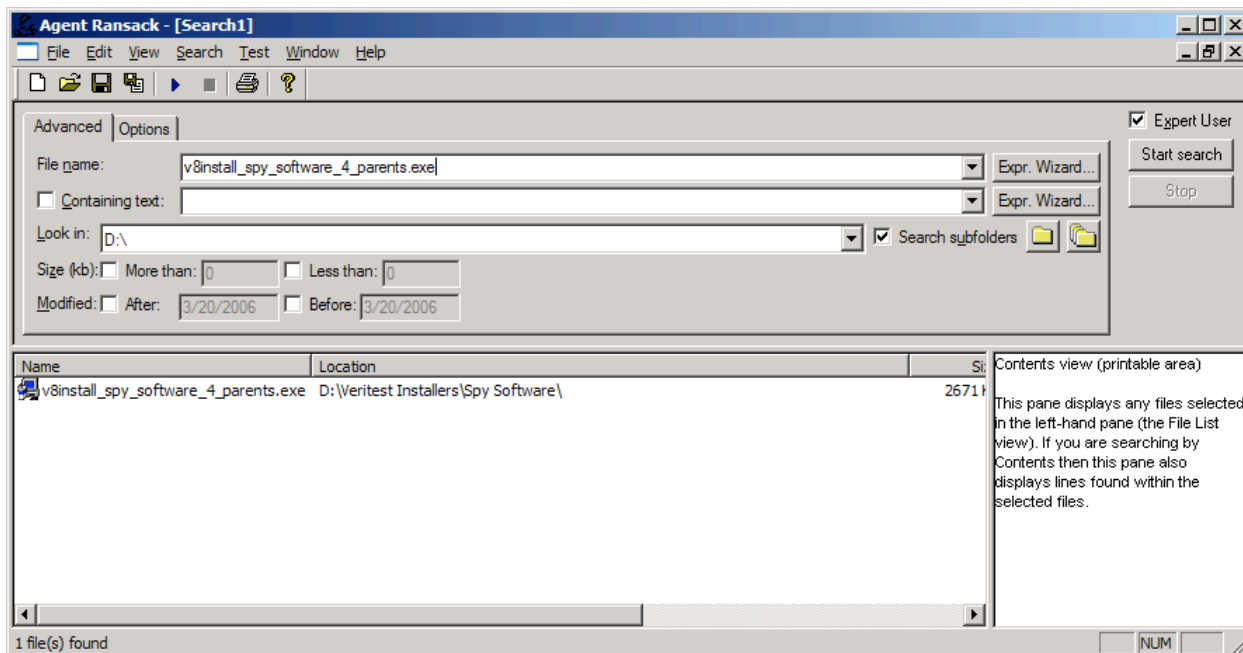


Figure 2 Installer is Spy Software

Searching farther through the Added Files Log the executable fbserver.exe is found, see Figure 3. It is then necessary to search the Filemon log to determine what created this .exe.

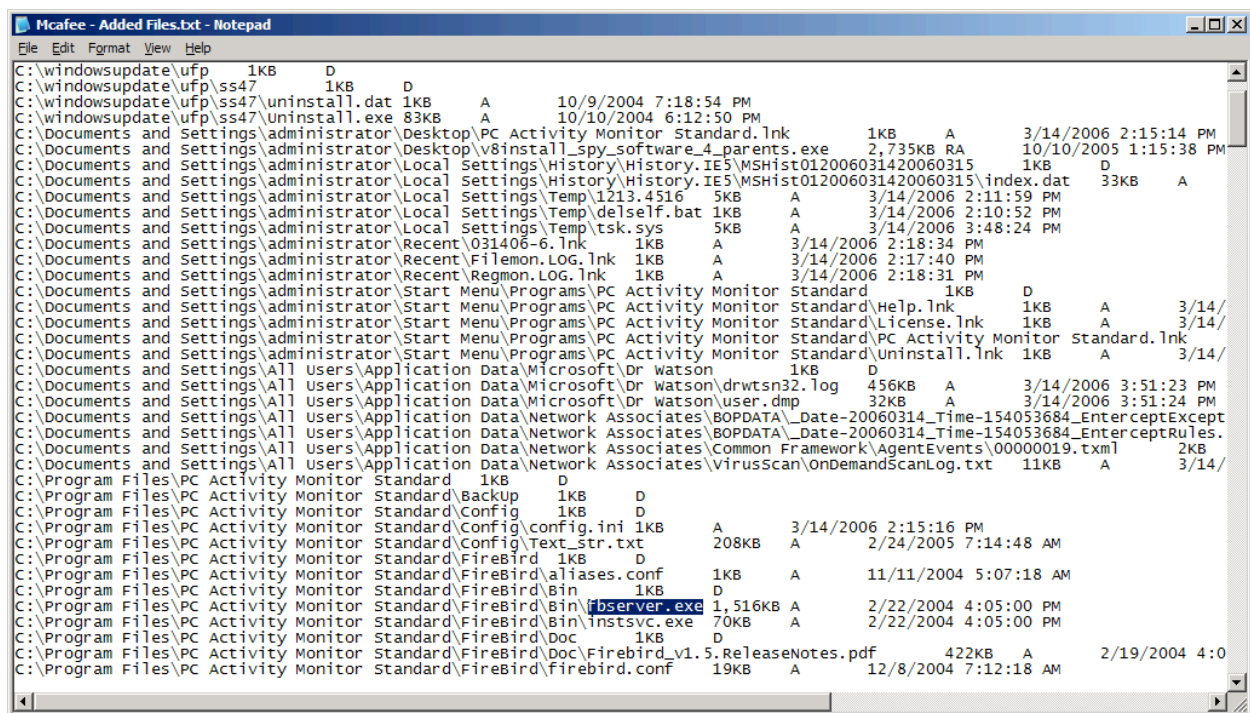


Figure 3 Executable left on disk

Searching within the Filemon log for the CREATE statement that goes along with fbserver.exe shows that the process pcstdt_setup.ex created fbserver.exe, see Figure 4.

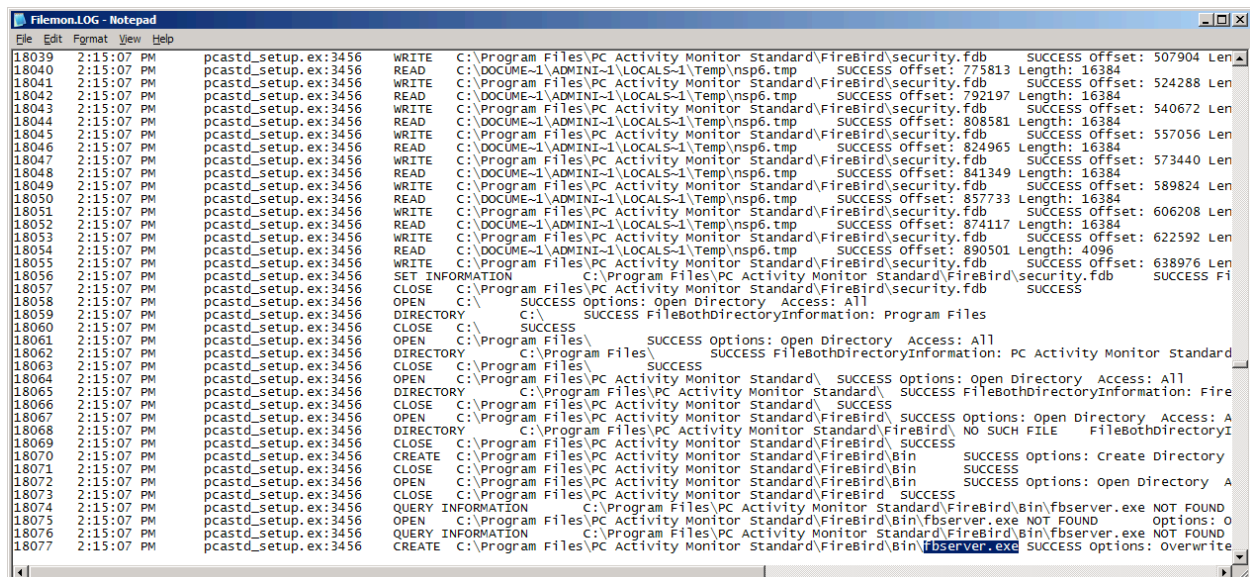


Figure 4 Filemon log

Searching the Installer CD shows that pcstdt_setup.exe is the PC Activity Monitor Installer, see Figure 5.

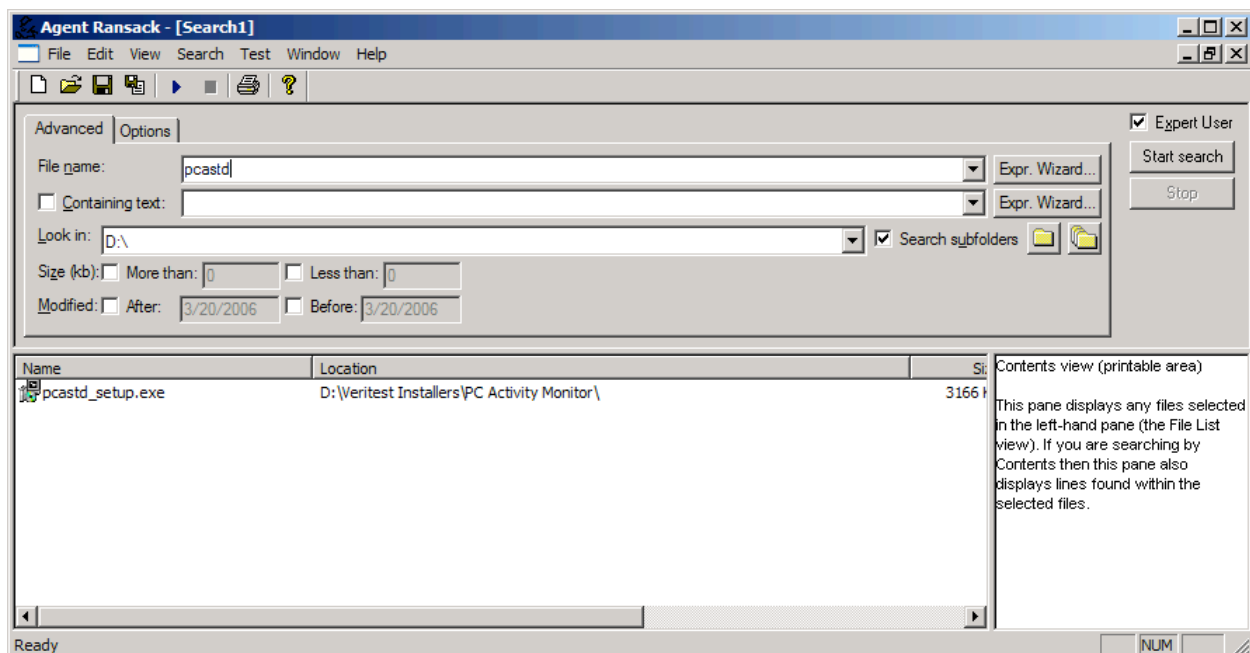


Figure 5

The next file to analyze is chp.dll, written to c:\windows\system32, see Figure 6.

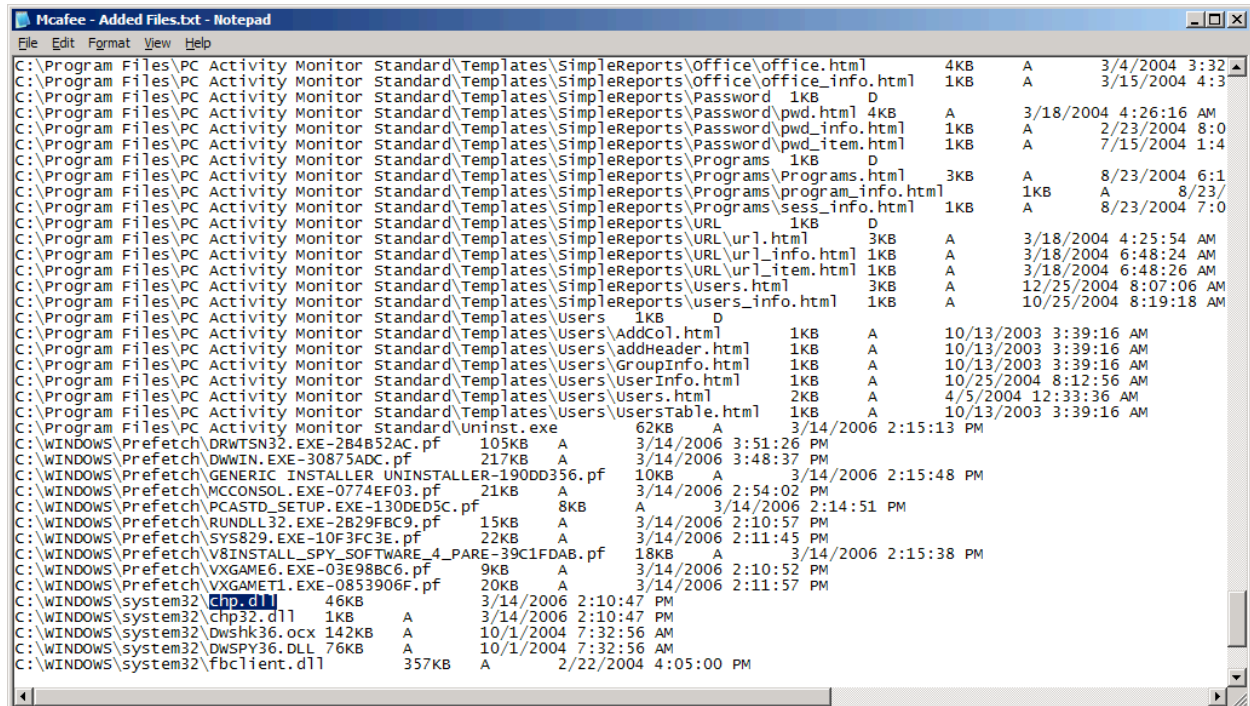
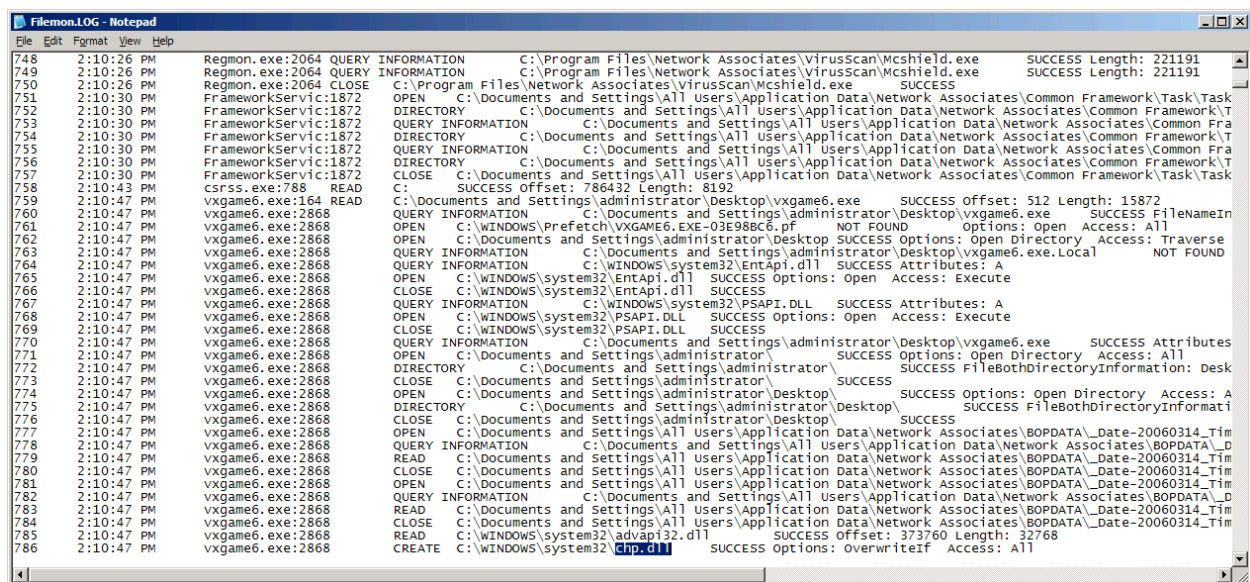


Figure 6

In the Filemon Log it is found that chp.dll was written by vxgame6.exe, see Figure 7.



```
Filemon.LOG - Notepad
File Edit Format View Help
748 2:10:26 PM Regmon.exe:2064 QUERY INFORMATION C:\Program Files\Network Associates\VirusScan\Mcshield.exe SUCCESS Length: 221191
749 2:10:26 PM Regmon.exe:2064 QUERY INFORMATION C:\Program Files\Network Associates\VirusScan\Mcshield.exe SUCCESS Length: 221191
750 2:10:26 PM Regmon.exe:2064 CLOSE C:\Program Files\Network Associates\VirusScan\Mcshield.exe SUCCESS
751 2:10:30 PM FrameworkService.exe:1872 OPEN C:\Documents and Settings\All users\Application Data\Network Associates\Common Framework\Task\Task
752 2:10:30 PM FrameworkService.exe:1872 DIRECTORY C:\Documents and Settings\All users\Application Data\Network Associates\Common Framework\Task\Task
753 2:10:30 PM FrameworkService.exe:1872 QUERY INFORMATION C:\Documents and Settings\All users\Application Data\Network Associates\Common Framework\Task\Task
754 2:10:30 PM FrameworkService.exe:1872 DIRECTORY C:\Documents and Settings\All users\Application Data\Network Associates\Common Framework\Task\Task
755 2:10:30 PM FrameworkService.exe:1872 QUERY INFORMATION C:\Documents and Settings\All users\Application Data\Network Associates\Common Framework\Task\Task
756 2:10:30 PM FrameworkService.exe:1872 DIRECTORY C:\Documents and Settings\All users\Application Data\Network Associates\Common Framework\Task\Task
757 2:10:30 PM FrameworkService.exe:1872 CLOSE C:\Documents and Settings\All users\Application Data\Network Associates\Common Framework\Task\Task
758 2:10:43 PM csrss.exe:788 READ C:\Documents and Settings\administrator\Desktop\vxgame6.exe SUCCESS Offset: 512 Length: 15872
759 2:10:47 PM vxgame6.exe:164 READ C:\Documents and Settings\administrator\Desktop\vxgame6.exe SUCCESS Offset: 512 Length: 15872
760 2:10:47 PM vxgame6.exe:2868 QUERY INFORMATION C:\Documents and Settings\administrator\Desktop\vxgame6.exe SUCCESS FileNameIn
761 2:10:47 PM vxgame6.exe:2868 OPEN C:\WINDOWS\Prefetch\VXGAME6.EXE-03E98BC6.pf NOT FOUND Options: Open Access: All
762 2:10:47 PM vxgame6.exe:2868 OPEN C:\Documents and Settings\administrator\Desktop\vxgame6.exe SUCCESS Options: Open Directory Access: Traverse
763 2:10:47 PM vxgame6.exe:2868 QUERY INFORMATION C:\Documents and Settings\administrator\Desktop\vxgame6.exe Local NOT FOUND
764 2:10:47 PM vxgame6.exe:2868 QUERY INFORMATION C:\WINDOWS\system32\Entapi.dll SUCCESS Attributes: A
765 2:10:47 PM vxgame6.exe:2868 OPEN C:\WINDOWS\system32\Entapi.dll SUCCESS Options: Open Access: Execute
766 2:10:47 PM vxgame6.exe:2868 CLOSE C:\WINDOWS\system32\Entapi.dll SUCCESS
767 2:10:47 PM vxgame6.exe:2868 QUERY INFORMATION C:\WINDOWS\system32\PSAPI.DLL SUCCESS Attributes: A
768 2:10:47 PM vxgame6.exe:2868 OPEN C:\WINDOWS\system32\PSAPI.DLL SUCCESS Options: Open Access: Execute
769 2:10:47 PM vxgame6.exe:2868 CLOSE C:\WINDOWS\system32\PSAPI.DLL SUCCESS
770 2:10:47 PM vxgame6.exe:2868 QUERY INFORMATION C:\Documents and Settings\administrator\Desktop\vxgame6.exe SUCCESS Attributes
771 2:10:47 PM vxgame6.exe:2868 OPEN C:\Documents and Settings\administrator\Desktop\vxgame6.exe SUCCESS Options: Open Directory Access: A
772 2:10:47 PM vxgame6.exe:2868 DIRECTORY C:\Documents and Settings\administrator\Desktop\vxgame6.exe SUCCESS FilebothDirectoryInformation: Desk
773 2:10:47 PM vxgame6.exe:2868 CLOSE C:\Documents and Settings\administrator\Desktop\vxgame6.exe SUCCESS Options: Open Directory Access: A
774 2:10:47 PM vxgame6.exe:2868 OPEN C:\Documents and Settings\administrator\Desktop\vxgame6.exe SUCCESS Options: Open Directory Access: A
775 2:10:47 PM vxgame6.exe:2868 DIRECTORY C:\Documents and Settings\administrator\Desktop\vxgame6.exe SUCCESS FilebothDirectoryInformation: Desk
776 2:10:47 PM vxgame6.exe:2868 CLOSE C:\Documents and Settings\administrator\Desktop\vxgame6.exe SUCCESS
777 2:10:47 PM vxgame6.exe:2868 OPEN C:\Documents and Settings\All users\Application Data\Network Associates\BOPDATA\_Date-20060314_Tim
778 2:10:47 PM vxgame6.exe:2868 QUERY INFORMATION C:\Documents and Settings\All users\Application Data\Network Associates\BOPDATA\_Date-20060314_Tim
779 2:10:47 PM vxgame6.exe:2868 READ C:\Documents and Settings\All users\Application Data\Network Associates\BOPDATA\_Date-20060314_Tim
780 2:10:47 PM vxgame6.exe:2868 CLOSE C:\Documents and Settings\All users\Application Data\Network Associates\BOPDATA\_Date-20060314_Tim
781 2:10:47 PM vxgame6.exe:2868 OPEN C:\Documents and Settings\All users\Application Data\Network Associates\BOPDATA\_Date-20060314_Tim
782 2:10:47 PM vxgame6.exe:2868 QUERY INFORMATION C:\Documents and Settings\All users\Application Data\Network Associates\BOPDATA\_Date-20060314_Tim
783 2:10:47 PM vxgame6.exe:2868 READ C:\Documents and Settings\All users\Application Data\Network Associates\BOPDATA\_Date-20060314_Tim
784 2:10:47 PM vxgame6.exe:2868 CLOSE C:\Documents and Settings\All users\Application Data\Network Associates\BOPDATA\_Date-20060314_Tim
785 2:10:47 PM vxgame6.exe:2868 READ C:\WINDOWS\system32\advapi32.dll SUCCESS Offset: 373760 Length: 32768
786 2:10:47 PM vxgame6.exe:2868 CREATE C:\WINDOWS\system32\advapi32.dll SUCCESS options: overwriteif Access: All
```

Figure 7

This file found on the Installer CD is the mspm-bot Installer, see Figure 8.

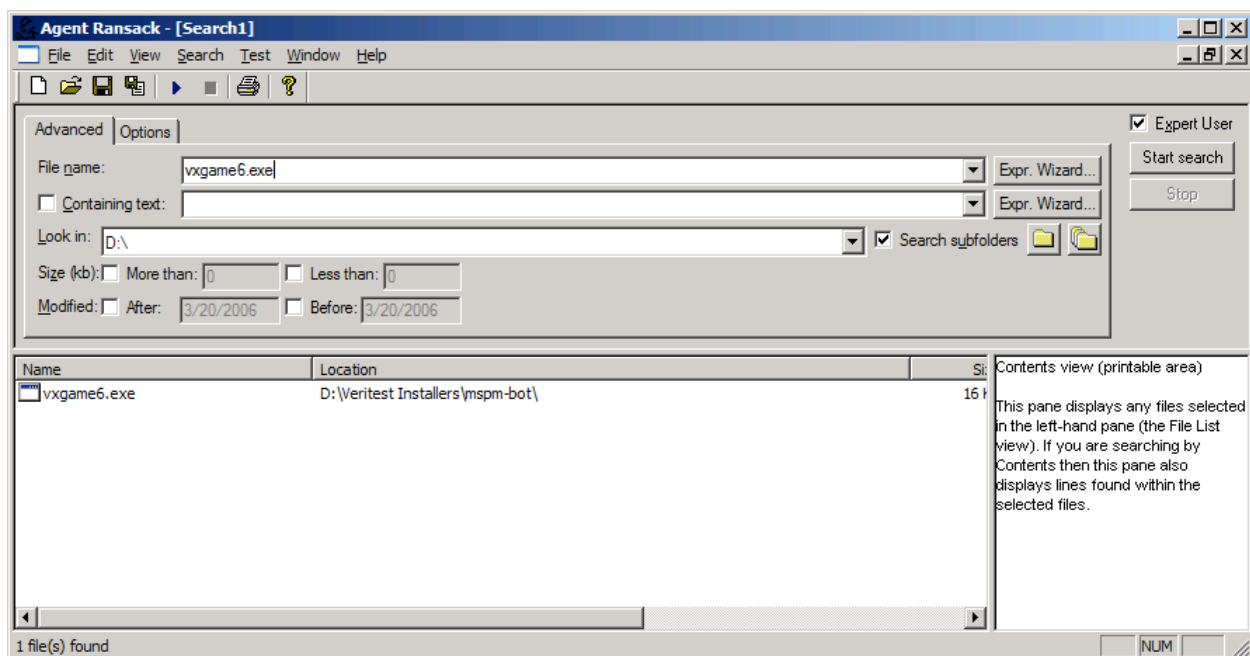
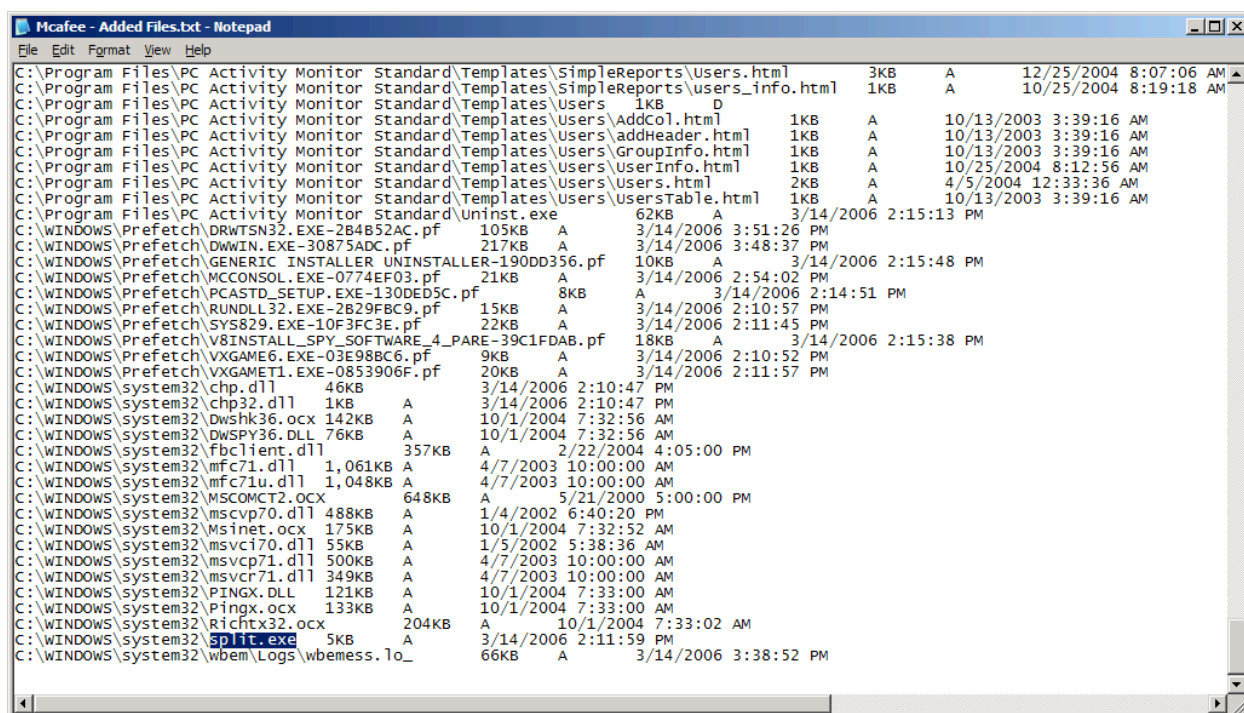


Figure 8

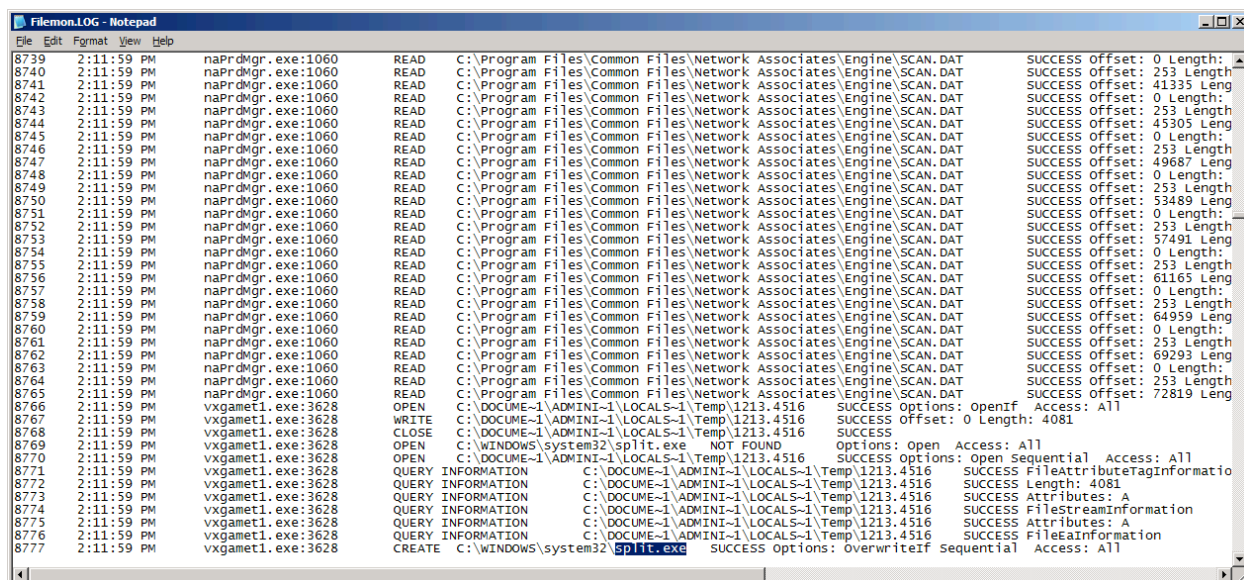
The last example is split.exe left in C:\Windows\system32, see Figures 9 and 10.



McAfee - Added Files.txt - Notepad

File	Size	Attributes	Date/Time
C:\Program Files\PC Activity Monitor\Standard\Templates\SimpleReports\users.html	3KB	A	12/25/2004 8:07:06 AM
C:\Program Files\PC Activity Monitor\Standard\Templates\SimpleReports\users_info.html	1KB	A	10/25/2004 8:19:18 AM
C:\Program Files\PC Activity Monitor\Standard\Templates\Users\1KB D			
C:\Program Files\PC Activity Monitor\Standard\Templates\Users\AddCol.html	1KB	A	10/13/2003 3:39:16 AM
C:\Program Files\PC Activity Monitor\Standard\Templates\Users\addHeader.html	1KB	A	10/13/2003 3:39:16 AM
C:\Program Files\PC Activity Monitor\Standard\Templates\Users\GroupInfo.html	1KB	A	10/13/2003 3:39:16 AM
C:\Program Files\PC Activity Monitor\Standard\Templates\Users\UserInfo.html	1KB	A	10/25/2004 8:12:56 AM
C:\Program Files\PC Activity Monitor\Standard\Templates\Users\Users.html	2KB	A	4/5/2004 12:33:36 AM
C:\Program Files\PC Activity Monitor\Standard\Templates\Users\UsersTable.html	1KB	A	10/13/2003 3:39:16 AM
C:\Program Files\PC Activity Monitor\Standard\Uninst.exe	62KB	A	3/14/2006 2:15:13 PM
C:\WINDOWS\Prefetch\DRWTSN32.EXE-2B4B52AC.pf	105KB	A	3/14/2006 3:51:26 PM
C:\WINDOWS\Prefetch\DWWIN.EXE-30875ADC.pf	217KB	A	3/14/2006 3:48:37 PM
C:\WINDOWS\Prefetch\GENERIC_INSTALLER_UNINSTALLER-190DD356.pf	10KB	A	3/14/2006 2:15:48 PM
C:\WINDOWS\Prefetch\MCCONSOL.EXE-0774EF03.pf	21KB	A	3/14/2006 2:54:02 PM
C:\WINDOWS\Prefetch\PCASTD_SETUP.EXE-130DED5C.pf	8KB	A	3/14/2006 2:14:51 PM
C:\WINDOWS\Prefetch\RUNDLL32.EXE-2B29FBC9.pf	15KB	A	3/14/2006 2:10:57 PM
C:\WINDOWS\Prefetch\SYS829.EXE-10F3FC3E.pf	22KB	A	3/14/2006 2:11:45 PM
C:\WINDOWS\Prefetch\V8INSTALL_SPY_SOFTWARE_4_PARE-39C1FDAB.pf	18KB	A	3/14/2006 2:15:38 PM
C:\WINDOWS\Prefetch\VXGAME6.EXE-03E98BC6.pf	9KB	A	3/14/2006 2:10:52 PM
C:\WINDOWS\Prefetch\VXGAMET1.EXE-0853906F.pf	20KB	A	3/14/2006 2:11:57 PM
C:\WINDOWS\system32\chp.dll	46KB	A	3/14/2006 2:10:47 PM
C:\WINDOWS\system32\chp32.dll	1KB	A	3/14/2006 2:10:47 PM
C:\WINDOWS\system32\Dwshk36.ocx	142KB	A	10/1/2004 7:32:56 AM
C:\WINDOWS\system32\DwSPY36.DLL	76KB	A	10/1/2004 7:32:56 AM
C:\WINDOWS\system32\Fbclient.dll	357KB	A	2/22/2004 4:05:00 PM
C:\WINDOWS\system32\mf71.dll	1,061KB	A	4/7/2003 10:00:00 AM
C:\WINDOWS\system32\mf71u.dll	1,048KB	A	4/7/2003 10:00:00 AM
C:\WINDOWS\system32\MSCOMCT2.OCX	648KB	A	5/21/2000 5:00:00 PM
C:\WINDOWS\system32\mscvp70.dll	488KB	A	1/4/2002 6:40:20 PM
C:\WINDOWS\system32\msinet.ocx	175KB	A	10/1/2004 7:32:52 AM
C:\WINDOWS\system32\msvc170.dll	55KB	A	1/5/2002 5:38:36 AM
C:\WINDOWS\system32\msvcp71.dll	500KB	A	4/7/2003 10:00:00 AM
C:\WINDOWS\system32\msvcr71.dll	349KB	A	4/7/2003 10:00:00 AM
C:\WINDOWS\system32\PINGX.DLL	121KB	A	10/1/2004 7:33:00 AM
C:\WINDOWS\system32\Pingx.ocx	133KB	A	10/1/2004 7:33:00 AM
C:\WINDOWS\system32\Richtx32.ocx	204KB	A	10/1/2004 7:33:02 AM
C:\WINDOWS\system32\Split.exe	5KB	A	3/14/2006 2:11:59 PM
C:\WINDOWS\system32\wbem\Logs\wbemess.1o_	66KB	A	3/14/2006 3:38:52 PM

Figure 9



Filemon.LOG - Notepad

Time	Process	Operation	Path	Result
8739 2:11:59 PM	naPrdMgr.exe:1060	READ	C:\Program Files\Common Files\Network Associates\Engine\SCAN.DAT	SUCCESS Offset: 0 Length: 253
8740 2:11:59 PM	naPrdMgr.exe:1060	READ	C:\Program Files\Common Files\Network Associates\Engine\SCAN.DAT	SUCCESS Offset: 41335 Leng
8741 2:11:59 PM	naPrdMgr.exe:1060	READ	C:\Program Files\Common Files\Network Associates\Engine\SCAN.DAT	SUCCESS Offset: 0 Length: 253
8742 2:11:59 PM	naPrdMgr.exe:1060	READ	C:\Program Files\Common Files\Network Associates\Engine\SCAN.DAT	SUCCESS Offset: 45305 Leng
8743 2:11:59 PM	naPrdMgr.exe:1060	READ	C:\Program Files\Common Files\Network Associates\Engine\SCAN.DAT	SUCCESS Offset: 0 Length: 253
8744 2:11:59 PM	naPrdMgr.exe:1060	READ	C:\Program Files\Common Files\Network Associates\Engine\SCAN.DAT	SUCCESS Offset: 49687 Leng
8745 2:11:59 PM	naPrdMgr.exe:1060	READ	C:\Program Files\Common Files\Network Associates\Engine\SCAN.DAT	SUCCESS Offset: 0 Length: 253
8746 2:11:59 PM	naPrdMgr.exe:1060	READ	C:\Program Files\Common Files\Network Associates\Engine\SCAN.DAT	SUCCESS Offset: 53489 Leng
8747 2:11:59 PM	naPrdMgr.exe:1060	READ	C:\Program Files\Common Files\Network Associates\Engine\SCAN.DAT	SUCCESS Offset: 0 Length: 253
8748 2:11:59 PM	naPrdMgr.exe:1060	READ	C:\Program Files\Common Files\Network Associates\Engine\SCAN.DAT	SUCCESS Offset: 57491 Leng
8749 2:11:59 PM	naPrdMgr.exe:1060	READ	C:\Program Files\Common Files\Network Associates\Engine\SCAN.DAT	SUCCESS Offset: 0 Length: 253
8750 2:11:59 PM	naPrdMgr.exe:1060	READ	C:\Program Files\Common Files\Network Associates\Engine\SCAN.DAT	SUCCESS Offset: 61165 Leng
8751 2:11:59 PM	naPrdMgr.exe:1060	READ	C:\Program Files\Common Files\Network Associates\Engine\SCAN.DAT	SUCCESS Offset: 0 Length: 253
8752 2:11:59 PM	naPrdMgr.exe:1060	READ	C:\Program Files\Common Files\Network Associates\Engine\SCAN.DAT	SUCCESS Offset: 64959 Leng
8753 2:11:59 PM	naPrdMgr.exe:1060	READ	C:\Program Files\Common Files\Network Associates\Engine\SCAN.DAT	SUCCESS Offset: 0 Length: 253
8754 2:11:59 PM	naPrdMgr.exe:1060	READ	C:\Program Files\Common Files\Network Associates\Engine\SCAN.DAT	SUCCESS Offset: 69293 Leng
8755 2:11:59 PM	naPrdMgr.exe:1060	READ	C:\Program Files\Common Files\Network Associates\Engine\SCAN.DAT	SUCCESS Offset: 0 Length: 253
8756 2:11:59 PM	naPrdMgr.exe:1060	READ	C:\Program Files\Common Files\Network Associates\Engine\SCAN.DAT	SUCCESS Offset: 72819 Leng
8757 2:11:59 PM	naPrdMgr.exe:1060	READ	C:\Program Files\Common Files\Network Associates\Engine\SCAN.DAT	SUCCESS Offset: 0 Length: 253
8758 2:11:59 PM	naPrdMgr.exe:1060	READ	C:\Program Files\Common Files\Network Associates\Engine\SCAN.DAT	SUCCESS Offset: 0 Length: 253
8759 2:11:59 PM	naPrdMgr.exe:1060	READ	C:\Program Files\Common Files\Network Associates\Engine\SCAN.DAT	SUCCESS Offset: 0 Length: 253
8760 2:11:59 PM	naPrdMgr.exe:1060	READ	C:\Program Files\Common Files\Network Associates\Engine\SCAN.DAT	SUCCESS Offset: 0 Length: 253
8761 2:11:59 PM	naPrdMgr.exe:1060	READ	C:\Program Files\Common Files\Network Associates\Engine\SCAN.DAT	SUCCESS Offset: 0 Length: 253
8762 2:11:59 PM	naPrdMgr.exe:1060	READ	C:\Program Files\Common Files\Network Associates\Engine\SCAN.DAT	SUCCESS Offset: 0 Length: 253
8763 2:11:59 PM	naPrdMgr.exe:1060	READ	C:\Program Files\Common Files\Network Associates\Engine\SCAN.DAT	SUCCESS Offset: 0 Length: 253
8764 2:11:59 PM	naPrdMgr.exe:1060	READ	C:\Program Files\Common Files\Network Associates\Engine\SCAN.DAT	SUCCESS Offset: 0 Length: 253
8765 2:11:59 PM	naPrdMgr.exe:1060	READ	C:\Program Files\Common Files\Network Associates\Engine\SCAN.DAT	SUCCESS Offset: 0 Length: 253
8766 2:11:59 PM	vxgamel1.exe:3628	OPEN	C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\1213.4516	SUCCESS Options: OpenIf Access: All
8767 2:11:59 PM	vxgamel1.exe:3628	WRITE	C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\1213.4516	SUCCESS Offset: 0 Length: 4081
8768 2:11:59 PM	vxgamel1.exe:3628	CLOSE	C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\1213.4516	SUCCESS
8769 2:11:59 PM	vxgamel1.exe:3628	OPEN	C:\WINDOWS\system32\split.exe	NOT FOUND Options: Open Access: All
8770 2:11:59 PM	vxgamel1.exe:3628	OPEN	C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\1213.4516	SUCCESS Options: open Sequential Access: All
8771 2:11:59 PM	vxgamel1.exe:3628	QUERY INFORMATION	C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\1213.4516	SUCCESS FileAttributeTagInformatio
8772 2:11:59 PM	vxgamel1.exe:3628	QUERY INFORMATION	C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\1213.4516	SUCCESS Length: 4081
8773 2:11:59 PM	vxgamel1.exe:3628	QUERY INFORMATION	C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\1213.4516	SUCCESS Attributes: A
8774 2:11:59 PM	vxgamel1.exe:3628	QUERY INFORMATION	C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\1213.4516	SUCCESS FileStreamInformation
8775 2:11:59 PM	vxgamel1.exe:3628	QUERY INFORMATION	C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\1213.4516	SUCCESS Attributes: A
8776 2:11:59 PM	vxgamel1.exe:3628	QUERY INFORMATION	C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\1213.4516	SUCCESS FileInformation
8777 2:11:59 PM	vxgamel1.exe:3628	CREATE	C:\WINDOWS\system32\split.exe	SUCCESS options: Overwriteif Sequential Access: All

Figure 10

The Filemon log shows that split.exe was written by vxgamet1.exe, see Figure 11.

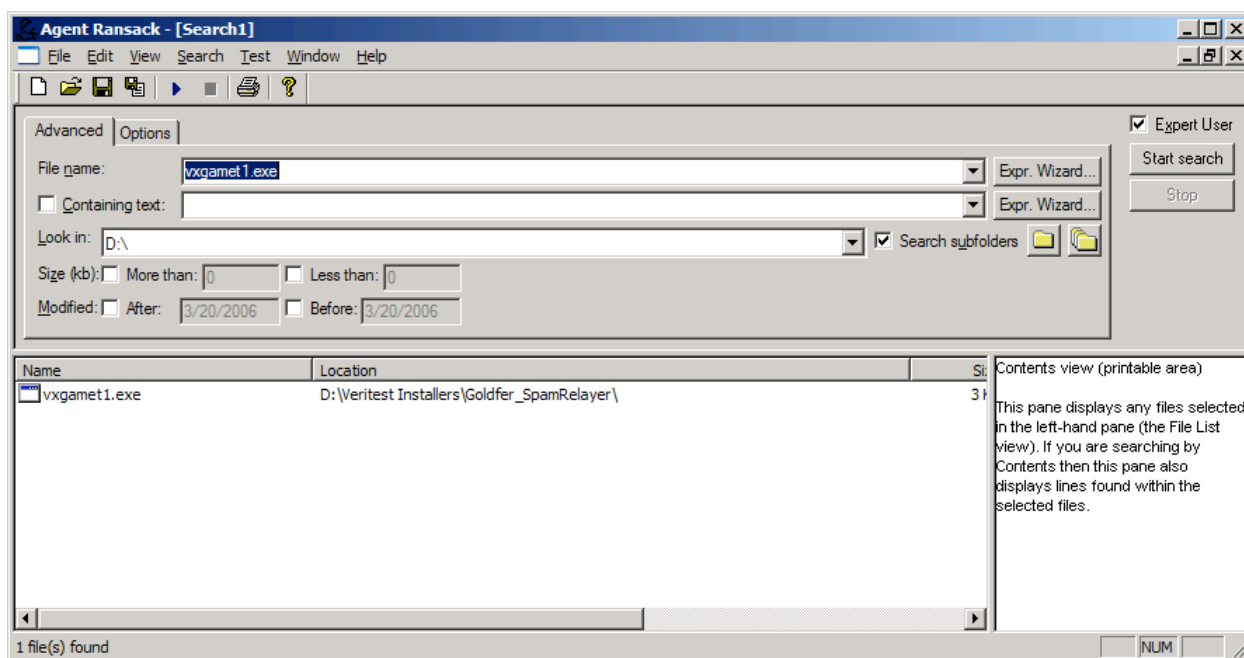


Figure 11

Searching the Installer CD it is found that vxgamet1.exe is the installer for Goldfer_SpamRelayer.

It is often advisable to search the Internet for information concerning the files left on disk. Searching Google for the filename split.exe reveals interesting results, see Figure 12.

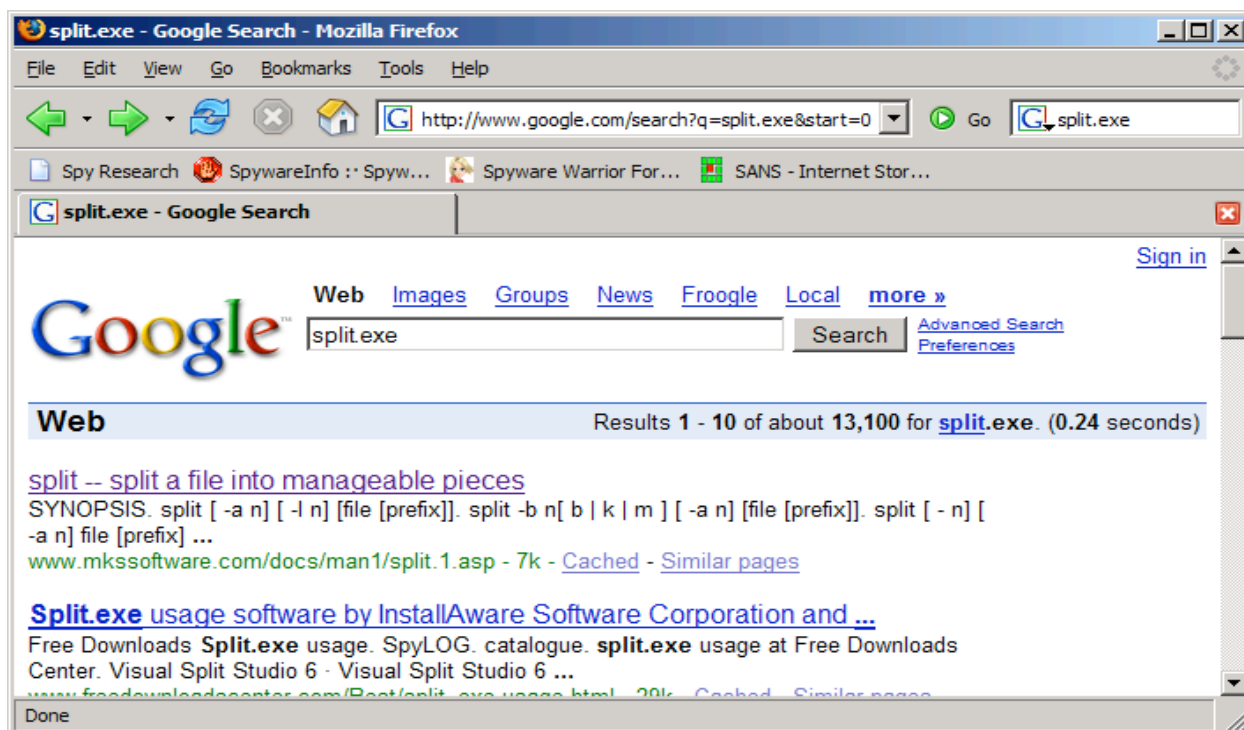


Figure 12

It is possible that the file left on disk split.exe is the utility mentioned in the first result. At this point, more investigation is needed such as looking at the internals of the file, running it on a clean machine, and seeing what changes it makes and what it attempts to do. If time permits, this is an advisable way to determine if this leftover file is truly malicious or if the spyware installed is putting legitimate files on the system to attempt to fool the anti-spyware software.

Method Summary

This testing methodology is a very accurate way to measure the capabilities of anti-spyware products in a controlled manner against a wide variety of threats. To get this kind of accuracy requires having a large sample of previously identified spyware installers, the time required to do a full round of installation, detection and removal of the spies, and then analysis of the logs and probably of the files themselves.

Given all these factors it is not advisable to attempt this level of testing, the time required is a limiting factor and proper analysis of the logs requires an intimate knowledge of the spies being tested against.

It is also not advisable to test in other manners including testing against a known infected machine, testing against a known installer of Spyware such as Kazaa or Grokster, or visiting a website known to distribute spyware via a “drive-by” exploit. The problems with these types of testing includes: an unknown amount of spies installed leads to inaccurate results of Clean versus Not Clean, a limited test bed of only a few pieces of adware installed do not truly show if an anti-spyware product can detect or remove keyloggers or Trojans, and there is still a learning curve to understand what the product has detected and removed fully and analysis of files leftover to determine if they truly constitute a threat to the user.

APPENDIX A: NETWORK TOPOLOGY

Each Enterprise software was installed to a dedicated Windows 2003 Standard Server. Each product in this test had three client PC's dedicated as Agents. All Server's and PC's were connected to a shared Ethernet Switch. All Server's and PC's obtained Internet Access via a Proxy Server.

