

# 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 antispyware applications:

- Webroot Spy Sweeper Enterprise 2.5.1
- Symantec AntiVirus Corproate 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

### **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.

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 test<sup>1</sup>. 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

<sup>&</sup>lt;sup>1</sup> 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.

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.

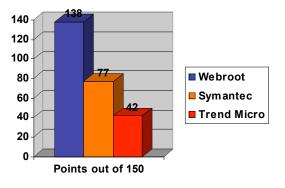
### VeriTest Enterprise Anti-Spyware Test Scoring:

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.

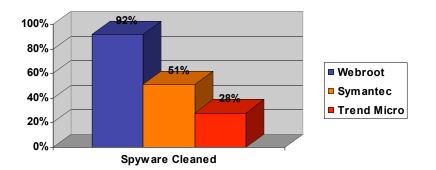


# **Test Findings**

### Spyware Identification and Removal Effectiveness Testing

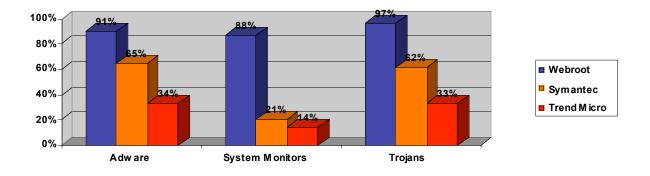
### Results

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> <li>The Installer was not removed from the desktop or the System32 directory.</li> <li>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.<sup>2</sup></li> <li>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.</li> <li>Any browser hijack(s) created by one of the installed spies.<sup>3</sup></li> </ul>
Clean:	<ul> <li>If none of the conditions of Dirty have been met the spy is considered Clean.</li> </ul>

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.

<sup>3</sup> Examples of browser hijacks include;

http://search.2020search.com/9894/search/redir.php?cid=shnv9894PCID=00000000000007858367&s=

<sup>&</sup>lt;sup>2</sup> 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.

HKEY\_CURRENT\_USER\Software\Microsoft\Search Assistant DefaultSearchURL

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/

📕 Mcafee - Added Files.txt - Notepad		
<u>File E</u> dit F <u>o</u> rmat <u>V</u> iew <u>H</u> elp		
C:\QUARANTINE 1KB D C:\QUARANTINE\A00011124.exe.Vir 17KE C:\QUARANTINE\infected.log 1KB C:\QUARANTINE\vxgame6.exe.Vir 17KE C:\Shot.log 11KB A 3/14 C:\windowsupdate 1KB D C:\windowsupdate\ufp 1KB D C:\windowsupdate\ufp\ss47 1KB C:\windowsupdate\ufp\ss47\uninstall.	A 3/14/2006 2:35:53 PM B RA 10/9/2005 8:19:13 PM 4/2006 3:55:23 PM D	1 PM
C:\windowsupdate\ufp\ss47\Uninstall. C:\Documents and Settings\administra C:\Documents and Settings\administra C:\Documents and Settings\administra C:\Documents and Settings\administra C:\Documents and Settings\administra C:\Documents and Settings\administra C:\Documents and Settings\administra	.exe 83KB A 10/10/2004 6:12:5 ator\Desktop\CActivity Monitor Stand ator\Desktop\CActivity Monitor Stand ator\Local Settings\History\History.IE ator\Local Settings\History\History.IE ator\Local Settings\Temp\213.4516 ator\Local Settings\Temp\213.4516 ator\Local Settings\Temp\213.4516 ator\Local Settings\Temp\213.4516 ator\Local Settings\Temp\213.4516 ator\Recent\031406-6.1nk 1KB A	50 PM dard.lnk 1KB A 3/14/2006 2:15:14 PM parents.exe 2,735KB RA 10/10/2005 1:15:38 PM 55/M5Hist012006031420060315 1KB D 55/M5Hist012006031420060315/index.dat 33KB A KB A 3/14/2006 2:11:59 PM LKB A 3/14/2006 2:10:52 PM 5KB A 3/14/2006 3:48:24 PM A 3/14/2006 2:18:34 PM
C:\Documents and Settings\administra C:\Documents and Settings\administra C:\Documents and Settings\administra C:\Documents and Settings\administra C:\Documents and Settings\All Users\ C:\Documents and Settings\All Users\	ator\Recent\Regmon.LOG.lnk 1KB A ator\Start Menu\Programs\PC Activity M ator\Start Menu\Programs\PC Activity M ator\Start Menu\Programs\PC Activity M ator\Start Menu\Programs\PC Activity M ator\Start Menu\Programs\PC Activity M \Application Data\Microsoft\Dr Watson \Application Data\Microsoft\Dr Watson	Monitor standard 1KB D Monitor standard\Help.lnk 1KB A 3/14/ Monitor standard\Help.lnk 1KB A 3/14/ Monitor standard\PC Activity Monitor Standard.lnk Monitor standard\Uninstall.lnk 1KB A 3/14/ 1KB D (drwtsn32.log 456KB A 3/14/2006 3:51:23 PM
<pre>C:\Documents and Settings\All Users\ C:\Documents and Settings\All Users\ C:\Documents and Settings\All Users\ C:\Documents and Settings\All Users\ C:\Program Files\PC Activity Monitor C:\Program Files\PC Activity Monitor</pre>	\Application Data\Network Associates\8 \Application Data\Network Associates\C \Application Data\Network Associates\V r Standard 1KB D r Standard\BackUp 1KB D r Standard\Config 1KB D	ioPDATA\_Date-20060314_Time-154053684_EnterceptExcept SOPDATA\_Date-20060314_Time-154053684_EnterceptRules. common Framework\AgentEvents\00000019.txml 2KB /irusScan\onDemandScanLog.txt 11KB A 3/14/
C:\Program Files\PC Activity Monitor C:\Program Files\PC Activity Monitor C:\Program Files\PC Activity Monitor C:\Program Files\PC Activity Monitor	r Standard\config\Text_štr.txt 2 r Standard\FireBird 1KB D	A 3/14/2006 2:15:16 PM 208KB A 2/24/2005 7:14:48 AM LKB A 11/11/2004 5:07:18 AM

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.

🔏 Agent Ransack - [Search1]	
Elle Edit View Search Test Window Help	
Advanced Options	Expert User
File name: v8install_spy_software_4_parents.exe	Expr. Wizard
<u>C</u> ontaining text:	Expr. Wizard     Stop
Look in: D:\	bfolders 🔲 🏠
Size (kb): More than: 0 Less than: 0	
Modified: After: 3/20/2006 Before: 3/20/2006	
]	
Name Location	Si: Contents view (printable area)
	71
	This pane displays any files selected in the left-hand pane (the File List
	711 This pane displays any files selected in the left-hand pane (the File List view). If you are searching by
	This pane displays any files selected in the left-hand pane (the File List view). If you are searching by Contents then this pane also
	711 This pane displays any files selected in the left-hand pane (the File List view). If you are searching by
	This pane displays any files selected in the left-hand pane (the File List view). If you are searching by Contents then this pane also displays lines found within the
	This pane displays any files selected in the left-hand pane (the File List view). If you are searching by Contents then this pane also displays lines found within the
	This pane displays any files selected in the left-hand pane (the File List view). If you are searching by Contents then this pane also displays lines found within the
	This pane displays any files selected in the left-hand pane (the File List view). If you are searching by Contents then this pane also displays lines found within the

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.

Mcafee - Added Files.		<u>_                                    </u>
C:\windowsupdate\ C:\Documents and C:\Documents and C:\Documents and C:\Documents and C:\Documents and C:\Documents and C:\Documents and C:\Documents and	<pre>Ufp 1KB D Ufp\ss47 LKB D Ufp\ss47\uninstall.dat1KB A 10/9/2004 7:18:54 PM Ufp\ss47\uninstall.dat1KB A 10/10/2004 6:12:50 PM Settings\administrator\besktop\vC Activity Monitor Standard.lnk 1KB A 3/14/2006 2:15:1 Settings\administrator\besktop\vC Activity Monitor Standard.lnk 1KB A 3/14/2006 2:15:1 Settings\administrator\besktop\vSinstall_spy_software_4_parents.exe 2,735KB RA 10/10/2005 1:15: Settings\administrator\bocal Settings\History\History.IE5\MSHist012006031420060315 1KB D Settings\administrator\bocal Settings\History\History.IE5\MSHist012006031420060315\index.dat 33KB Settings\administrator\bocal Settings\Temp\1213.4516 5KB A 3/14/2006 2:10:52 PM Settings\administrator\bocal Settings\Temp\tsk.sys 5KB A 3/14/2006 3:48:24 PM Settings\administrator\bocal Settings\Temp\tsk.sys 5KB A 3/14/2006 2:10:52 PM Settings\administrator\bocal Settings\Temp\tsk.sys 5KB A 3/14/2006 3:48:24 PM Settings\administrator\bocal Settings\Temp\tsk.sys 5KB A 3/14/2006 3:48:24 PM</pre>	
C:\Documents and C:\Documents and C:\Documents and C:\Documents and C:\Documents and C:\Documents and C:\Documents and C:\Documents and C:\Documents and C:\Documents and	Settings\administrator\Start Menu\Programs\PC Activitý Monitor Standard\License.lnk 1KB A Settings\administrator\Start Menu\Programs\PC Activity Monitor Standard\PC Activity Monitor Standard.ln Settings\administrator\Start Menu\Programs\PC Activity Monitor Standard\PC Activity Monitor Standard.ln Settings\all users\Application Data\Microsoft\Dr Watson 1KB D Settings\All users\Application Data\Microsoft\Dr Watson\drwtsn32.log 456KB A 3/14/2006 3:51:2 Settings\All users\Application Data\Microsoft\Dr Watson\user.dmp 32KB A 3/14/2006 3:51:2 Settings\All users\Application Data\Microsoft\Dr Watson\user.dmp 32KB A 3/14/2006 3:51:2 Settings\All users\Application Data\Microsoft\Dr Watson\user.dmp 32KB A 3/14/2006 3:51:2 Settings\All users\Application Data\Network Associates\BOPDATA\_Date-20060314_Time-154053684_EnterceptE	3/14/ 3 PM 4 PM Except
C:\program Files\ C:\program Files\		3/14/
	PC Activity Monitor Standard (FireBird DOC) FireDird_VI.3.RefeaseNotes.pdf 422KB A 2/19/200 PC Activity Monitor Standard (FireBird firebird.conf 19KB A 12/8/2004 7:12:18 AM	,4 4:0 ▼

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 pcastd\_setup.ex created fbserver.exe, see Figure 4.

📕 Filemon.LO	DG - Notepad			_ 🗆 ×
Eile Edit For	rmat <u>V</u> iew <u>H</u> elp			
	:15:07 PM	pcastd_setup.ex:3456	WRITE C:\Program Files\PC Activity Monitor Standard\FireBird\security.fdb SUCCESS Offset: 5	07904 Len 🔺
	:15:07 PM	pcastd_setup.ex:3456	READ C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\nsp6.tmp SUCCESS offset: 775813 Length: 16384	
	:15:07 PM	pcastd_setup.ex:3456	WRITE C:\Program Files\PC Activity Monitor Standard\FireBird\security.fdb SUCCESS Offset: 5	24288 Len
	:15:07 PM	pcastd_setup.ex:3456	READ C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\nsp6.tmp SUCCESS Offset: 792197 Length: 16384	
	:15:07 PM	pcastd_setup.ex:3456	WRITE C:\Program Files\PC Activity Monitor Standard\FireBird\security.fdb SUCCESS Offset: 5	40672 Len
	:15:07 PM	pcastd_setup.ex:3456	READ C:\DOCUME~1\ADMINI~1\LOCAL5~1\Temp\nsp6.tmp SUCCESS Offset: 808581 Length: 16384	
	:15:07 PM	pcastd_setup.ex:3456	WRITE C:\Program Files\PC Activity Monitor Standard\FireBird\security.fdb SUCCESS Offset: 5	57056 Len
	:15:07 PM	pcastd_setup.ex:3456	READ C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\nsp6.tmp SUCCESS offset: 824965 Length: 16384	
	:15:07 PM	pcastd_setup.ex:3456	WRITE C:\Program Files\PC Activity Monitor Standard\FireBird\security.fdb SUCCESS Offset: 5	73440 Len
	:15:07 PM	pcastd_setup.ex:3456	READ C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\nsp6.tmp SUCCESS Offset: 841349 Length: 16384	
	:15:07 PM	pcastd_setup.ex:3456	WRITE C:\Program Files\PC Activity Monitor Standard\FireBird\security.fdb SUCCESS Offset: 5	89824 Len
	:15:07 PM	pcastd_setup.ex:3456	READ C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\nsp6.tmp SUCCESS Offset: 857733 Length: 16384	
	:15:07 PM	pcastd_setup.ex:3456	WRITE C:\Program Files\PC Activity Monitor Standard\FireBird\security.fdb SUCCESS Offset: 6	06208 Len
	:15:07 PM	pcastd_setup.ex:3456	READ C:\DOCUME~1\ADMINI~1\LOCAL5~1\Temp\nsp6.tmp SUCCESS Offset: 874117 Length: 16384	
	:15:07 PM	pcastd_setup.ex:3456	WRITE C:\Program Files\PC Activity Monitor Standard\FireBird\security.fdb SUCCESS Offset: 6	22592 Len
	:15:07 PM	pcastd_setup.ex:3456	READ C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\nsp6.tmp SUCCESS Offset: 890501 Length: 4096	
	:15:07 PM	pcastd_setup.ex:3456	WRITE C:\Program Files\PC Activity Monitor Standard\FireBird\security.fdb SUCCESS Offset: 6	
	:15:07 PM	pcastd_setup.ex:3456		UCCESS Fi
	:15:07 PM	pcastd_setup.ex:3456	CLOSE C:\Program Files\PC Activity Monitor Standard\FireBird\security.fdb SUCCESS	
	:15:07 PM	pcastd_setup.ex:3456	OPEN C:\ SUCCESS Options: Open Directory Access: All	
	:15:07 PM	pcastd_setup.ex:3456	DIRECTORY C:\ SUCCESS FileBothDirectoryInformation: Program Files	
	:15:07 PM	pcastd_setup.ex:3456	CLOSE C:\ SUCCESS	
	:15:07 PM	pcastd_setup.ex:3456	OPEN C:\Program Files\ SUCCESS Options: Open Directory Access: All	
	:15:07 PM	pcastd_setup.ex:3456	DIRECTORY C:\Program Files\ SUCCESS FileBothDirectoryInformation: PC Activity Monitor	Standard
	:15:07 PM	pcastd_setup.ex:3456	CLOSE C:\Program Files\ SUCCESS	
	:15:07 PM	pcastd_setup.ex:3456	OPEN C:\Program Files\PC Activity Monitor Standard\ SUCCESS Options: Open Directory Access:	A]]
	:15:07 PM	pcastd_setup.ex:3456	DIRECTORY C:\Program Files\PC Activity Monitor Standard\ SUCCESS FileBothDirectoryInformat	ion: Fire
18066 2	:15:07 PM	pcastd_setup.ex:3456	CLOSE C:\Program Files\PC Activity Monitor Standard\ SUCCESS	
	:15:07 PM	pcastd_setup.ex:3456	OPEN C:\Program Files\PC Activity Monitor Standard\FireBird\ SUCCESS Options: Open Directory	
	:15:07 PM	pcastd_setup.ex:3456	DIRECTORY C:\Program Files\PC Activity Monitor Standard\FireBird\ NO SUCH FILE FileBothD	irectoryI
	:15:07 PM	pcastd_setup.ex:3456	CLOSE C:\Program Files\PC Activity Monitor Standard\FireBird\ SUCCESS	
	:15:07 PM	pcastd_setup.ex:3456	CREATE C:\Program Files\PC Activity Monitor Standard\FireBird\Bin SUCCESS Options: Create D	irectory 📃
	:15:07 PM	pcastd_setup.ex:3456	CLOSE C:\Program Files\PC Activity Monitor Standard\FireBird\Bin SUCCESS	-
	:15:07 PM	pcastd_setup.ex:3456	OPEN C:\Program Files\PC Activity Monitor Standard\FireBird\Bin SUCCESS Options: Open Dir	ectory A
	:15:07 PM	pcastd_setup.ex:3456	CLOSE C:\Program Files\PC Activity Monitor Standard\FireBird SUCCESS	
	:15:07 PM	pcastd_setup.ex:3456	QUERY INFORMATION C:\Program files\PC Activity Monitor Standard\FireBird\Bin\fbserver.exe N	
	:15:07 PM	pcastd_setup.ex:3456		ptions: 0
	:15:07 PM	pcastd_setup.ex:3456	QUERY INFORMATION C:\Program files\PC Activity Monitor Standard\FireBird\Bin\fbserver.exe N	
18077 2	:15:07 PM	pcastd_setup.ex:3456	CREATE C:\Program Files\PC Activity Monitor Standard\FireBird\Bin\ <mark>fbserver.exe</mark> SUCCESS Options:	Overwrite
		•		<u> </u>
•				•
			-	

#### Figure 4 Filemon log

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

& Agent Ransack - [Search1]			
File Edit View Search Test Wi	ndow Help		_8×
🗅 🖆 🖬 🥦 🕨 🔳 🎒 🤶			
Advanced Options			Expert User
File name: pcastd			Expr. Wizard
Containing text:			Expr. Wizard
Look in: D:\		<ul> <li>Search</li> </ul>	n subfolders 🚊 🛅
Size (kb): More than:	Less than: 0		
Modified: After: 3/20/2006	Before: 3/20/2006		
]			
Name	Location		Si: Contents view (printable area)
			SI, Contents view (printable area)
pcastd_setup.exe	D:\Veritest Installers\PC Activity Monitor\		31661
資 pcastd_setup.exe	D:\Veritest Installers\PC Activity Monitor\		3166 H This pane displays any files selected
浳。 pcastd_setup.exe	D:\Veritest Installers\PC Activity Monitor\	I	31661
"譚pcastd_setup.exe	D: \Veritest Installers\PC Activity Monitor \		3166) This pane displays any files selected in the left-hand pane (the File List view). If you are searching by Contents then this pane also
"聞"pcastd_setup.exe	D: \Veritest Installers\PC Activity Monitor \		3166) This pane displays any files selected in the left-hand pane (the File List view). If you are searching by Contents then this pane also displays lines found within the
"聞"pcastd_setup.exe	D: \Veritest Installers\PC Activity Monitor \		3166) This pane displays any files selected in the left-hand pane (the File List view). If you are searching by Contents then this pane also
ॷॎॕPpcastd_setup.exe	D: \Veritest Installers\PC Activity Monitor \		3166) This pane displays any files selected in the left-hand pane (the File List view). If you are searching by Contents then this pane also displays lines found within the
"譚 pcastd_setup.exe	D:\Veritest Installers\PC Activity Monitor\		3166) This pane displays any files selected in the left-hand pane (the File List view). If you are searching by Contents then this pane also displays lines found within the
ॷॎॕॖpcastd_setup.exe	D:\Veritest Installers\PC Activity Monitor\		3166) This pane displays any files selected in the left-hand pane (the File List view). If you are searching by Contents then this pane also displays lines found within the
读 pcastd_setup.exe	D: \Veritest Installers\PC Activity Monitor \		3166) This pane displays any files selected in the left-hand pane (the File List view). If you are searching by Contents then this pane also displays lines found within the

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

Mcafee - Added Files.txt - Notepad				
Edit Format View Help				
<pre>\Program Files\PC Activity Monitor Standard\Templates\SimpleReports\Office\office.html</pre>	4KB	А		04 3:32
<pre>\Program Files\PC Activity Monitor Standard\Templates\SimpleReports\Office\office_info.html</pre>	1KB	A	3/15/2	004 4:3
Program Files\PC Activity Monitor Standard\Templates\SimpleReports\Password 1KB D		2 /1 0 /2		
<program 4kb<br="" activity="" files\pc="" monitor="" standard\templates\simplereports\password\pwd.html="">Program Files\PC Activity Monitor Standard\Templates\SimpleReports\Password\pwd_info.html</program>	А 1КВ	3/18/2 A	004 4:26	004 8:0
Program Files/PC Activity Monitor Standard/Templates/SimpleReports/Password/pwd_item.html	1KB	Ä		004 8.0
Program Files/PC Activity Monitor Standard Templates/SimpleReports/Programs IKB D	TIND	<u>^</u>	1/13/2	004 1.4
Program Files PC Activity Monitor Standard Templates SimpleReports Programs Programs.html	ЗКВ	А	8/23/2	004 6:1
Program Files\PC Activity Monitor Standard\Templates\SimpleReports\Programs\program_info.ht	ml	1KB	A	8/23/
Program Files\PC Activity Monitor Standard\Templates\SimpleReports\Programs\Sess_info.html	1KB	Α	8/23/2	004 7:0
<pre>\Program Files\PC Activity Monitor Standard\Templates\SimpleReports\URL 1KB D</pre>				
Program Files\PC Activity Monitor Standard\Templates\SimpleReports\URL\url.html 3KB	A		004 4:25	
Program Files/PC Activity Monitor Standard/Templates/SimpleReports/URL/url_info.html 1KB	A		004 6:48	
<pre>\Program Files\PC Activity Monitor Standard\Templates\SimpleReports\URL\url_item.html 1KB \Program Files\PC Activity Monitor Standard\Templates\SimpleReports\Users.html 3KB</pre>	A		004 6:48 2004 8:0	
Program Files/PC Activity Monitor Standard/Templates/SimplexeportS/UserS.ntml 3KB	A		2004 8:0	
Program Files/PC Activity Monitor Standard Templates/Users 1KB D	~	10/23/	2004 0.1	9.10 A
Program Files/PC Activity Monitor Standard/Templates/Users/AddCol.html 1KB A	10/13	/2003 3:3	9:16 AM	
Program Files\PC Activity Monitor Standard\Templates\Users\addHeader.html 1KB A		/2003 3:3		
Program Files\PC Activity Monitor Standard\Templates\Users\GroupInfo.html 1KB A	10/13	/2003 3:3	9:16 AM	
Program Files\PC Activity Monitor Standard\Templates\Users\UserInfo.html 1KB A		/2004 8:1		
<pre>\Program Files\PC Activity Monitor Standard\Templates\Users\Users.html 2KB A</pre>		004 12:33		
Program Files\PC Activity Monitor Standard\Templates\Users\UsersTable.html 1KB A		/2003 3:3	9:16 AM	
Program Files/PC Activity Monitor Standard/Uninst.exe 62KB A 3/14/2006 2:15	:13 PM			
WINDOWS\Prefetch\DRWTSN32.EXE-284B52AC.pf 105KB A 3/14/2006 3:51:26 PM WINDOWS\Prefetch\DWWIN.EXE-30875ADC.pf 217KB A 3/14/2006 3:48:37 PM				
<pre>\windows\Prefetch\Dwwin.exe-30875aDc.pf 217KB A 3/14/2006 3:48:37 PM \windows\Prefetch\Generic installer uninstaller-190DD356.pf 10KB A 3/14/2006 2:15</pre>	•18 DM			
WINDOWS\Prefetch\MCCONSOL.EXE-0774EF03.pf 21KB A 3/14/2006 2:54:02 PM	.40 114			
WINDOWS\Prefetch\PCASTD_SETUP.EXE-130DED5C.pf 8KB A 3/14/2006 2:14:51 PM				
WINDOWS\Prefetch\RUNDLL32.EXE-2829FBC9.pf 15KB A 3/14/2006 2:10:57 PM				
WINDOWS\Prefetch\SYS829.EXE-10F3FC3E.pf 22KB A 3/14/2006 2:11:45 PM				
wINDOWS\Prefetch\V8INSTALL_SPY_SOFTWARE_4_PARE-39C1FDAB.pf 18KB A 3/14/2006 2:15	:38 PM			
WINDOWS\Prefetch\VXGAME6.EXE-03E98BC6.pf 9KB A 3/14/2006 2:10:52 PM				
WINDOWS\Prefetch\VXGAMET1.EXE-0853906F.pf 20KB A 3/14/2006 2:11:57 PM				
WINDOWS\system32\chp.dll 46KB 3/14/2006 2:10:47 PM WINDOWS\system32\chp32.dll 1KB A 3/14/2006 2:10:47 PM				
<pre>\windows\system32\chp32.dll 1KB A 3/14/2006 2:10:47 PM \windows\system32\dwshk36.ocx 142KB A 10/1/2004 7:32:56 AM</pre>				
WINDOWS/System32/DWSPY36.DLL 76KB A 10/1/2004 7:32:36 AM				
WINDOWS/System32/fbclient.dll 357KB A 2/22/2004 4:05:00 PM				
				•

### Figure 6

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

📕 Filemo	n.LOG - Notepad		
<u>Eile E</u> dit	Format <u>V</u> iew <u>H</u> elp		
Ele Edit 748 749 750 751 753 754 755 755 755 755 755 755 755 755 755	Pgmat         Yew         Help           2:10:26         PM           2:10:26         PM           2:10:26         PM           2:10:20         PM           2:10:20         PM           2:10:30         PM           2:10:30         PM           2:10:30         PM           2:10:30         PM           2:10:47         PM           2:10:47	Regmon. exe:2064 QUERY Regmon. exe:2064 QUERY Regmon. exe:2064 CLOSE FrameworKservic:1872 FrameworKservic:1872 FrameworKservic:1872 FrameworKservic:1872 FrameworKservic:1872 FrameworKservic:1872 FrameworKservic:1872 Csrss.exe:788 READ vxgame6.exe:2868	INFORMATION C:\Program Files\Network Associates\VirusScan\Mcshield.exe SUCCESS Length: 221191 LiPRORMATION C:\Program Files\Network Associates\VirusScan\Mcshield.exe SUCCESS Length: 221191 C:\Program Files\Network Associates\VirusScan\Mcshield.exe SUCCESS Length: 221191 C:\Program Files\Network Associates\VirusScan\Mcshield.exe SUCCESS Length: 221191 DPEN C:\Documents and Settings\All user\Application Data\Network Associates\Common Framework\Task\Task DTRECTORY C:\Documents and Settings\All user\Application Data\Network Associates\Common Framework\Task\Task DTRECTORY C:\Documents and Settings\All user\Application Data\Network Associates\Common Framework\T DUERY INFORMATION C:\Documents and Settings\All user\Application Data\Network Associates\Common Framework\T DUERY INFORMATION C:\Documents and Settings\All user\Application Data\Network Associates\Common Framework\T CLOSE C:\Documents and Settings\All user\Application Data\Network Associates\Common Framework\T CLOSE C:\Documents and Settings\All user\Application Data\Network Associates\Common Framework\Task\Task C: SUCCESS offset: 786432 Length: 8192 C:\Documents and Settings\All user\Application Data\Network Associates\Common Framework\Task\Task C: SUCCESS offset: 512 Length: 15872 QUERY INFORMATION C:\Documents and Settings\Administrator\Desktop\vxgame6.exe SUCCESS offors: 512 Length: 15872 QUERY INFORMATION C:\Documents and Settings\Administrator\Desktop\vxgame6.exe Local NOT FollyD OFEN C:\Documents and Settings\All users\Application Data\Network Associates\Common Framevork\Task\Task C: SUNDOWS\System32\FAPFI.DLL SUCCESS OFfons: Open Access: All NOT FOUND QUERY INFORMATION C:\Documents and Settings\Administrator\Desktop\vxgame6.exe SUCCESS Attributes C:\MINDOWS\System32\FAPFI.DLL SUCCESS OFEN C:\Documents and Settings\Administrator\ SUCCESS FileBothDirectoryAccess: All DEECTORY C:\Documents and Settings\Administrator\ SUCCESS FileBothDirectoryInformation: Desk CLOSE C:\Documents and Settings\Administrator\ SUCCESS FileBothDirectory
778 779 780 781 782 783 784 785 786	2:10:47 PM 2:10:47 PM 2:10:47 PM 2:10:47 PM 2:10:47 PM 2:10:47 PM 2:10:47 PM 2:10:47 PM 2:10:47 PM	vxgame6.exe:2868 vxgame6.exe:2868 vxgame6.exe:2868 vxgame6.exe:2868 vxgame6.exe:2868 vxgame6.exe:2868 vxgame6.exe:2868 vxgame6.exe:2868 vxgame6.exe:2868	QUERY INFORMATION C:\Documents and Settings\All users\Application Data\Metwork Associates\BoPDATA\_D READ C:\Documents and Settings\All users\Application Data\Metwork Associates\BoPDATA\_Date-20060314_Tim CLOSE C:\Documents and Settings\All users\Application Data\Metwork Associates\BoPDATA\_Date-20060314_Tim OPEN C:\Documents and Settings\All users\Application Data\Metwork Associates\BoPDATA\_Date-20060314_Tim QUERY INFORMATION C:\Documents and Settings\All users\Application Data\Metwork Associates\BoPDATA\_Date-20060314_Tim CLOSE C:\Documents and Settings\All users\Application Data\Metwork Associates\BoPDATA\_Date-20060314_Tim CLOSE C:\Documents and Settings\All users\Application Data\Metwork Associates\BoPDATA\_Date-20060314_Tim CLOSE C:\Documents and Settings\All users\Application Data\Metwork Associates\BoPDATA\_Date-20060314_Tim READ C:\WINDOWS\System32\advapi32.dll SUCCESS Offset: 373760 Length: 32768 CREATE C:\WINDOWS\System32\advap32.dll SUCCESS Options: OverwriteIf Access: All
•			

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

& Agent Ransack - [Search1]		
<u> </u>	<u>N</u> indow <u>H</u> elp	
] D 🛎 🖬 🗞   ▶ 🔳 😂   🧐	?	
Advanced Options		Expert User
File name: vxgame6.exe		Expr. Wizard Start search
Containing text:		Expr. Wizard Stop
Look in: D:\	▼ V Sea	arch subfolders 🔲 🔄
Size (kb): More than: 0	Less than: 0	
Modified: After: 3/20/2006	Before: 3/20/2006	
1		
J		
Name	Location	<u>Si</u> Contents view (printable area)
Name vxgame6.exe	Location D:\Veritest Installers\mspm-bot\	161
		16 F This pane displays any files selected in the left-hand pane (the File List
		16 F This pane displays any files selected in the left-hand pane (the File List wiew). If you are searching by
		16 F This pane displays any files selected in the left-hand pane (the File List view). If you are searching by Conterts then this pane also
		16 F This pane displays any files selected in the left-hand pane (the File List wiew). If you are searching by
		16 H This pane displays any files selected in the left-hand pane (the File List view). If you are searching by Contents then this pane also displays lines found within the
		16 H This pane displays any files selected in the left-hand pane (the File List view). If you are searching by Contents then this pane also displays lines found within the
		16 H This pane displays any files selected in the left-hand pane (the File List view). If you are searching by Contents then this pane also displays lines found within the
		16 H This pane displays any files selected in the left-hand pane (the File List view). If you are searching by Contents then this pane also displays lines found within the

Figure 8

The last example is s	plit.exe left in C:\Windows\sv	ystem32, see Figures 9 and 10.

Mcafee - Added Files.txt - Notepad					_ 🗆 ×
File Edit Format View Help					
C:\Program Files\PC Activity Monitor Standard\ C:\Program Files\PC Activity Monitor Standard\				12/25/2004 10/25/2004	8:07:06 AM
C:\Program Files\PC Activity Monitor Standard\ C:\Program Files\PC Activity Monitor Standard\		S_IIIIO.IICIIII IKI	5 A	10/23/2004	0.19.10 AM
C:\Program Files\PC Activity Monitor Standard		1KB A	10/13/	2003 3:39:16	AM
C:\Program Files\PC Activity Monitor Standard	Templates\Users\addHeader.ht		10/13/	2003 3:39:16	AM
C:\Program Files\PC Activity Monitor Standard\				2003 3:39:16	
C:\Program Files\PC Activity Monitor Standard				2004 8:12:56	
C:\Program Files\PC Activity Monitor Standard\ C:\Program Files\PC Activity Monitor Standard\				04 12:33:36 A 2003 3:39:16	
C:\Program Files\PC Activity Monitor Standard\		3/14/2006		2005 5.55.10	
C:\WINDOWS\Prefetch\DRWTSN32.EXE-2B4B52AC.pf	105KB A 3/14/2006				
C:\WINDOWS\Prefetch\DWWIN.EXE-30875ADC.pf	217KB A 3/14/2006				
C:\WINDOWS\Prefetch\GENERIC INSTALLER UNINSTAL		3/14/2006	2:15:48 PM		
C:\WINDOWS\Prefetch\MCCONSOL.EXE-0774EF03.pf C:\WINDOWS\Prefetch\PCASTD_SETUP.EXE-130DED5C.p	21KB A 3/14/2006 of 8KB A 3/1	2:54:02 PM 14/2006 2:14:51 I	M		
C:\WINDOWS\Prefetch\RUNDLL32.EXE-2B29FBC9.pf	15KB A 3/14/2006		-141		
C:\WINDOWS\Prefetch\SYS829.EXE-10F3FC3E.pf	22KB A 3/14/2006				
C:\WINDOWS\Prefetch\V8INSTALL_SPY_SOFTWARE_4_P	ARE-39C1FDAB.pf 18KB A	3/14/2006	2:15:38 PM		
C:\WINDOWS\Prefetch\VXGAME6.EXE-03E98BC6.pf	9KB A 3/14/2006				
C:\WINDOWS\Prefetch\VXGAMET1.EXE-0853906F.pf	20KB A 3/14/2006	2:11:57 PM			
C:\WINDOWS\system32\chp.dll 46KB C:\WINDOWS\system32\chp32.dll 1KB A	3/14/2006 2:10:47 PM 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\mfc71.dll 1,061KB A	4/7/2003 10:00:00 AM				
C:\WINDOWS\system32\mfc71u.dll 1,048KB A C:\WINDOWS\system32\MSCOMCT2.OCX 648KB	4/7/2003 10:00:00 AM A 5/21/2000 5:00:00	DM			
C:\WINDOWS\System32\mscvp70.dll 488KB A	A 5/21/2000 5:00:00 1 1/4/2002 6:40:20 PM	PIM			
C:\WINDOWS\system32\Msinet.ocx 175KB A	10/1/2004 7:32:52 AM				
C:\WINDOWS\system32\msvci70.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 C:\WINDOWS\system32\Pingx.ocx 133KB A	10/1/2004 7:33:00 AM 10/1/2004 7:33:00 AM				
C:\WINDOWS\System32\Richtx32.ocx 204KB	A 10/1/2004 7:33:00 AM	ΔΜ			
C:\WINDOWS\system32\split.exe 5KB A	3/14/2006 2:11:59 PM				
C:\WINDOWS\system32\wbem\Logs\wbemess.lo_	66KB A 3/14/2006	3:38:52 PM			
					· · · · · · · · · · · · · · · · · · ·
4					

📕 Filemo	n.LOG - Notepad		
<u>Eile E</u> dit	Format <u>V</u> iew <u>H</u> elp		
3739	2:11:59 PM	naPrdMgr.exe:1060	READ C:\Program Files\Common Files\Network Associates\Engine\SCAN.DAT SUCCESS Offset: 0 Lengt
3740	2:11:59 PM	naPrdMgr.exe:1060	READ C:\Program Files\Common Files\Network Associates\Engine\SCAN.DAT SUCCESS Offset: 253 Len
741	2:11:59 PM	naPrdMgr.exe:1060	READ C:\Program Files\Common Files\Network Associates\Engine\SCAN.DAT SUCCESS Offset: 41335 L
742	2:11:59 PM	naPrdMgr.exe:1060	READ C:\Program Files\Common Files\Network Associates\Engine\SCAN.DAT SUCCESS Offset: 0 Lengt
743	2:11:59 PM	naPrdMgr.exe:1060	READ C:\Program Files\Common Files\Network Associates\Engine\SCAN.DAT SUCCESS Offset: 253 Len
744	2:11:59 PM	naPrdMgr.exe:1060	READ C:\Program Files\Common Files\Network Associates\Engine\SCAN.DAT SUCCESS Offset: 45305 L
745	2:11:59 PM	naPrdMor.exe:1060	READ C:\Program Files\Common Files\Network Associates\Engine\SCAN.DAT SUCCESS Offset: 0 Lengt
746	2:11:59 PM	naPrdMgr.exe:1060	READ C:\Program Files\Common Files\Network Associates\Engine\SCAN.DAT SUCCESS Offset: 253 Len
747	2:11:59 PM	naPrdMor.exe:1060	READ C:\Program Files\Common Files\Network Associates\Engine\SCAN.DAT SUCCESS Offset: 49687 L
748	2:11:59 PM	naPrdMgr.exe:1060	READ C:\Program Files\Common Files\Network Associates\Engine\SCAN.DAT SUCCESS Offset: 0 Lengt
749	2:11:59 PM	naPrdMgr.exe:1060	READ C:\Program Files\Common Files\Network Associates\Engine\SCAN.DAT SUCCESS Offset: 253 Len
750	2:11:59 PM	naPrdMgr.exe:1060	READ C:\Program Files\Common Files\Network Associates\Engine\SCAN.DAT SUCCESS Offset: 53489 L
751	2:11:59 PM	naPrdMgr.exe:1060	READ C:\Program Files\Common Files\Network Associates\Engine\SCAN.DAT SUCCESS Offset: 0 Lengt
752	2:11:59 PM	naPrdMgr.exe:1060	READ C:\Program Files\Common Files\Network Associates\Engine\SCAN.DAT SUCCESS Offset: 253 Len
753	2:11:59 PM	naPrdMgr.exe:1060	READ C:\Program Files\Common Files\Network Associates\Engine\SCAN.DAT SUCCESS Offset: 57491 L
754	2:11:59 PM	naPrdMgr.exe:1060	READ C:\Program Files\Common Files\Network Associates\Engine\SCAN.DAT SUCCESS Offset: 0 Lengt
755	2:11:59 PM	naPrdMgr.exe:1060	READ C:\Program Files\Common Files\Network Associates\Engine\SCAN.DAT SUCCESS Offset: 253 Len
756	2:11:59 PM	naPrdMgr.exe:1060	READ C:\Program Files\Common Files\Network Associates\Engine\SCAN.DAT SUCCESS Offset: 61165 L
757	2:11:59 PM	naPrdMgr.exe:1060	READ C:\Program Files\Common Files\Vectorkork Associates\Engine\SCAN.DAT SUCCESS Offset: 0 Lengt
758	2:11:59 PM	naPrdMdr.exe:1060	READ C:\Program Files\Common Files\Network Associates\Engine\SCAN.DAT SUCCESS Offset: 253 Len
759	2:11:59 PM	naPrdMgr.exe:1060	READ C:\Program Files\Common Files\Network Associates\Engine\SCAN.DAT SUCCESS Offset: 64959 L
760	2:11:59 PM	naPrdMgr.exe:1060	READ C:\Program Files\Common Files\Verwork Associates\Engine\SCAN.DAT SUCCESS Offset: 0 Lengt
761	2:11:59 PM	naPrdMgr.exe:1060	READ C:\Program Files\Common Files\Network Associates\Engine\SCAN.DAT SUCCESS Offset: 0 Lengt
762	2:11:59 PM	naPrdMgr.exe:1060	READ C:\Program Files\Common Files\Network Associates\Engine\SCAN.DAT SUCCESS Offset: 235 Een
762	2:11:59 PM		READ C:\Program Files\Common Files\Network Associates\Engine\SCAN.DAT SUCCESS Offset: 02295 L
		naPrdMgr.exe:1060	
764	2:11:59 PM	naPrdMgr.exe:1060	READ C:\Program Files\Common Files\Network Associates\Engine\SCAN.DAT SUCCESS Offset: 253 Len
765	2:11:59 PM	naPrdMgr.exe:1060	READ C:\Program Files\Common Files\Network Associates\Engine\SCAN.DAT SUCCESS Offset: 72819 L
766	2:11:59 PM	vxgamet1.exe:3628	OPEN C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\1213.4516 SUCCESS Options: OpenIf Access: All
767	2:11:59 PM	vxgamet1.exe:3628	WRITE C:\DOCUME-1\ADMINI-1\LOCALS-1\Temp\1213.4516 SUCCESS Offset: 0 Length: 4081
768	2:11:59 PM	vxgamet1.exe:3628	CLOSE C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\1213.4516 SUCCESS
769	2:11:59 PM	vxgamet1.exe:3628	OPEN C:\WINDOWS\system32\split.exe NOT FOUND Options: Open Access: All
770	2:11:59 PM	vxgamet1.exe:3628	OPEN C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\1213.4516 SUCCESS Options: Open Sequential Access: All
771	2:11:59 PM	vxgamet1.exe:3628	QUERY INFORMATION C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\1213.4516 SUCCESS FileAttributeTagInforma
772	2:11:59 PM	vxgamet1.exe:3628	QUERY INFORMATION C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\1213.4516 SUCCESS Length: 4081
773	2:11:59 PM	vxgamet1.exe:3628	QUERY INFORMATION C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\1213.4516 SUCCESS Attributes: A
774	2:11:59 PM	vxgamet1.exe:3628	QUERY INFORMATION C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\1213.4516 SUCCESS FilestreamInformation
775	2:11:59 PM	vxgamet1.exe:3628	QUERY INFORMATION C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\1213.4516 SUCCESS Attributes: A
776	2:11:59 PM	vxgamet1.exe:3628	QUERY INFORMATION C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\1213.4516 SUCCESS FileEaInformation
777	2:11:59 PM	vxgamet1.exe:3628	CREATE C:\WINDOWS\system32\split.exe SUCCESS Options: OverwriteIf Sequential Access: All
		-	· ·

Figure 10

🖧 Agent Ransack - [Search1]			
<u>File E</u> dit <u>V</u> iew <u>S</u> earch <u>T</u> est <u>W</u>	indow <u>H</u> elp		X
🗅 🖻 🖬 🗞 🕨 🖌 🗉 🕌 💡			
Advanced Options			Expert User
File name: vxgamet 1.exe		<b>_</b>	Expr. Wizard
Containing text:		-	Expr. Wizard
Look in: D:\		▼ ▼ Search subfold	iers 🔲 🎦
Size (kb): More than: 0	Less than: 0		
Modified: After: 3/20/2006	Before: 3/20/2006		
J			
Name			
	Location	Sit	Contents view (printable area)
vxgamet1.exe	D:\Veritest Installers\Goldfer_SpamRelayer\	31	
		31	Contents view (printable area) This pane displays any files selected in the left-hand pane (the File List
		31	This pane displays any files selected in the left-hand pane (the File List view). If you are searching by
		31	This pane displays any files selected in the left-hand pane (the File List view). If you are searching by Contents then this pane also
		3)	This pane displays any files selected in the left-hand pane (the File List view). If you are searching by Contents then this pane also displays lines found within the
		3)	This pane displays any files selected in the left-hand pane (the File List view). If you are searching by Contents then this pane also
		3)	This pane displays any files selected in the left-hand pane (the File List view). If you are searching by Contents then this pane also displays lines found within the
		3)	This pane displays any files selected in the left-hand pane (the File List view). If you are searching by Contents then this pane also displays lines found within the
vxgamet1.exe		31	This pane displays any files selected in the left-hand pane (the File List view). If you are searching by Contents then this pane also displays lines found within the
		3)	This pane displays any files selected in the left-hand pane (the File List view). If you are searching by Contents then this pane also displays lines found within the

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.

😻 split.exe - Google Search - Mozilla Firefox		
Edit     View     Go     Bookmarks     Tools     Help		
A      A		
📄 Spy Research 🧶 SpywareInfo : · Spyw 👔 Spyware Warrior For 📕 SANS - Internet Stor		
C split.exe - Google Search		
Google Web Images Groups News Froogle Local more » split.exe Search Preferences		
Web Results 1 - 10 of about 13,100 for split.exe. (0.24 seconds)		
<u>split split a file into manageable pieces</u> SYNOPSIS. split [ -a n] [ -l n] [file [prefix]]. split -b n[ b   k   m ] [ -a n] [file [prefix]]. split [ - n] [ -a n] file [prefix] www.mkssoftware.com/docs/man1/split.1.asp - 7k - <u>Cached</u> - <u>Similar pages</u> <u>Split.exe</u> usage software by InstallAware Software Corporation and		
Free Downloads Split.exe usage. SpyLOG. catalogue. split.exe usage at Free Downloads Center. Visual Split Studio 6 · Visual Split Studio 6		
Done		

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.

