



Confidence in a connected world.



A Testing Methodology for Rootkit Removal Effectiveness

Virus Bulletin 2007

Josh Harriman

Symantec Security Response

- Quick look at some current malware testing methods
 - How these approaches will not work for rootkit testing

- Types of threats this testing will (*and will not*) cover
 - Persistent vs. Non-persistent

- Tools needed to conduct testing

- Testing method step-by-step
 - Note – To be used for testing not discovery

➤ Flat file scanning

- Basic scanning of static files

➤ On demand scanning

- Test to determine if malware can be blocked before it can get on the system properly
 - Downloaded from the web
 - Move or copy operations on static files

- Problems with this testing???
 - Files are not executed
 - Doesn't reflect real-world scenarios

- In order to fully test the detection AND removal capabilities of the product, you must execute the threats!
 - Not always an easy task
 - Takes time and resources
 - But it must be done in order to have a complete and comprehensive review of the product

- Need to monitor the system for all changes made by the threat after execution
- Tools used to capture these changes are well know and proven
 - But will they work for rootkit testing???
- You cannot and **SHOULD NOT** rely on the product under test to **TELL** you the results of their actions (detection and removal)
 - Use independent tools for proper verification

➤ User mode

- System hooking in user/application space
- Needs to perform the patching of all running applications

➤ Kernel mode

- System hooking in system/kernel space
- Depending on technique, only needs to patch one place in the system

➤ *Others – some PoC (proof-of-concept)*

- VMware based (SubVirt – Software, Blue Pill – Hardware)
- PCI – Creating a persistent rootkit in the System BIOS via ACPI

When malware meets rootkits - whitepaper



Table 2: List of malware and security risks that use rootkit techniques to hide files, processes or registry keys. In some cases it is possible to observe completely different rootkit techniques used by variants of the same family (e.g. Backdoor/Graybird). Some malware, like W32/Loxbot.A@mm, contain a modified copy of FU rootkit (msdirectx.sys) embedded in their code.

Name	Threat Category			Rootkit Characteristics				
	Worm /Virus	Backdoor /Trojan	Adware/ Spyware	DLL/IAT hooking	SDT/IDT hooking	DKOM	Use SYS driver	Use "Physical Memory"
Adware/Elitebar			X	X				
Adware/CommonName			X		X		X	
Spyware/Search			X		X		X	
Spyware/Elpowkeylogger			X		X		X	
Spyware/Apropos.C			X	X	X		X	
Backdoor/Graybird ^a		X			X		X	
Backdoor/Haxdoor ^a		X			X		X	
Backdoor/Darkmoon ^a		X			X		X	
Backdoor/Berbew ^a		X		X	X		X	
Backdoor/Ryejet ^a		X			X		X	
Trojan/Drivus		X			X		X	
PWSteal/Raidys		X			X		X	
W32/Spybot.NLX	X				X		X	
W32/Theals.A@mm	X			X				
W32/Tdiserv.A	X				X		X	
W32.Mytob.AR@mm					X		X	
W32.Loxbot.A@mm	X				X		X	
W32.Myfip.H@mm	X					X		X
W32.Fanbot.A@mm	X					X		X

a - Data refers to the threat family, not just an individual threat.

- Two types of threats to deal with but only one can be covered by this testing method
 - Persistent – Will create/drop/leave traces on the system that can survive a reboot
 - Non-persistent – Will not create/drop/leave traces on the system and will not survive a reboot.

Traces consist of file and registry changes

- Persistent threats will be covered since we can monitor the changes with our tools

➤ Tools

- Monitoring
 - Filemon/Regmon (now ProcessMonitor)
 - System modification (File/Registry) tool (e.g. Regshot)
 - GMER
 - ICESword
- Offline
 - BartPE Live Windows BootCD (Created by Bart Lagerweij)
 - Alien Registry Viewer
 - File compare/diff program (e.g. Windiff)

- Need to employ '*forensic*' type techniques during testing
 - Offline analysis of filesystem and registry

- Regular monitoring tools could *miss* most changes
 - Most tools use *Windows* API calls (which can be bypassed)
 - Some tools could be targeted by the threat and become ineffective

- Some anti-rootkit tools will work for some threats
 - Pros and Cons will be highlighted

➤ Pros

- Most are free
- Most are easy to use
- Most will find quite a few of the rootkit threats currently in the wild

➤ Cons

- Some are not as clear in their reporting as to what they find
- Quite a few are written by rootkit authors themselves
- Popular anti-rootkit tools are targeted by some rootkits

➤ Pros

- Most are free
- Most are easy to use
- Will find almost all changes made to the system

➤ Cons

- You might not find all the changes, and that is **IMPORTANT**
- Some tools are targeted and the threats will not perform all of their nefarious actions

➤ Using offline analysis – Baseline snapshot

- Boot system with BootCD
- For the filesystem...
- Create a text file with filesystem directory listings using the cmd program
 - `X:\i386\System32>dir /s /a /b /o C:\ > base.txt`
 - Use an UPPER CASE letter for the systemroot drive (e.g. C:\). This will help when using the diff program later.
 - *Obviously this doesn't have to be an UPPER CASE letter, but it must be consistent for each snapshot.*

➤ Using offline analysis – Baseline snapshot

- For the registry...
- Copy on-disk registry HIVES
 - Located here → %WINDOWS%\System32\config
 - User profile → Documents and Settings*<user>*\NTUSER.dat

Windiff issues with 'small' changes...



```
WinDiff
File Edit View Expand Options Mark Help
.test_case.txt : .files_after.txt C:\INF\Workshop\Apropos\Before\test_case.txt : C:\INF\Workshop\Apropos\After\

27620 <! c:\WINDOWS\WinSxS\Policies\x86_policy.7.0.Microsoft.Windows.CPlusPlusRuntime_6595b64
27621 <! c:\WINDOWS\WinSxS\x86_Microsoft.Tools.VisualStudio.Runtime-Libraries_6595b64144cc
27622 <! c:\WINDOWS\WinSxS\x86_Microsoft.Tools.VisualStudio.Runtime-Libraries_6595b64144cc
27623 <! c:\WINDOWS\WinSxS\x86_Microsoft.Tools.VisualStudio.Runtime-Libraries_6595b64144cc
27624 <! c:\WINDOWS\WinSxS\x86_Microsoft.Tools.VisualStudio.Runtime-Libraries_6595b64144cc
27625 <! c:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.0.0_x-w
27626 <! c:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.21
27627 <! c:\WINDOWS\WinSxS\x86_Microsoft.Windows.CPlusPlusRuntime_6595b64144ccf1df_7.0.0.0_x-
27628 <! c:\WINDOWS\WinSxS\x86_Microsoft.Windows.CPlusPlusRuntime_6595b64144ccf1df_7.0.0.0_x-
27629 <! c:\WINDOWS\WinSxS\x86_Microsoft.Windows.CPlusPlusRuntime_6595b64144ccf1df_7.0.2600.2
27630 <! c:\WINDOWS\WinSxS\x86_Microsoft.Windows.CPlusPlusRuntime_6595b64144ccf1df_7.0.2600.2
27631 <! c:\WINDOWS\WinSxS\x86_Microsoft.Windows.GdiPlus_6595b64144ccf1df_1.0.0.0_x-ww_8d353f
27632 <! c:\WINDOWS\WinSxS\x86_Microsoft.Windows.GdiPlus_6595b64144ccf1df_1.0.2600.2180_x-ww
27633 <! c:\WINDOWS\WinSxS\x86_Microsoft.Windows.Networking.Dxmrtsp_6595b64144ccf1df_5.2.2.3_x
27634 <! c:\WINDOWS\WinSxS\x86_Microsoft.Windows.Networking.RtcDll_6595b64144ccf1df_5.2.2.3_x
27635 <! c:\WINDOWS\WinSxS\x86_Microsoft.Windows.Networking.RtcRes_6595b64144ccf1df_5.2.2.3_e

|> C:\Documents and Settings\Administrator\Favorites\Links
|> C:\Documents and Settings\Administrator\Favorites\Desktop.ini
|> C:\Documents and Settings\Administrator\Favorites\MSN.com.url
|> C:\Documents and Settings\Administrator\Favorites\Radio Station Guide.url
|> C:\Documents and Settings\Administrator\Favorites\Links\Customize Links.url
|> C:\Documents and Settings\Administrator\Favorites\Links\Free Hotmail.url
|> C:\Documents and Settings\Administrator\Favorites\Links\Windows Marketplace.url
|> C:\Documents and Settings\Administrator\Favorites\Links\Windows Media.url
|> C:\Documents and Settings\Administrator\Favorites\Links\Windows.url
|> C:\Documents and Settings\Administrator\Local Settings\Application Data
|> C:\Documents and Settings\Administrator\Local Settings\History
|> C:\Documents and Settings\Administrator\Local Settings\Temp
|> C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files
```

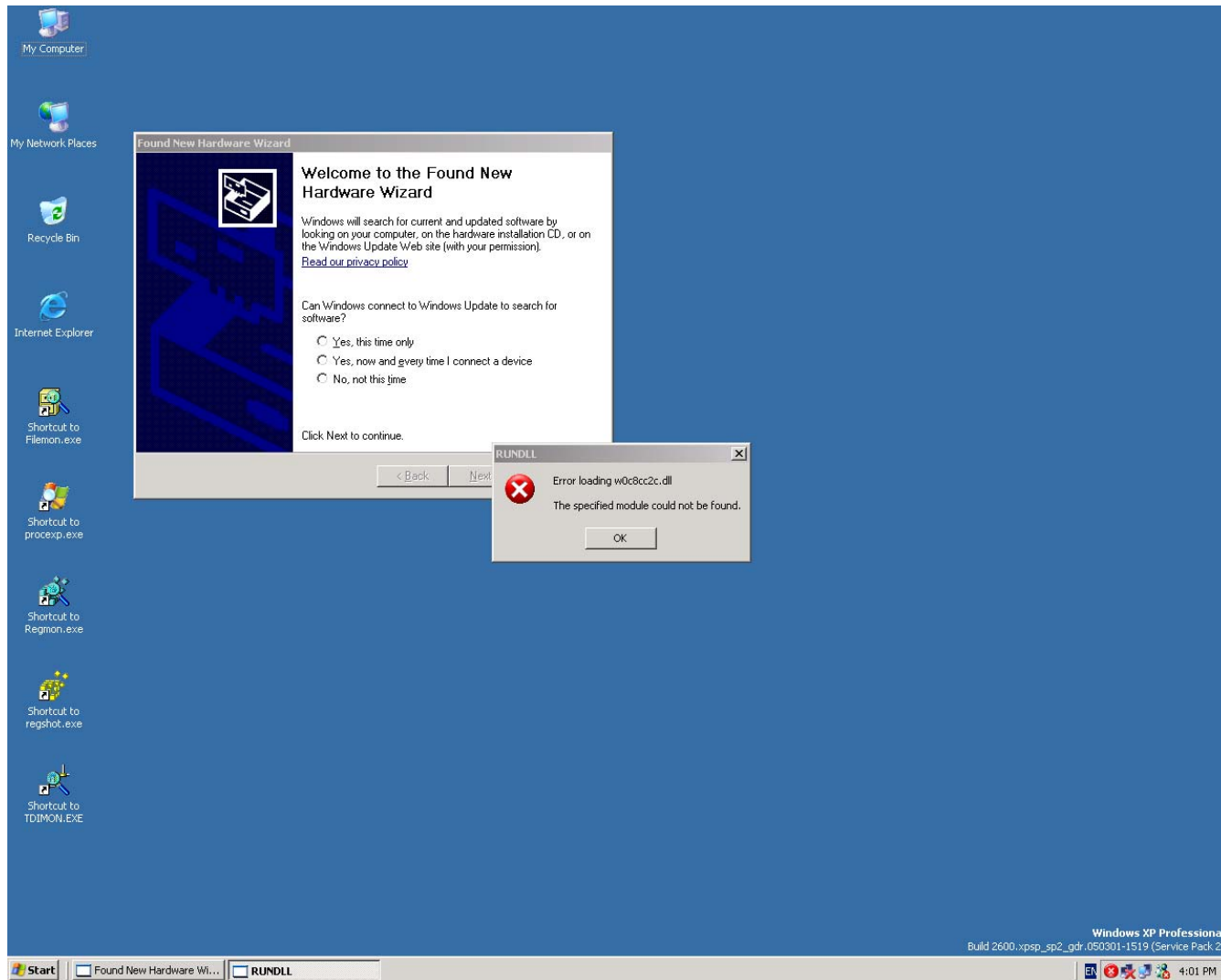
➤ Using offline analysis – Infection snapshot

- Boot system back to normal state
- Execute rootkit sample(s)
- Restart system and boot up again with BootCD
- Create a text file with filesystem listings
 - `X:\i386\System32>dir /s /a /b /o C:\ > infect.txt`
- Copy on-disk registry HIVES
 - `%WINDOWS%\System32\config`
 - `Documents and Settings\<user>\NTUSER.dat`

➤ Using offline analysis

- Boot system back to normal state
- Run a FULL system scan with the product under test
- Record results from the product
- Note any issues with the test system during/after scan

Watch for system errors (from threat or product)



➤ Using offline analysis – Cleaned snapshot

- Boot system with BootCD
- Create a text file with filesystem listings
 - `X:\i386\System32>dir /s /a /b /o C:\ > clean.txt`
- Copy on-disk registry HIVES
 - `%WINDOWS%\System32\config`
 - `Documents and Settings\<user>\NTUSER.dat`

➤ Using offline analysis

- Use ARV (Alien Registry Viewer – or similar) to export each registry image gathered during testing
 - Base image
 - Infected image
 - Cleaned image

➤ Using offline analysis

- Run file compare/diff program on exported registry HIVES and filesytem directory listings.
 - Base vs. Infected listings for 'what was added by the threat'
 - Infected vs. Clean listings for 'what was removed by the product'

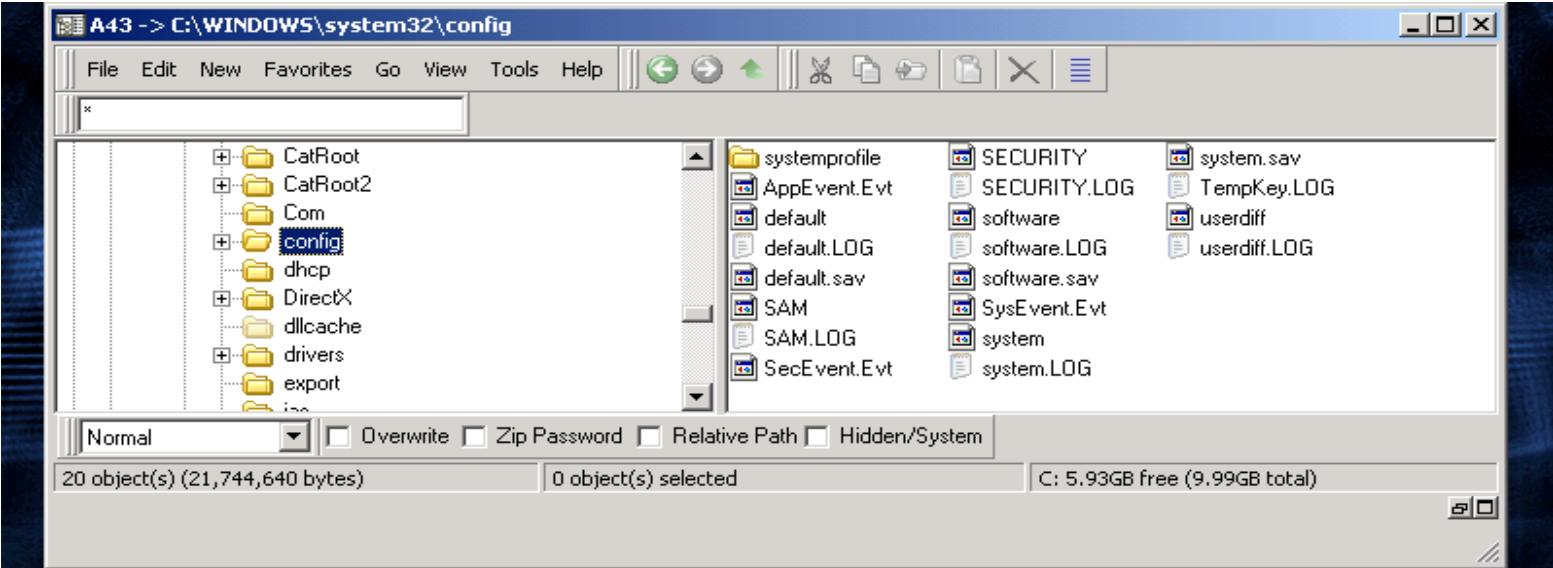
➤ Reporting the results

- Why we need all the traces/changes
- Can be broken into buckets for reporting percentages
 - Critical files and registry keys/values
 - Non-critical files/registry
- Was rootkit scanning on by default – good one to note for consumers

➤ Reporting the results

- Higher percentages don't always mean a better score
 - Product A removed 80% of the traces but missed critical files
 - Product B removed 70% of the traces but only missed non-critical files

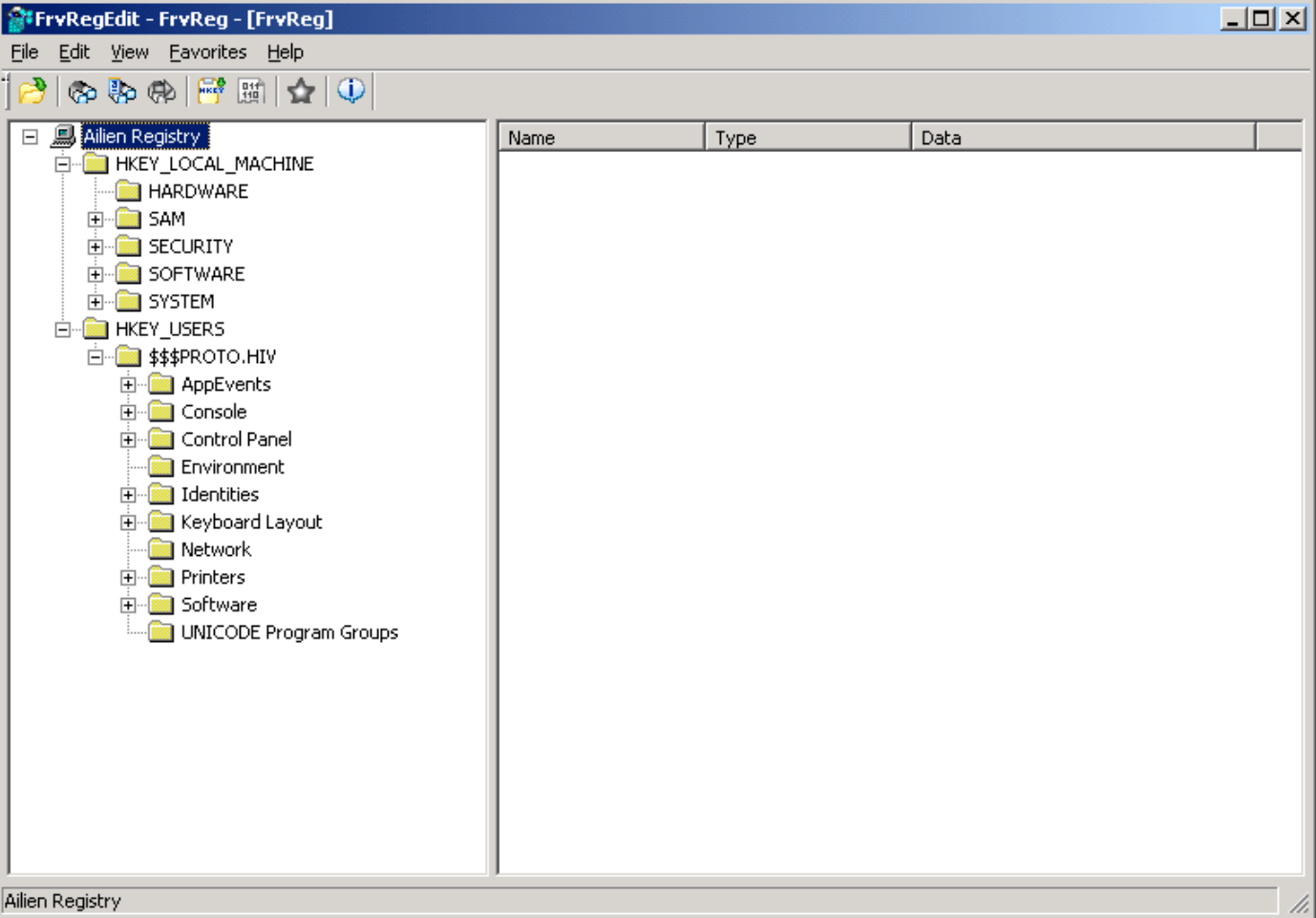
Example with Spyware.Apropos.C



created with PE-Builder



Example with Spyware.Apropos.C



Example with Spyware.Apropos.C



```
WinDiff
File Edit View Expand Options Mark Help
.\clean_files_before.txt : .\files_after.txt C:\INF\Workshop\Apropos\Before\clean_files_before.txt : C:\INF\Workshop\Apropos
Outline
13292 C:\Program Files\Common Files\System\Ole DB\resources\1033\MSOLAP80.RLL
13293 C:\Program Files\Common Files\System\Ole DB\resources\1033\OLAPUIR.RLL
13294 C:\Program Files\HangRep\HANGREP.EXE
13295 C:\Program Files\InstallShield Installation Information\{6BE2A4A4-99FB-48ED-AE1E-4}
13296 C:\Program Files\InstallShield Installation Information\{6BE2A4A4-99FB-48ED-AE1E-4}
13297 C:\Program Files\InstallShield Installation Information\{6BE2A4A4-99FB-48ED-AE1E-4}
!> C:\Program Files\Insworks\Cache
!> C:\Program Files\Insworks\ace.dll
!> C:\Program Files\Insworks\AI_06-12-2006.log
!> C:\Program Files\Insworks\cmuleacc.exe
!> C:\Program Files\Insworks\data.bin
!> C:\Program Files\Insworks\exetgsvc.exe
!> C:\Program Files\Insworks\WinGenerics.dll
13298 C:\Program Files\Internet Explorer\Connection Wizard
13299 C:\Program Files\Internet Explorer\PLUGINS
13300 C:\Program Files\Internet Explorer\SIGNUP
13301 C:\Program Files\Internet Explorer\HMMAPI.DLL
13302 C:\Program Files\Internet Explorer\iedw.exe
13303 C:\Program Files\Internet Explorer\IEXPLORE.EXE
13304 C:\Program Files\Internet Explorer\Connection Wizard\icwconn.dll
13305 C:\Program Files\Internet Explorer\Connection Wizard\icwconn1.exe
13306 C:\Program Files\Internet Explorer\Connection Wizard\icwconn2.exe
13307 C:\Program Files\Internet Explorer\Connection Wizard\icwdl.dll
13308 C:\Program Files\Internet Explorer\Connection Wizard\icwhelp.dll
13309 C:\Program Files\Internet Explorer\Connection Wizard\icwip.dun
13310 C:\Program Files\Internet Explorer\Connection Wizard\icwres.dll
13311 C:\Program Files\Internet Explorer\Connection Wizard\icwrmind.exe
13312 C:\Program Files\Internet Explorer\Connection Wizard\icwtutor.exe
13313 C:\Program Files\Internet Explorer\Connection Wizard\icwutil.dll
13314 C:\Program Files\Internet Explorer\Connection Wizard\icw25a.dun
```

Example with Spyware.Apropos.C



The screenshot displays a Windows XP desktop environment. In the background, a window titled 'wincff' shows a list of files and folders. The foreground features a Notepad window titled 'WcwChangeReport.txt - Notepad' containing the following text:

```
-----  
Change Report for ODAY-XP (FILE SYSTEM)  
Change Id-5 taken on wed Dec 06 13:36:37 2006 AND change Id-4 taken on wed Dec 06 01:01:26 2006  
Change Id-5 label wed Dec 06 13:36:37 2006 AND change Id-4 Label AS: wed Dec 06 01:01:26 2006  
-----
```

A 'Find' dialog box is open over the Notepad window, with 'Insworks' entered in the 'Find what:' field. The 'Direction' is set to 'Down'. Below the dialog box, the Notepad window shows file details for 'C:\Documents and Settings\Administrator\Local Settings\Temp\vmwareDn\00000f00' and several prefetch files:

```
****  
C:\Documents and Settings\Administrator\Local Settings\Temp\vmwareDn\00000f00  
File size: 16384 (Bytes)  
Creation time: 6/12/2006 (13:31:31)  
Last write time: 6/12/2006 (13:31:31)  
File Version: -  
C:\WINDOWS\Prefetch\4NT.EXE-01BA63DC.pf  
File size: 17254 (Bytes) -  
Creation time: 6/12/2006 (13:35:33) -  
Last write time: 6/12/2006 (13:35:33) -  
File Version: -  
C:\WINDOWS\Prefetch\APROPOS_C.EXE-1A9DFCE0.pf  
File size: 15570 (Bytes) -  
Creation time: 6/12/2006 (13:35:9) -  
Last write time: 6/12/2006 (13:35:9) -  
File Version: -  
C:\WINDOWS\Prefetch\CMULEACC.EXE-07120C17.pf  
File size: 16556 (Bytes) -  
Creation time: 6/12/2006 (13:35:19) -  
Last write time: 6/12/2006 (13:35:19) -  
File Version: -
```

A small error dialog box titled 'Cannot find "Insworks"' is also visible, with an 'OK' button.

Example with Spyware.Apropos.C



The screenshot shows a Notepad window titled "WcwChangeReport.txt - Notepad" displaying a registry change report. The report includes file information for "C:\pagefile.sys" and a summary of registry changes for "ODAY-XP (REGISTRY)". A "Find" dialog box is open over the report, with "CviP2A" entered in the "Find what:" field. The "Match case" checkbox is unchecked, and the "Direction" is set to "Down".

File Information:

Creation time:	4/9/2006 (15:1:17)	4/9/2006 (15:1:17)
Last write time:	6/12/2006 (13:35:9)	18/9/2006 (17:26:16)
File Version:	-	-

C:\pagefile.sys

File size:	805306368 (Bytes)	805306368 (Bytes)
Creation time:	4/9/2006 (15:1:16)	4/9/2006 (15:1:16)
Last write time:	6/12/2006 (13:31:16)	4/12/2006 (13:52:15)
File Version:	-	-

Change Report for ODAY-XP (REGISTRY)
Change Id-5 taken on wed Dec 06 13:36:37 2006 AND change Id-4 taken on wed Dec 06 01:01:26 2006
Change Id-5 label wed Dec 06 13:36:37 2006 AND Change Id-4 label AS: wed Dec 06 01:01:26 2006

Number of Registry Items added : 195
Number of Registry Items deleted : 116
Number of Registry Items changed : 127

*****Registry Items Added*****

Registry\HKEY_LOCAL_MACHINE\SOFTWARE\Classes\aspfile\PersistentHandler
New Data: {eec97550-47a9-11cf-b952-00aa0051fe20}
Old Data: -

ADDED KEY Registry\HKEY_LOCAL_MACHINE\SOFTWARE\Classes\aspfile\PersistentHandler

Registry\HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{0482E074-C5B7-101A-82E0-08002B36A333}\PersistentHandler\
New Data: {098f2470-bae0-11cd-b579-08002b30bfeb}
Old Data: -

ADDED KEY Registry\HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{0482E074-C5B7-101A-82E0-08002B36A333}\PersistentHandler

Registry\HKEY_LOCAL_MACHINE\SOFTWARE\Classes\msgfile\PersistentHandler\
New Data: {098f2470-bae0-11cd-b579-08002b30bfeb}
Old Data: -

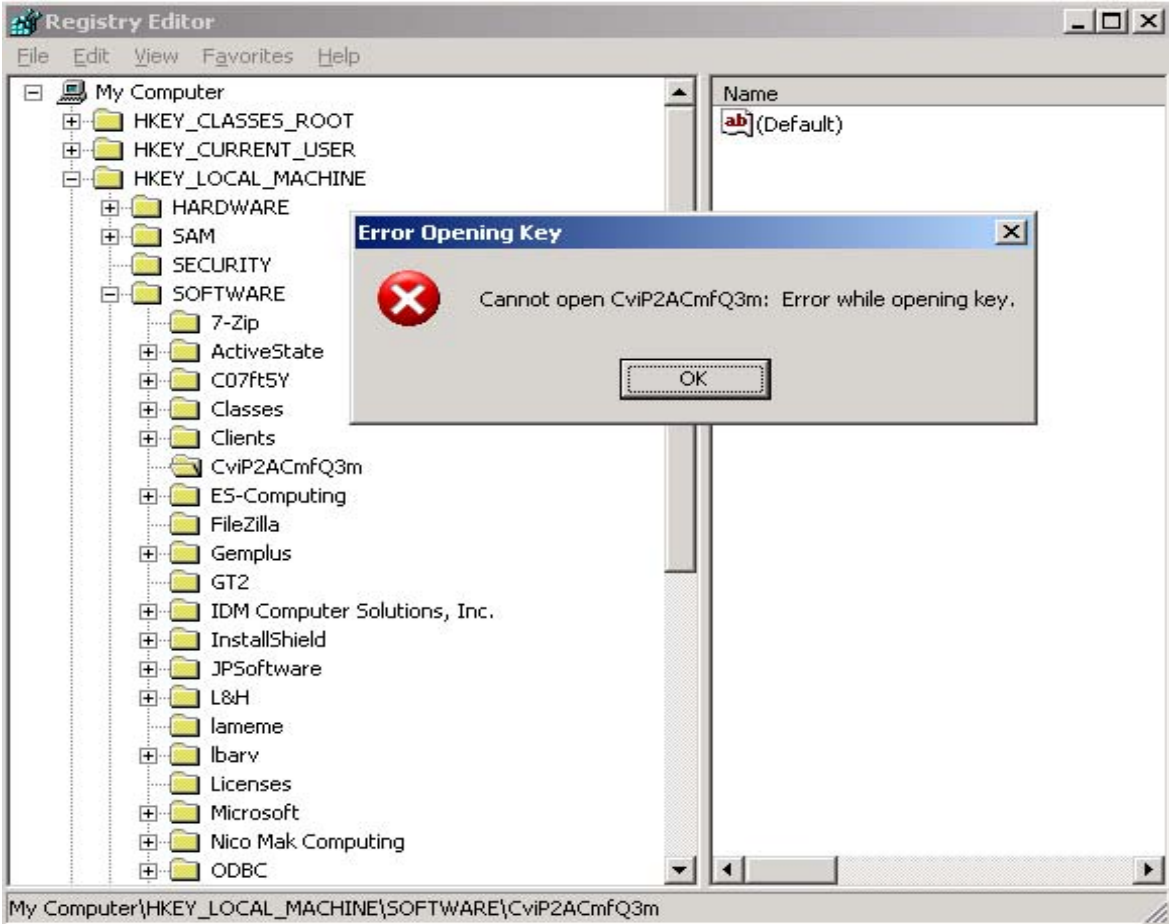
ADDED KEY Registry\HKEY_LOCAL_MACHINE\SOFTWARE\Classes\msgfile\PersistentHandler

ADDED KEY Registry\HKEY_LOCAL_MACHINE\SOFTWARE\CviP2AcmfQ3m

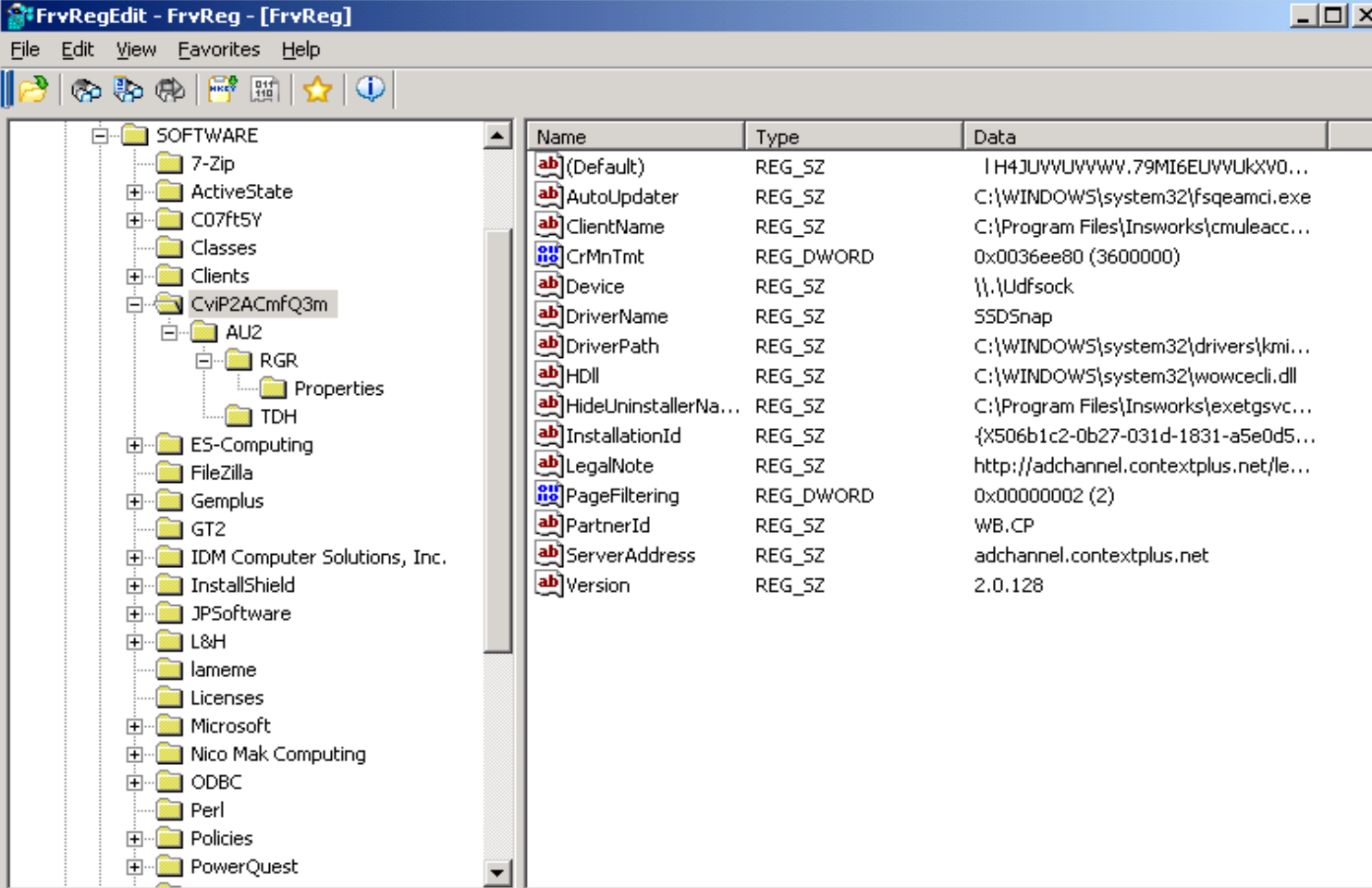
Registry\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\EventSystem\{26c409cc-ae86-11d1-b616-00805fc79216}\Subscriptions\{14661AE2-610E-4
New Data: 1
Old Data: -

Registry\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\EventSystem\{26c409cc-ae86-11d1-b616-00805fc79216}\Subscriptions\{14661AE2-610E-4

Example with Spyware.Apropos.C



Example with Spyware.Apropos.C



FrvRegEdit - FrvReg - [FrvReg]

File Edit View Favorites Help

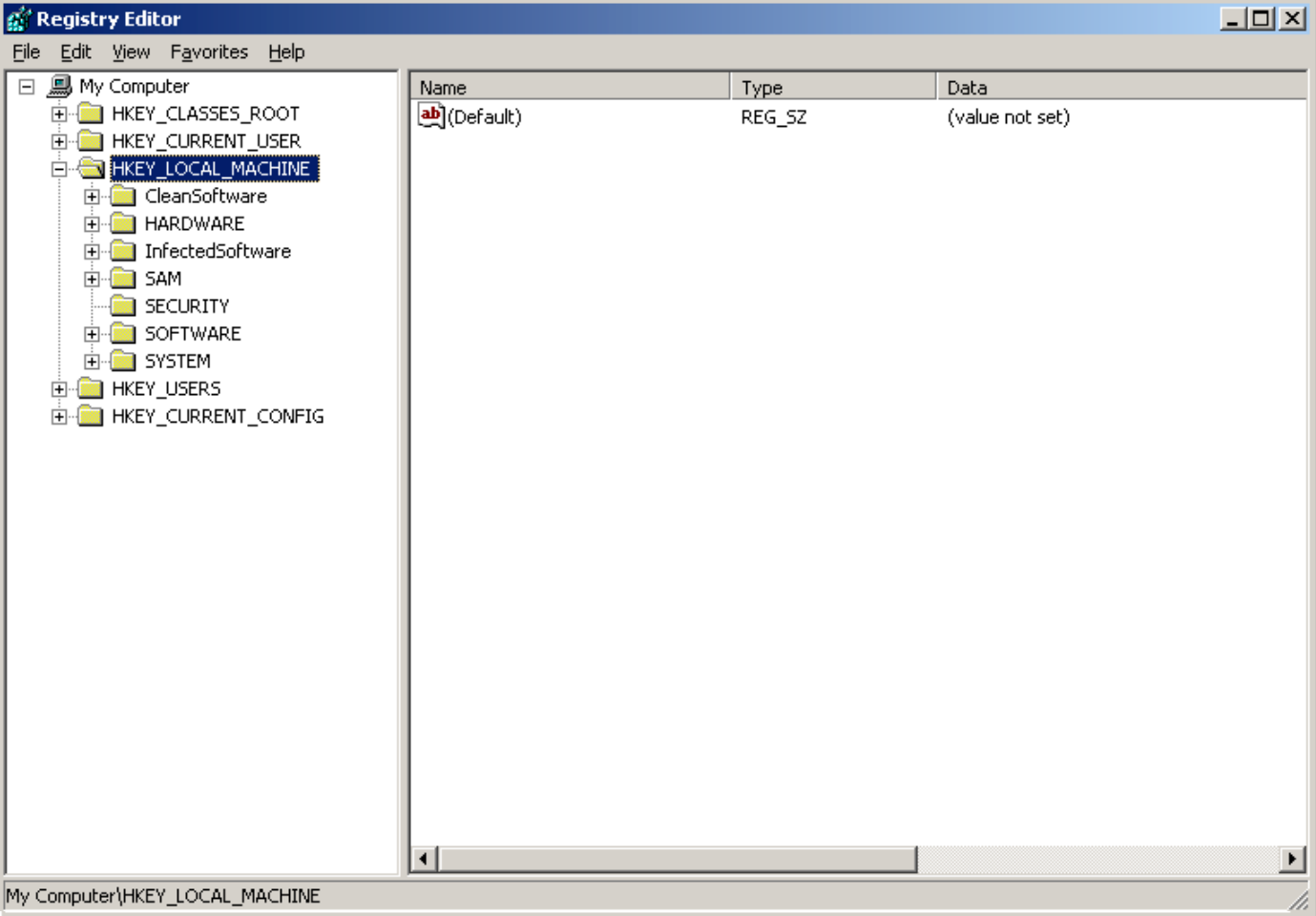
SOFTWARE

- 7-Zip
- ActiveState
- C07ft5Y
- Classes
- Clients
- CviP2ACmfQ3m
 - AU2
 - RGR
 - Properties
 - TDH
- ES-Computing
- FileZilla
- Gemplus
- GT2
- IDM Computer Solutions, Inc.
- InstallShield
- JPSoftware
- L&H
- lameme
- Licenses
- Microsoft
- Nico Mak Computing
- ODBC
- Perl
- Policies
- PowerQuest

Name	Type	Data
(Default)	REG_SZ	I H4JUUVUUVWV.79MI6EUUVUkXV0...
AutoUpdater	REG_SZ	C:\WINDOWS\system32\fsqeamci.exe
ClientName	REG_SZ	C:\Program Files\Insworks\cmuleacc...
CrMnTmt	REG_DWORD	0x0036ee80 (3600000)
Device	REG_SZ	\\.\Udfsock
DriverName	REG_SZ	SSDSnap
DriverPath	REG_SZ	C:\WINDOWS\system32\drivers\kmi...
HDll	REG_SZ	C:\WINDOWS\system32\wowcecli.dll
HideUninstallerNa...	REG_SZ	C:\Program Files\Insworks\exetgsvc...
InstallationId	REG_SZ	{X506b1c2-0b27-031d-1831-a5e0d5...
LegalNote	REG_SZ	http://adchannel.contextplus.net/le...
PageFiltering	REG_DWORD	0x00000002 (2)
PartnerId	REG_SZ	WB.CP
ServerAddress	REG_SZ	adchannel.contextplus.net
Version	REG_SZ	2.0.128

Aliens Registry\HKEY_LOCAL_MACHINE\SOFTWARE\CviP2ACmfQ3m (01-01-1970)

Using Regedit to load offline HIVES



Using Regedit to load offline HIVES



```
WinDiff
File Edit View Expand Options Mark Help
.\cleansoftware.reg : .\infectedsoftware.reg C:\INF\CleanSoftware.reg : C:\INF\InfectedSoftware.reg Outline
17340 @=""C:\Program Files\Internet Explorer\iexplore.exe""
17341
|> [HKEY_LOCAL_MACHINE\SOFTWARE\CviP2ACmFQ3m]
|> @="" I H4JUUVUUUUWU.79MI6EUUVUUKXU0qv1w0 VMSMN8GbaU7LCP8LMVEGCHNGALWMSM""
|> "Device"=""\\\\.\\Udfsock""
|> "DriverPath"=""C:\\WINDOWS\\system32\\drivers\\kmintmgr.sys""
|> "DriverName"=""SSDSnap""
|> "HideUninstallerName"=""C:\\Program Files\\Insworks\\exetgsvc.exe""
|> "HD11"=""C:\\WINDOWS\\system32\\wowcecli.dll""
|> "ServerAddress"=""adchannel.contextplus.net""
|> "LegalNote"=""http://adchannel.contextplus.net/legal-note/nonbranded.html""
|> "PartnerId"=""WB.CP""
|> "InstallationId"=""{X506b1c2-0b27-031d-1831-a5e0d582d5fa}""
|> "PageFiltering"=dword:00000002
|> "CrMnTnt"=dword:0036ee80
|> "ClientName"=""C:\\Program Files\\Insworks\\cmuleacc.exe""
|> "AutoUpdater"=""C:\\WINDOWS\\system32\\fsqeamci.exe""
|> "Version"=""2.0.128""
|>
|> [HKEY_LOCAL_MACHINE\SOFTWARE\CviP2ACmFQ3m\AU2]
|> "AP"=""/DUNM=""\\\\.\\Udfsock"" /INSC=""AU""""
|> "SU"=""http://au.contextplus.net/services/AUserver""
|> "NPT"=""2006:12:07-12:35:10:578""
|> @=""2006:12:06-13:35:10:640""
|>
|> [HKEY_LOCAL_MACHINE\SOFTWARE\CviP2ACmFQ3m\AU2\RGR]
|>
|> [HKEY_LOCAL_MACHINE\SOFTWARE\CviP2ACmFQ3m\AU2\RGR\Properties]
|> "CP.cv"=hex:43,50,2e,63,76,00,32,2e,30,2e,31,32,38,00,31,36,30,31,3a,30,31,3a,\
|> 30,31,2d,30,30,3a,30,30,3a,30,30,3a,30,30,30,00,00
|> "CP.id"=hex:43,50,2e,69,64,00,7b,58,35,30,36,62,31,63,32,2d,30,62,32,37,2d,30,\
|> 33,31,64,2d,31,38,33,31,2d,61,35,65,30,64,35,38,32,64,35,66,61,7d,00,31,36,\
|> 30,31,3a,30,31,3a,30,31,2d,30,30,3a,30,30,3a,30,30,3a,30,30,30,00,00
```


➤ Downside....

- You will need to load 'each' HIVE (software, security, etc...) and export each one separately as a .reg file. Then run windiff on each (base vs. infected vs. cleaned)
- They could each be +/- 20MB in size
- When using ARV and you export 'all' of the HIVES as one .reg file, the size is roughly 2MB

Example with Trojan.Ascesso



```
WinDiff
File Edit View Expand Options Mark Help
.\files_clean.txt : .\files_after.txt C:\TEMP\Ascesso\before\files_clean.txt : C:\TEMP\Ascesso\new\files_after.txt
19515 C:\WINDOWS\River Sumida.bmp
19516 C:\WINDOWS\Santa Fe Stucco.bmp
19517 C:\WINDOWS\SchedLgU.Txt
19518 C:\WINDOWS\sessmgr.setup.log
19519 C:\WINDOWS\SET3.tmp
19520 C:\WINDOWS\SET4.tmp
19521 C:\WINDOWS\SET8.tmp
19522 C:\WINDOWS\setupact.log
19523 C:\WINDOWS\setupapi.log
19524 C:\WINDOWS\setuperr.log
19525 C:\WINDOWS\setuplog.txt
!> C:\WINDOWS\smsys.dat
19526 C:\WINDOWS\Soap Bubbles.bmp
19527 C:\WINDOWS\Sti_Trace.log
19528 C:\WINDOWS\system.ini
19529 C:\WINDOWS\tabletoc.log
19530 C:\WINDOWS\TASKMAN.EXE
19531 C:\WINDOWS\tsoc.log
19532 C:\WINDOWS\twain.dll
19533 C:\WINDOWS\twain_32.dll
19534 C:\WINDOWS\twunk_16.exe
19535 C:\WINDOWS\twunk_32.exe
19536 C:\WINDOWS\UC.PIF
19537 C:\WINDOWS\vb.ini
19538 C:\WINDOWS\vbaddin.ini
19539 C:\WINDOWS\vmreg32.dll
19540 C:\WINDOWS\wiadebug.log
19541 C:\WINDOWS\wiasercv.log
19542 C:\WINDOWS\win.ini
19543 C:\WINDOWS\WindowsShell.Manifest
19544 C:\WINDOWS\WindowsUpdate.log
19545 C:\WINDOWS\winhelp.exe
```

Example with Trojan.Acesso



filemon.txt - Notepad

File Edit Format View Help

Summary of written/modified files:

File	PID	Process name
C:	3340	(sym1csvc.exe)
C:\\$Directory	3340	(sym1csvc.exe)
C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\Perflib_Perfdata_95c.dat	3340	(sym1csvc.exe)
C:\DOCUME~1\ALLUSE~1\APPLIC~1\Symantec\SPBBC\BBNotify.log	1560	(ccsvchst.exe)
C:\DOCUME~1\ALLUSE~1\APPLIC~1\Symantec\SPBBC\SPPolicy.log	1560	(ccsvchst.exe)
C:\INSTALLED\WCW\NAV07_VM\wcSystem.bak	1260	(wcwService.exe)
C:\INSTALLED\WCW\NAV07_VM\wcSystem.wc	1260	(wcwService.exe)
C:\INSTALLED\WCW\NAV07_VM\wcw.bak	1260	(wcwService.exe)
C:\INSTALLED\WCW\NAV07_VM\wcw.ini	1260	(wcwService.exe)
C:\INSTALLED\WCW\NAV07_VM\wcw.tmp	1260	(wcwService.exe)
C:\INSTALLED\WCW\NAV07_VM\wcfscatindex.bak	1260	(wcwService.exe)
C:\INSTALLED\WCW\NAV07_VM\wcfscatindex.wcw	1260	(wcwService.exe)
C:\INSTALLED\WCW\NAV07_VM\wcfssnap.bak	1260	(wcwService.exe)
C:\INSTALLED\WCW\NAV07_VM\wcfssnap.wcw	1260	(wcwService.exe)
C:\INSTALLED\WCW\NAV07_VM\wcregcatindex.bak	1260	(wcwService.exe)
C:\INSTALLED\WCW\NAV07_VM\wcregcatindex.wcw	1260	(wcwService.exe)
C:\INSTALLED\WCW\NAV07_VM\wcregsnap.bak	1260	(wcwService.exe)
C:\INSTALLED\WCW\NAV07_VM\wcregsnap.wcw	1260	(wcwService.exe)
C:\INSTALLED\WCW\wcwsvlog.txt	1260	(wcwService.exe)
C:\Program Files\Common Files\Symantec Shared\CCPD-LC\sym1crst.dll	3340	(sym1csvc.exe)
C:\Program Files\Common Files\Symantec Shared\SNDFW.log	1560	(ccsvchst.exe)
C:\WINDOWS\Prefetch\2.EXE-0F7AC23C.pf	1080	(svchost.exe)
C:\WINDOWS\system32\Drivers\Beep.sys	2844	(2.exe)
C:\WINDOWS\system32\Drivers\Cdaudio.sys	2844	(2.exe)
C:\WINDOWS\system32\CatRoot2\edb.chk	1080	(svchost.exe)
C:\WINDOWS\system32\CatRoot2\edb.log	1080	(svchost.exe)
C:\WINDOWS\system32\CatRoot2\tmp.edb	1080	(svchost.exe)
C:\WINDOWS\system32\CatRoot2\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\catdb	1080	(svchost.exe)
C:\WINDOWS\system32\config\software	3340	(sym1csvc.exe)
C:\WINDOWS\system32\config\software.LOG	3340	(sym1csvc.exe)
C:\WINDOWS\system32\dllcache\beep.sys	708	(winlogon.exe)
C:\WINDOWS\system32\dllcache\beep.sys.new	708	(winlogon.exe)
C:\WINDOWS\system32\dllcache\cdaudio.sys	708	(winlogon.exe)
C:\WINDOWS\system32\dllcache\cdaudio.sys.new	708	(winlogon.exe)

- Need to employ offline analysis techniques in order to capture all traces created by the threat under test
- Be aware that some monitoring tools could *miss* these traces and cannot be relied upon in all cases
- Don't rely on the product under test to dictate the final results. Use 3rd party tools to verify your findings

THANK YOU



THANK YOU FOR YOUR
TIME!

Questions???