

Privatefirewall 5.0 - Malware and Adware Use Cases

1. Introduction

Privatefirewall is a desktop defense application comprised of several distinct technology layers designed to block or mitigate the damage caused by intrusion, virus and other malware attacks. Privatefirewall includes the following layers of defense technology:

- Personal, desktop or endpoint firewall
 - o Port Manager
 - o Packet Filter
 - o URL Filter
 - o Application Control Engine
- Registry Monitor
- Process Monitor/Manager
- Email Anomaly Analyzer/Manager

Privatefirewall detects malware and intrusions based on behaviors characteristic of unauthorized system use. Some of these include:

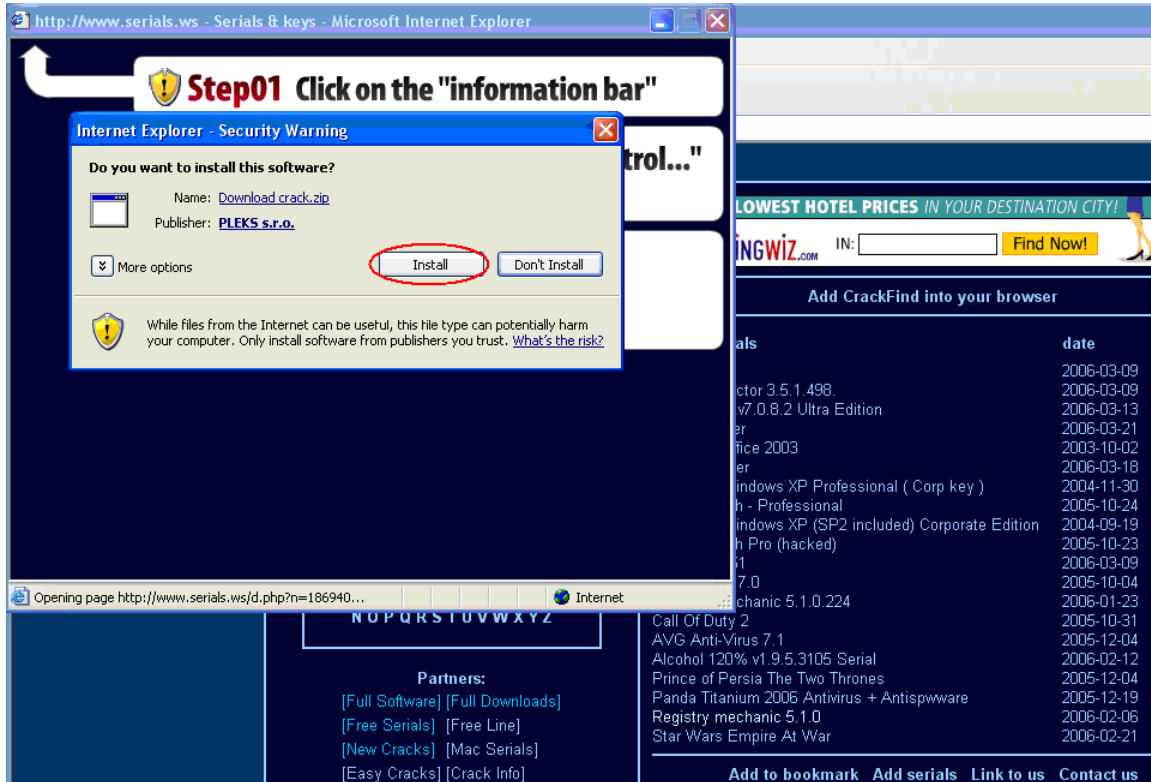
- Attempt to access a protected registry area
- Attempt to access a protected object
- Attempt to Initiate a foreign process
- Attempt to control Windows service
- Attempt to create a DNS request
- Attempt to initiate outgoing TCP traffic

Privatefirewall is available as a stand-alone application for personal and home computing and as a centrally managed offering called Endpoint Security Console. For more information, please visit www.privacyware.com.

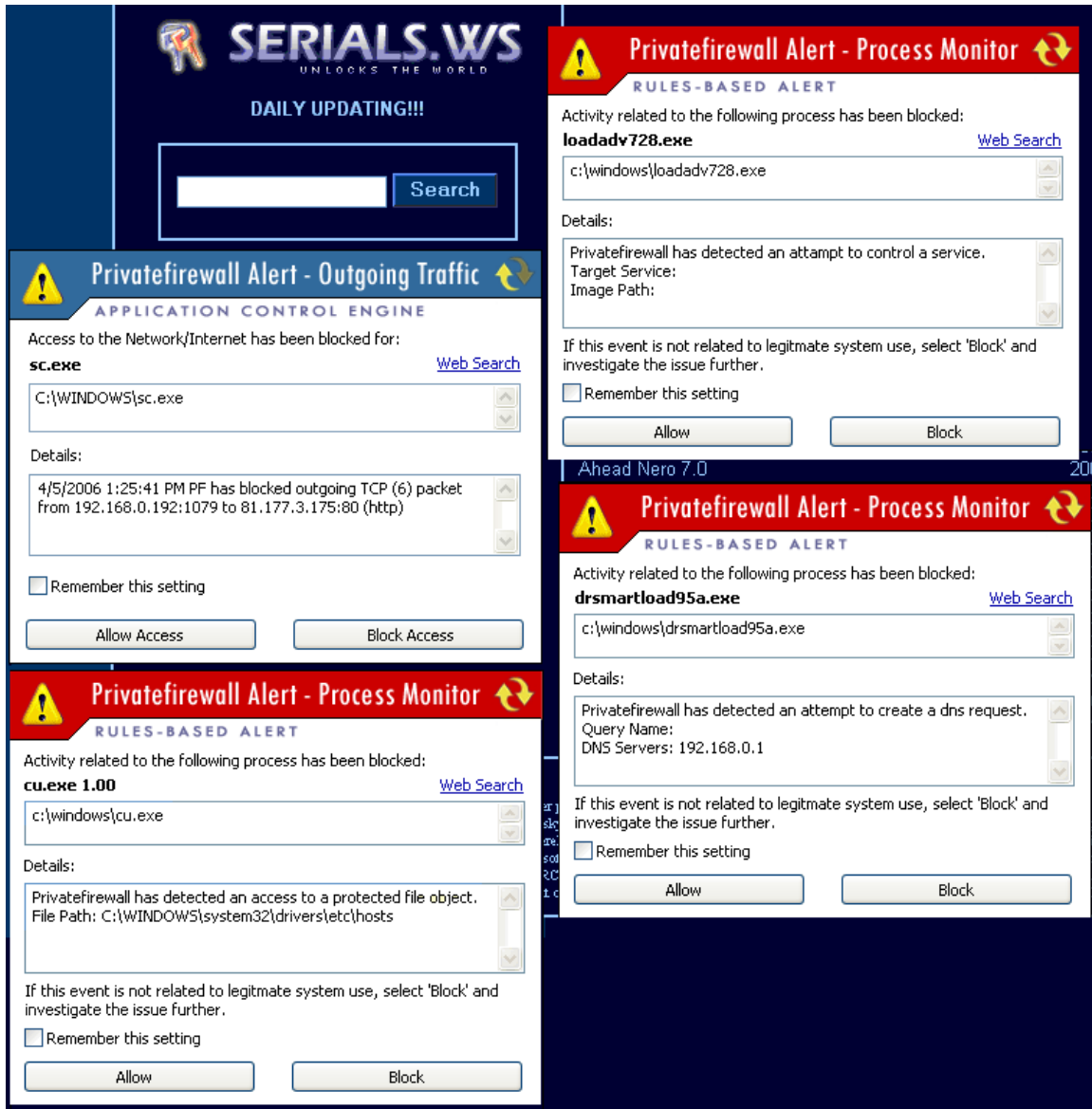
2. Case 1 – Malicious software installed as an ActiveX control

The following use case illustrates a scenario wherein a malicious file is downloaded and executed (in this case an ActiveX file). If undetected, the malware will cause system infection on several levels. i.e. rootkit, Trojan and adware.

- a. Into the browser, enter the following URL: www.serials.ws . This website can deploy the Hearse.Rootkit infection.
- b. Select the first link that claims to be a crack or keygen. The site requires installing ActiveX to enable download of the software crack.



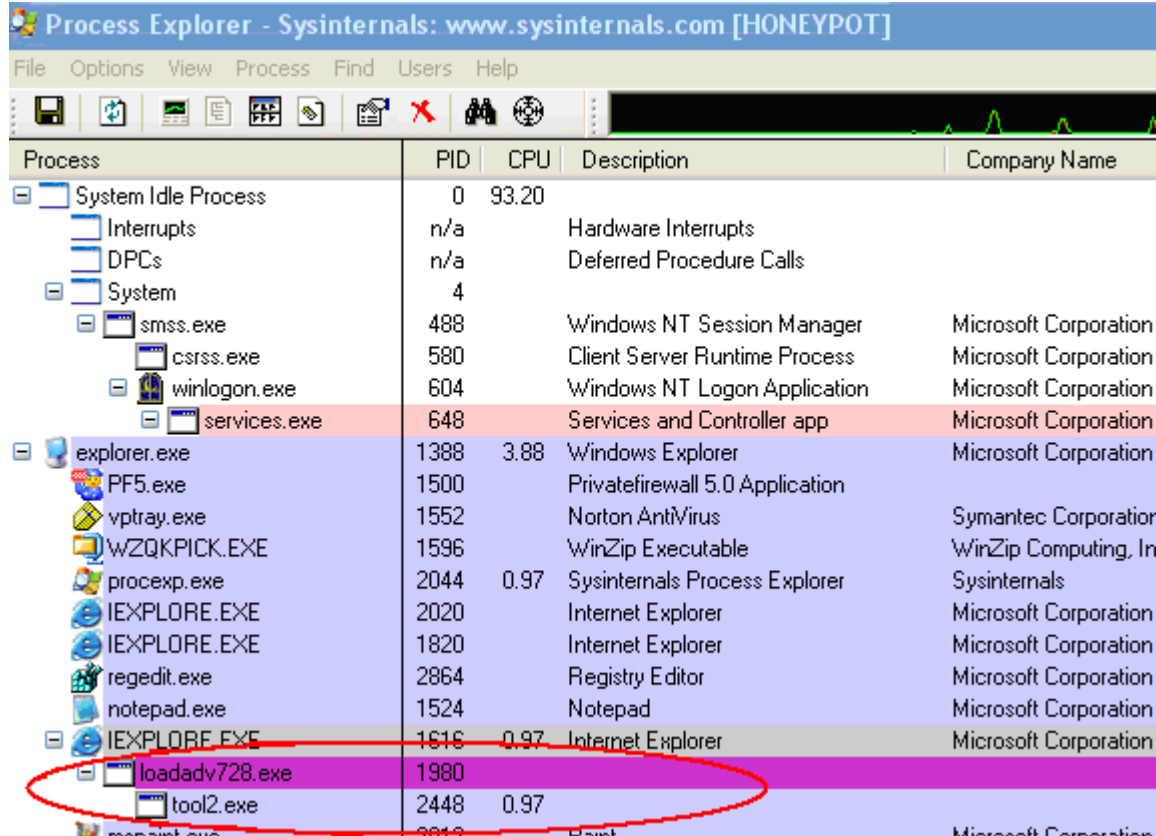
c. If the Install button is selected, Privatefirewall 5.0 immediately reacts to the unknown executable with either a Firewall or Process Monitor alert.



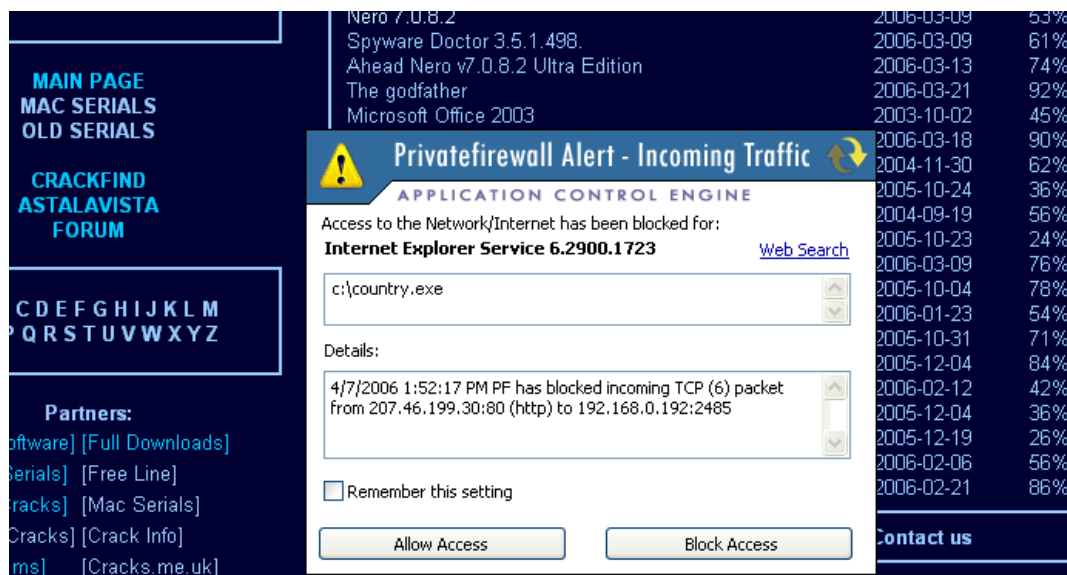
d. Regardless of alert type, the 'Block' button must be selected to prevent the malicious file from launching and to maintain system integrity.

3. If Privatefirewall was not installed and/or the installation of the malware had been allowed, the system would have been extensively infected.

a. First, the downloaded executable starts creating new processes.



b. Privatefirewall 5.0 continues to provide alerts for each unknown process.



c. Additional malicious processes are created, one of which is 'paytime.exe'.

Process	PID	CPU	Description	Company Name
System Idle Process	0	45.63		
Interrupts	n/a	0.97	Hardware Interrupts	
DPCs	n/a		Deferred Procedure Calls	
System	4	7.77		
smss.exe	488		Windows NT Session Manager	Microsoft Corporation
csrss.exe	580		Client Server Runtime Process	Microsoft Corporation
winlogon.exe	604		Windows NT Logon Application	Microsoft Corporation
services.exe	648	0.97	Services and Controller app	Microsoft Corporation
explorer.exe	1388	6.80	Windows Explorer	Microsoft Corporation
PF5.exe	1500		Privatefirewall 5.0 Application	
vptray.exe	1552		Norton AntiVirus	Symantec Corporation
WZQKPICK.EXE	1596		WinZip Executable	WinZip Computing, Inc.
procexp.exe	2044	1.94	Sysinternals Process Explorer	Sysinternals
IEXPLORE.EXE	2020		Internet Explorer	Microsoft Corporation
IEXPLORE.EXE	1820		Internet Explorer	Microsoft Corporation
regedit.exe	2864		Registry Editor	Microsoft Corporation
notepad.exe	1524		Notepad	Microsoft Corporation
IEXPLORE.EXE	1616	0.97	Internet Explorer	Microsoft Corporation
loadadv728.exe	1980			
tool2.exe	2448	2.91		
country.exe	316		Internet Explorer Service	Microsoft Corporation
iooschedule.exe	516	32.04	Internet Explorer Update Schedule	Microsoft Corporation
paytime.exe	2572	0.97	explorer	Microsoft Corporation
mspaint.exe	2012		Paint	Microsoft Corporation

Additional detail on paytime.exe:

paytime - paytime.exe - Process Information

Process File: paytime.exe
Process Name: Dialer.W32.TIBS

Description: paytime.exe is a process registered as a dialler which can use your computer's telephone line to dial high cost toll numbers without your consent or knowledge. It is a registered security risk and should be removed immediately.
[For More Info About paytime.exe - Get WinTasks 5 Pro Now!](#)

d. Privatefirewall 5.0 will generate an alert for every new executable created by malware.

Process	PID	CPU	Description	Company Name
System Idle Process	0			
Interrupts	n/a		Hardware Interrupts	
DPCs	n/a		Deferred Procedure Calls	
System	4	2.97		
smss.exe	488		Windows NT Session Manager	Microsoft Corporation
csrss.exe	580	6.93	Client Server Runtime Process	Microsoft Corporation
winlogon.exe	604		Windows NT Logon Application	Microsoft Corporation
services.exe	648	0.99	Services and Controller app	Microsoft Corporation
MSGSYS.E...	172		CBA - Message System	Intel Corporation
wdfmgr.exe	1932		Windows User Mode Driver Manager	
svchost.exe	788		Generic Host Process for Win32 Services	
svchost.exe	2600		Generic Host Process for Win32 Services	
lsass.exe	660		LSA Shell (Export Version)	
explorer.exe	1388	11.88	Windows Explorer	
PF5.exe	1500	0.99	Privatefirewall 5.0 Application	
vp trays.exe	1552		Norton AntiVirus	
WZQKPKICK.EXE	1596		WinZip Executable	
proce xp.exe	2044		Sysinternals Process Explorer	
IEXPLORE.EXE	2020		Internet Explorer	
IEXPLORE.EXE	1820		Internet Explorer	
regedit.exe	2864		Registry Editor	
notepad.exe	1524		Notepad	
IEXPLORE.EXE	1616		Internet Explorer	
mspaint.exe	2012		Paint	
tool2.exe	2448	0.99		
paytime.exe	2572		explorer	
ieschedule.exe	516		Internet Explorer Update Schedule	
rundll32.exe	2656		Run a DLL as an App	Microsoft Corporation
tool5.exe	1336			

e. Several registry keys are modified: services, windows and winlogon settings for local and current user as well as ShellServiceObjectDelayLoad for Adware AZE-bar.

Name	Type	Data
ab\{Default}	REG_SZ	
ab\Microsoft Windows Logon Process	REG_SZ	C:\WINDOWS\winlogon.exe
ab\Microsoft Windows Session Manager Subsystem	REG_SZ	C:\WINDOWS\smss.exe
ab\Privatefirewall	REG_SZ	C:\Program Files\Privacyware\Privatefirewall 5.0\PF5.exe
ab\SysTray	REG_SZ	c:\Program Files\paytime.exe
ab\vp trays	REG_SZ	C:\Program Files\NavNT\vp trays.exe

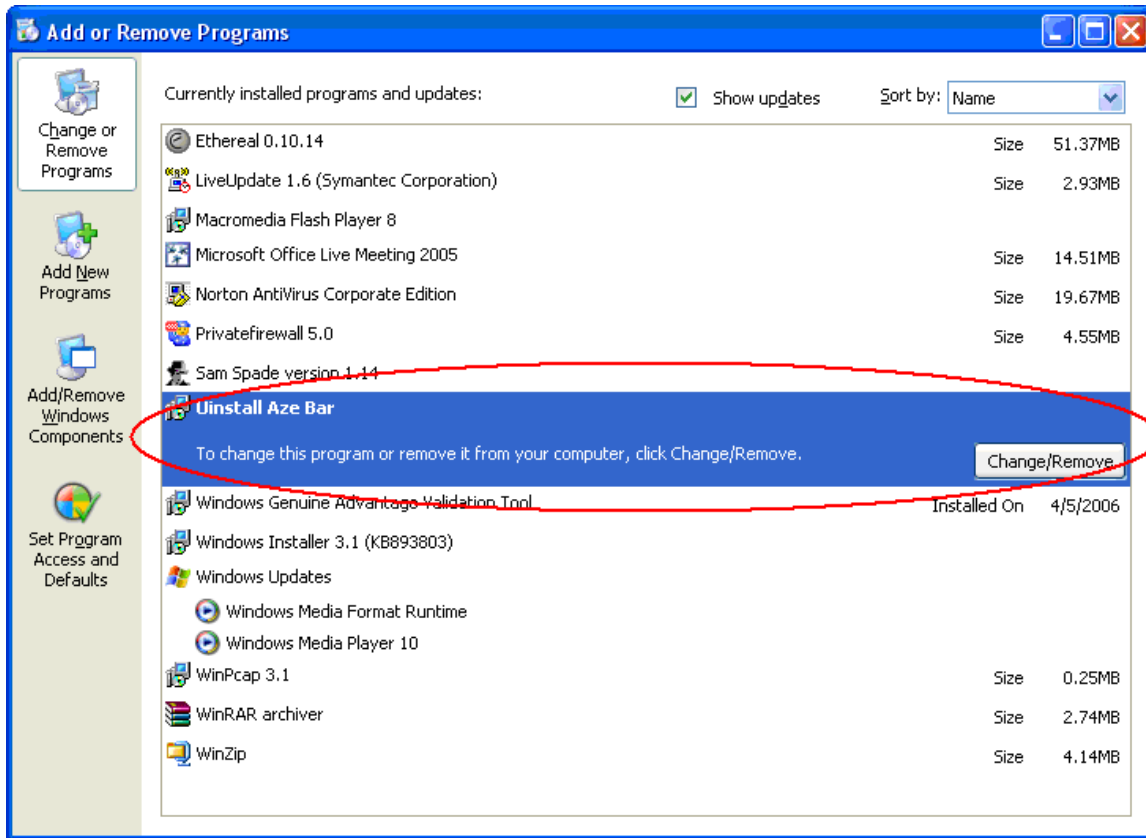
f. The winlogon shell key value was changed.

The screenshot shows the Windows Registry Editor with the following registry path selected: `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell`. The 'Shell' value is being edited to `logon Files\Common Files\Microsoft Shared\Web Folders\ibm00001.exe`.

Name	Type	Data
(Default)	REG_SZ	(value not set)
	REG_SZ	0
	REG_SZ	0
	REG_SZ	0
ssions	REG_DWORD	0x00000001 (1)
Name	REG_SZ	HONEYPOT
me	REG_SZ	
	REG_DWORD	0x00000001 (1)
	REG_SZ	0 0 0
nt	REG_SZ	10
mand	REG_SZ	no
	REG_SZ	HONEYPOT
DefaultDomainName	REG_SZ	
DefaultUserName	REG_SZ	
Forceunlocklogon	REG_DWORD	0x00000000 (0)
HibernationPreviouslyEnabled	REG_DWORD	0x00000001 (1)
LegalNoticeCaption	REG_SZ	
LegalNoticeText	REG_SZ	
LogonType	REG_DWORD	0x00000001 (1)
passwordexpirywarning	REG_DWORD	0x0000000e (14)
PowerdownAfterShutdown	REG_SZ	0
ReportBootOk	REG_SZ	1
scremoveoption	REG_SZ	0
SFCDisable	REG_DWORD	0x00000000 (0)
SfcQuota	REG_DWORD	0xffffffff (4294967295)
Shell	REG_SZ	explorer.exe
ShowLogonOptions	REG_DWORD	0x00000000 (0)
ShutdownWithoutLogon	REG_SZ	0
System	REG_SZ	
UIHost	REG_EXPAND_SZ	logonui.exe
Userinit	REG_SZ	C:\WINDOWS\system32\userinit.exe,
VmApplet	REG_SZ	rundll32 shell32,Control_RunDLL "sysdm.cpl"
WinStationsDisabled	REG_SZ	0

In the foreground, a Privatefirewall Alert - Outgoing Traffic dialog box is displayed. It indicates that access to the Network/Internet has been blocked for 'outlook wabber 5.10.0167' because it attempted to create a dns request. The details show the query name and DNS servers. The user is prompted to either 'Allow Access' or 'Block Access'.

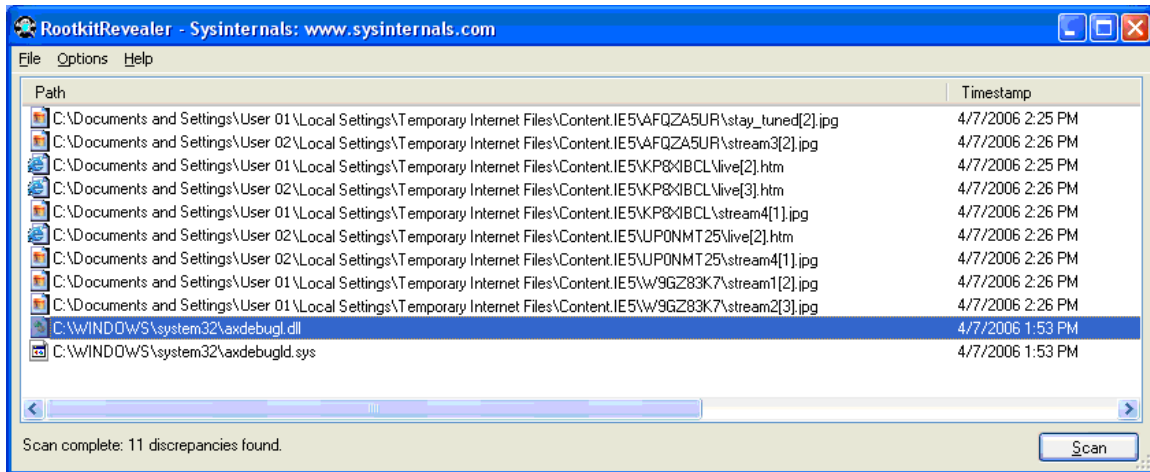
g. Aze-Bar malware was installed



h. Once completed, Symantec AntiVirus with updated definitions identified the following items:

Date	Filename	Virus Name	Virus Type	Action Taken	Computer	User	Original Location	Status
4/7/2006 2:18:45 PM	reger.exe	Trojan.Adclicker	File	Quarantined	HONEYPOT	User 01	C:\WINDOWS\system32\	Infected
4/7/2006 2:18:26 PM	ndcmgibd.dll	Trojan.Tannick.B	File	Quarantined	HONEYPOT	User 01	C:\WINDOWS\system32\	Infected
4/7/2006 2:18:08 PM	mpdgiaml.exe	Trojan.Dropper	File	Quarantined	HONEYPOT	User 02	C:\WINDOWS\system32\	Infected
4/7/2006 2:17:53 PM	ib6.dll	PWSteal.Trojan	File	Left alone	HONEYPOT	User 02	C:\WINDOWS\system32\	Infected
4/7/2006 2:14:36 PM	smss.exe	Trojan.Horse	File	Quarantined	HONEYPOT	User 01	C:\WINDOWS\	Infected
4/7/2006 2:14:35 PM	sc.exe	Download.Trojan	File	Quarantined	HONEYPOT	User 01	C:\WINDOWS\	Infected
4/7/2006 2:12:18 PM	paytime.exe	Trojan.Horse	File	Quarantined	HONEYPOT	User 02	C:\Program Files\	Infected
4/7/2006 2:11:26 PM	ibm00001.exe	Trojan.Anserin	File	Quarantined	HONEYPOT	User 01	C:\Program Files\Common Fi...	Infected
4/7/2006 2:11:19 PM	ms1.exe	Download.Trojan	File	Quarantined	HONEYPOT	User 02	C:\	Infected
4/7/2006 2:11:19 PM	kl1.exe	Trojan.Anserin	File	Quarantined	HONEYPOT	User 01	C:\	Infected
4/7/2006 2:11:11 PM	rpxsdpoa[1].txt	Trojan.Dropper	File	Quarantined	HONEYPOT	User 02	C:\Documents and Settings\...	Infected
4/7/2006 2:11:10 PM	lgkqadw[1].txt	Trojan.Horse	File	Quarantined	HONEYPOT	User 02	C:\Documents and Settings\...	Infected
4/7/2006 2:11:10 PM	ib6[1].dll	PWSteal.Trojan	File	Quarantined	HONEYPOT	User 01	C:\Documents and Settings\...	Infected
4/7/2006 2:11:04 PM	qtonlgf[1].txt	Trojan.Anserin	File	Quarantined	HONEYPOT	User 01	C:\Documents and Settings\...	Infected
4/7/2006 2:09:42 PM	qlcvfku[1].htm	Backdoor.Trojan	File	Quarantined	HONEYPOT	User 02	C:\Documents and Settings\...	Infected
4/7/2006 2:09:41 PM	install[1].htm	Download.Trojan	File	Quarantined	HONEYPOT	User 02	C:\Documents and Settings\...	Infected
4/7/2006 2:04:38 PM	wpxawgqp[1].txt	Download.Trojan	File	Quarantined	HONEYPOT	User 01	C:\Documents and Settings\...	Infected
4/7/2006 2:02:03 PM	dnlsv.exe	Download.Trojan	File	Left alone	HONEYPOT	User 02	C:\Documents and Settings\...	Infected
4/7/2006 2:01:32 PM	country.exe	Backdoor.Trojan	File	Quarantined	HONEYPOT	User 01	C:\	Infected

- i. The Rootkit Revealer showed that the computer was infected. These files were not visible from Windows Explorer and were only visible in Safe Mode.



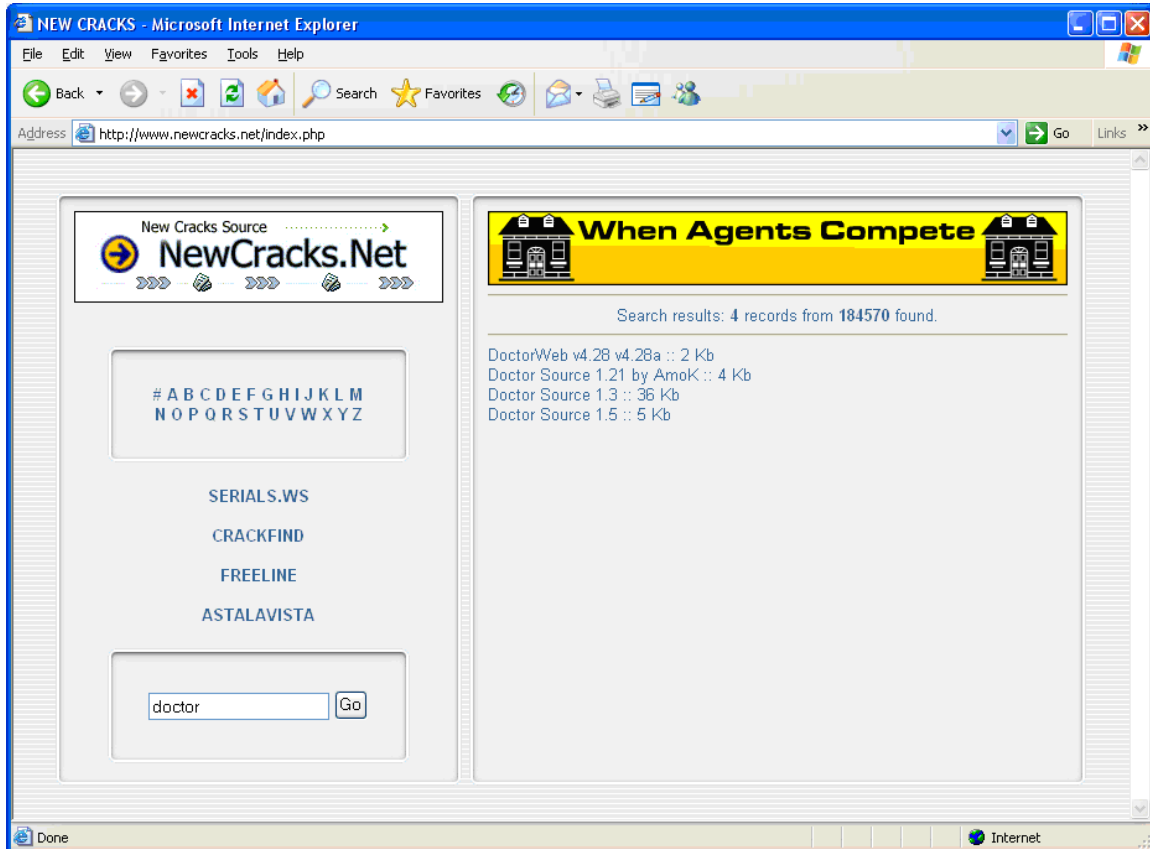
- j. The 'hosts' file was modified to block access to common security sites.



4. Case 2 – Visiting a malicious web site.

System infection via stealthy malware has become increasingly common by simply linking or surfing to a malicious site. The scenario described below illustrates a typical example of this type of infection.

- a. Navigate to www.newcracks.net or <http://foto-pompe-pompini.com> (Note: Make sure you have the latest MS patches installed, especially for the WMF exploit. The second link launches the exploit immediately!)
- b. If www.newcracks.net is used, search for 'doctor'



c. After selecting the first link in the search results (DoctorWeb v4.28), an attack is launched. As a result, the trusted process rundll32.exe creates a malicious process named 'a.exe'. Even if rundll32.exe is allowed to run, Privatefirewall 5.0 will provide an alert for the child process.

Process	PID	CPU	Description	Company Name
System Idle Process	0			
Interrupts	n/a		Hardware Interrupts	
DPCs	n/a	0.97	Deferred Procedure Calls	
System	4			
smss.exe	456		Windows NT Session Mana...	Microsoft Corporation
csrss.exe	512	0.97	Client Server Runtime Process	Microsoft Corporation
winlogon.exe	536		Windows NT Logon Applica...	Microsoft Corporation
services.exe	580	0.97	Services and Controller app	Microsoft Corporation
alg.exe	440			
svchost.exe	1588			
msiexec.exe	1576			
defwatch.exe	2444			
rtvscan.exe	2472			
MSGSYS.E...	2624			
svchost.exe	3980			
lsass.exe	592			
wpabaln.exe	1124			
explorer.exe	1268	1.94		
PF5.exe	1420	5.83		
WZQKPICK.EXE	1448			
mspaint.exe	3956			
IEXPLORE.EXE	220	82.52		
rundll32.exe	2068	0.98		
a.exe	2120			
procexp.exe	1732	5.83		
taskmgr.exe	1908			
vp trays.exe	2828			

Privatefirewall Alert - Process Monitor

RULES-BASED ALERT

Activity related to the following process has been blocked:

Run a DLL as an App 5.1.2600.2180 [Web Search](#)

c:\windows\system32\rundll32.exe

Details:

Privatefirewall has detected an attempt to create a process.
Command line: a.exe

If this event is not related to legitimate system use, select 'Block' and investigate the issue further.

Remember this setting

Allow Block

d. Even if the above process is allowed and rundll32.exe is launched, Privatefirewall 5.0 will generate another alert for the child process.

Process Explorer - Sysinternals: www.sysinternals.com [HONEYPOT]

Process	PID	CPU	Description	Company Name
System Idle Process	0	95.10		
Interrupts	n/a	0.98	Hardware Interrupts	
DPCs	n/a		Deferred Procedure Calls	
System	4			
smss.exe	456		Windows NT Session Mana...	Microsoft Corporation
csrss.exe	512		Client Server Runtime Process	Microsoft Corporation
winlogon.exe	536		Windows NT Logon Applica...	Microsoft Corporation
services.exe	580	0.98	Services and Controller app	Microsoft Corporation
svchost.exe	7			
svchost.exe	8			
svchost.exe	8			
wscntfy.exe	3			
svchost.exe	9			
svchost.exe	10			
spoolsv.exe	13			
pfsvc.exe	16			
alg.exe	4			
svchost.exe	15			
defwatch.exe	24			
rtvscan.exe	24			
MSGSYS.E...	26			
svchost.exe	39			
lsass.exe	5			
wpabaln.exe	11			
explorer.exe	12			
PF5.exe	14			
WZQKPICK.EXE	14			
taskmgr.exe	1908		Windows TaskManager	Microsoft Corporation
wptrau.exe	2828		Norton AntiVirus	Symantec Corporation
a.exe	2120			
scmt16.exe	2168			

Privatefirewall Alert - Process Monitor

RULES-BASED ALERT

Activity related to the following process has been blocked:

a.exe [Web Search](#)

c:\Documents and Settings\User 01\Local Settings\Temp\a.exe

Details:

Privatefirewall has detected an access to a protected file object.
File Path: c:\vyfnc.exe

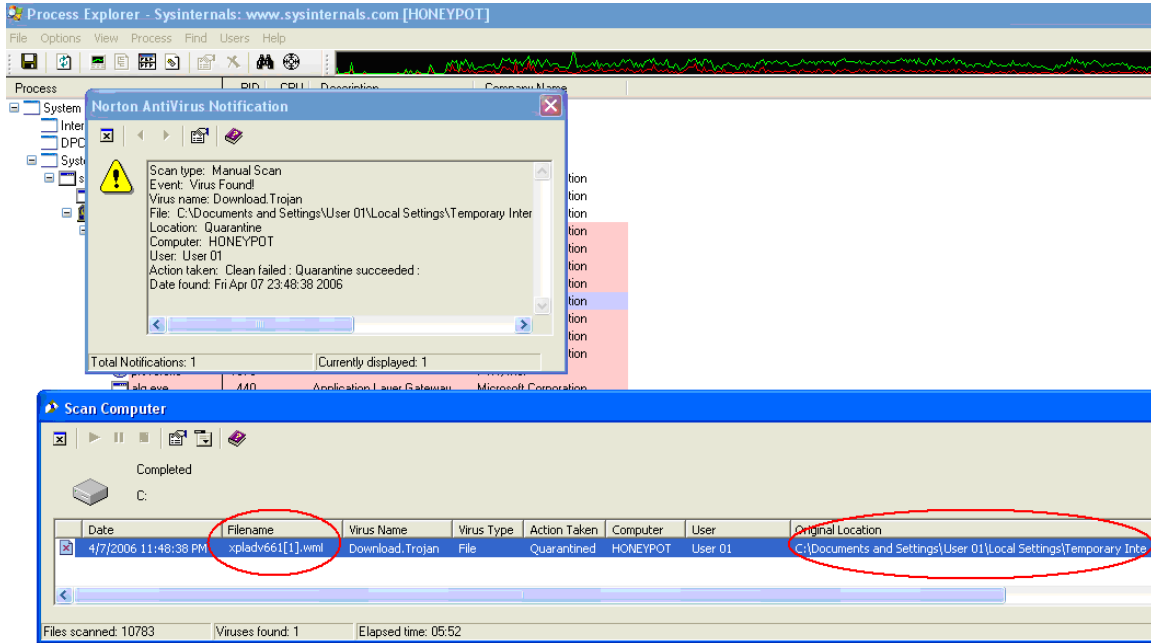
If this event is not related to legitimate system use, select 'Block' and investigate the issue further.

Remember this setting

e. Since the malicious process could not start, there was no system damage and running processes return to normal.

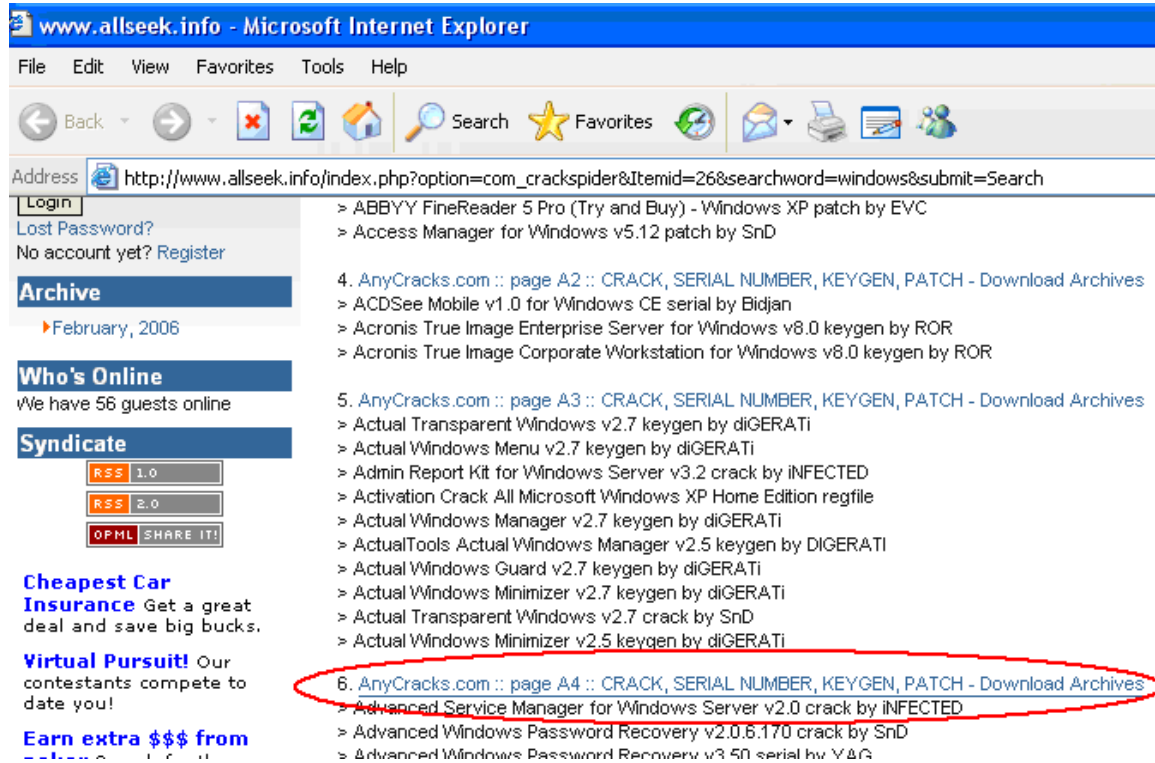
Process	PID	CPU	Description	Company Name
System Idle Process	0	95.05		
Interrupts	n/a		Hardware Interrupts	
DPCs	n/a		Deferred Procedure Calls	
System	4	0.99		
smss.exe	456		Windows NT Session Mana...	Microsoft Corporation
csrss.exe	512		Client Server Runtime Process	Microsoft Corporation
winlogon.exe	536		Windows NT Logon Applica...	Microsoft Corporation
services.exe	580	0.99	Services and Controller app	Microsoft Corporation
svchost.exe	744		Generic Host Process for Wi...	Microsoft Corporation
svchost.exe	804		Generic Host Process for Wi...	Microsoft Corporation
svchost.exe	868		Generic Host Process for Wi...	Microsoft Corporation
wsentfy.exe	396		Windows Security Center N...	Microsoft Corporation
svchost.exe	920		Generic Host Process for Wi...	Microsoft Corporation
svchost.exe	1036		Generic Host Process for Wi...	Microsoft Corporation
spoolsv.exe	1304		Spooler SubSystem App	Microsoft Corporation
pfsvc.exe	1676			PWI, Inc.
alg.exe	440		Application Layer Gateway ...	Microsoft Corporation
svchost.exe	1588		Generic Host Process for Wi...	Microsoft Corporation
defwatch.exe	2444		Virus Definition Daemon	Symantec Corporation
rtvscan.exe	2472		Norton AntiVirus	Symantec Corporation
MSGSYS.E...	2624		CBA -- Message System	Intel Corporation
svchost.exe	3980		Generic Host Process for Wi...	Microsoft Corporation
lsass.exe	592		LSA Shell (Export Version)	Microsoft Corporation
wpabaln.exe	1124		Windows WPA Balloon Rem...	Microsoft Corporation
explorer.exe	1268		Windows Explorer	Microsoft Corporation
PF5.exe	1420	1.98	Privatefirewall 5.0 Application	
WZQKPICK.EXE	1448		WinZip Executable	WinZip Computing, Inc.
mspaint.exe	3956		Paint	Microsoft Corporation
procexp.exe	1732	0.99	Sysinternals Process Explorer	Sysinternals
taskmgr.exe	1908		Windows TaskManager	Microsoft Corporation
vp trays.exe	2828		Norton AntiVirus	Symantec Corporation

f. Running Symantec AntiVirus after the test shows a downloaded WMF that was stored in a temporary Internet folder used to spearhead the attack.



g. If the 'a.exe' process was to run, there would be an infection similar to Case #1.

h. Another scenario is when an attack initiated by a WMF exploit leads to a known Trojan. If the #6 link in the screenshot below is selected, a known WMF exploit is launched....



www.allseek.info - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Search Favorites

Address http://www.allseek.info/index.php?option=com_crackspider&Itemid=26&searchword=windows&submit=Search

Login
Lost Password?
No account yet? Register

Archive
February, 2006

Who's Online
We have 56 guests online

Syndicate
RSS 1.0
RSS 2.0
OPML SHARE IT!

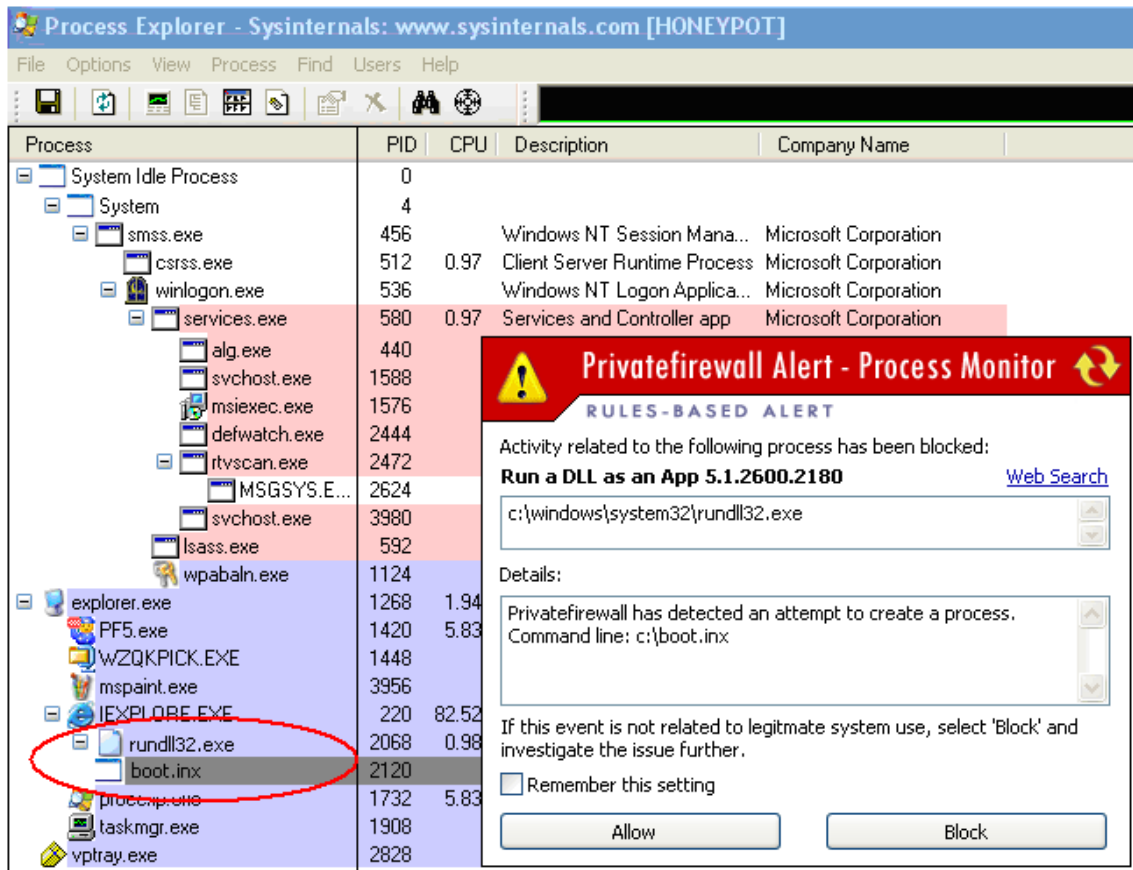
Cheapest Car Insurance Get a great deal and save big bucks.

Virtual Pursuit! Our contestants compete to date you!

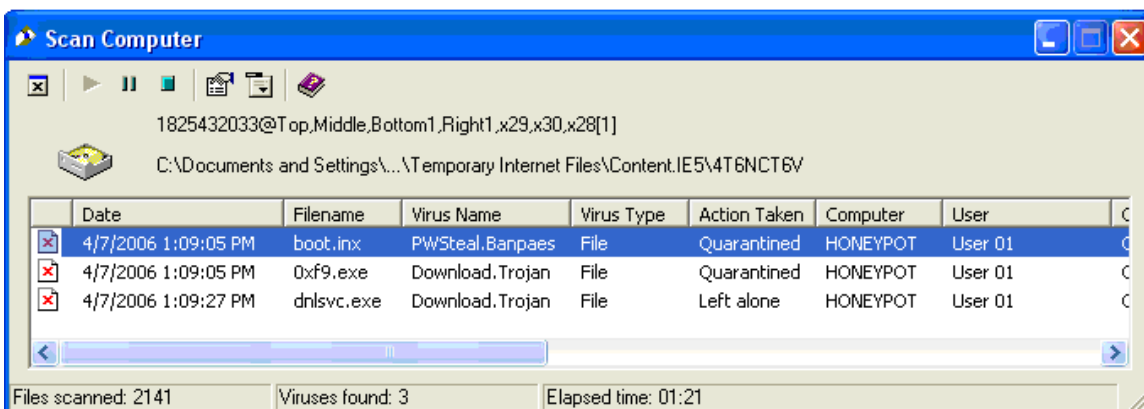
Earn extra \$\$\$ from

- > ABBYY FineReader 5 Pro (Try and Buy) - Windows XP patch by EVC
- > Access Manager for Windows v5.12 patch by SnD
- 4. AnyCracks.com :: page A2 :: CRACK, SERIAL NUMBER, KEYGEN, PATCH - Download Archives
 - > ACDSee Mobile v1.0 for Windows CE serial by Bidjan
 - > Acronis True Image Enterprise Server for Windows v8.0 keygen by ROR
 - > Acronis True Image Corporate Workstation for Windows v8.0 keygen by ROR
- 5. AnyCracks.com :: page A3 :: CRACK, SERIAL NUMBER, KEYGEN, PATCH - Download Archives
 - > Actual Transparent Windows v2.7 keygen by diGERATi
 - > Actual Windows Menu v2.7 keygen by diGERATi
 - > Admin Report Kit for Windows Server v3.2 crack by INFECTED
 - > Activation Crack All Microsoft Windows XP Home Edition regfile
 - > Actual Windows Manager v2.7 keygen by diGERATi
 - > ActualTools Actual Windows Manager v2.5 keygen by DIGERATI
 - > Actual Windows Guard v2.7 keygen by diGERATi
 - > Actual Windows Minimizer v2.7 keygen by diGERATi
 - > Actual Transparent Windows v2.7 crack by SnD
 - > Actual Windows Minimizer v2.5 keygen by diGERATi
- 6. AnyCracks.com :: page A4 :: CRACK, SERIAL NUMBER, KEYGEN, PATCH - Download Archives
 - > Advanced Service Manager for Windows Server v2.0 crack by INFECTED
 - > Advanced Windows Password Recovery v2.0.6.170 crack by SnD
 - > Advanced Windows Password Recovery v3.50 serial by Y&G

...and an attempt to run the boot.inx file is initiated, triggering another alert by Privatefirewall 5.0.



If access is allowed, the virus identified as 'PWSteal.Banpaes' will be created.



5. Conclusion

Vulnerabilities at the desktop or endpoint level are increasing in volume, complexity and severity. Conventional technologies, i.e. signature-based anti-virus/anti-spyware and personal firewalls are limited in their effectiveness in defending endpoint computers from such threats. By alerting users when new processes as well as new/unknown child processes are being invoked, and an ability to stop such activity, Privatefirewall 5.0 provides an effective and unique defense from numerous forms of malware viruses.