

Objective and Methodology:

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

To demonstrate Privatefirewall's effectiveness at detecting threats not typically addressed by "personal firewall" applications, a list of top 20 viruses collected primarily (other well-known viruses were also added) from leading anti-virus vendor Kaspersky Lab (Nov-Jan 2006) was utilized to perpetrate attacks on a Privacyware PC. Tests were performed using a Windows XP SP2 (2 virtual processors, 192 Mb RAM). The host machine is a Pentium 4 (2800 Mhz) with HT, 1024 Mb RAM.

Results Summary:

The results were recorded and are documented in the following tables. **In summary, Privatefirewall 5.0 performed flawlessly, achieving a perfect score of 100%, detecting 20 of the 20 viruses without the use of virus definitions.**

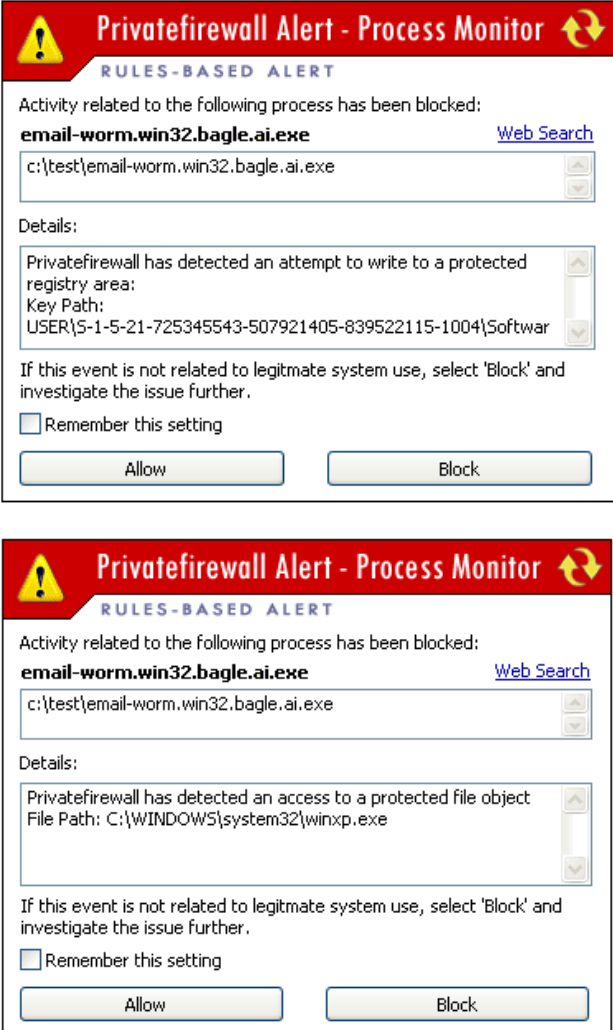
Privatefirewall detected these viruses based on behaviors characteristic of unauthorized system use. These include:

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

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 as they are either only able to detect something that has already been discovered or the technology is not designed to provide the type of protection required of the threat. In keeping with a "defense-in-depth" strategy, Privacyware espouses a layered approach to defense that enables an array of threat types to be identified based on the system behavior that accompanies or precedes them. In this way, personal computer users and IT managers within small, medium or large organizations can more effectively and proactively protect the environments for which they are responsible.

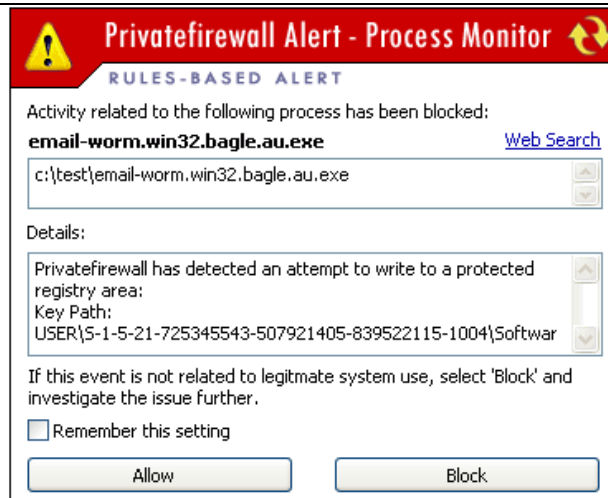
Privacyware Privatefirewall is one such solution. Privatefirewall is available as a stand-alone application for personal and home computing and as a centrally managed offering called Endpoint Security Console. For more information, please visit www.privacyware.com.


Worm/Virus/Malware name	Description/What it does	How PC was infected	What action Privatefirewall took	Processes launched by this vulnerability, that attempted to access internet, or other actions detected by Privatefirewall
<p>Email-Worm.Win32.Bagle.ai</p>	<p>The worm opens port 1080 and another port chosen at random. It then tracks port activity. It uses its own SMTP server to send messages. It tracks the execution of most well-known antivirus products and firewalls and terminates these processes.</p>	<p>This worm spreads via the Internet as an attachment to infected messages and also via P2P networks.</p>	 <p>The screenshots show two instances of a 'Privatefirewall Alert - Process Monitor' dialog box. Both are titled 'RULES-BASED ALERT' and state that activity related to the process 'email-worm.win32.bagle.ai.exe' has been blocked. The first alert details an attempt to write to a protected registry area with the key path 'USER\5-1-5-21-725345543-507921405-839522115-1004\Softwar'. The second alert details an attempt to access a protected file object at the path 'C:\WINDOWS\system32\winxp.exe'. Both alerts include a 'Remember this setting' checkbox and 'Allow' and 'Block' buttons.</p>	<p>Attempt to access protected registry area, and access protected Windows object associated with windows executable WINXP.EXE</p>

**Email-
Worm.Win32.Bagle.au**

Bagle.au opens TCP port 81 and listens for further commands. For instance, the worm installs a proxy server that can be controlled via this port. Bagle.au attempts to block firewalls and antivirus solutions by stopping their processes.

This worm spreads via the Internet as an attachment to infected messages and also via P2P networks.



Privatefirewall Alert - Process Monitor 

RULES-BASED ALERT

Activity related to the following process has been blocked:
email-worm.win32.bagle.au.exe [Web Search](#)

c:\test\email-worm.win32.bagle.au.exe

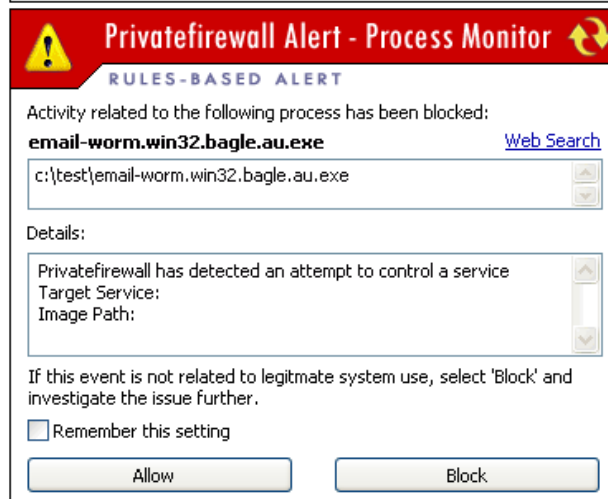
Details:


Privatefirewall has detected an attempt to write to a protected registry area:
Key Path:
USER\5-1-5-21-725345543-507921405-839522115-1004\Softwar

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

Remember this setting

Allow Block



Privatefirewall Alert - Process Monitor 

RULES-BASED ALERT

Activity related to the following process has been blocked:
email-worm.win32.bagle.au.exe [Web Search](#)

c:\test\email-worm.win32.bagle.au.exe

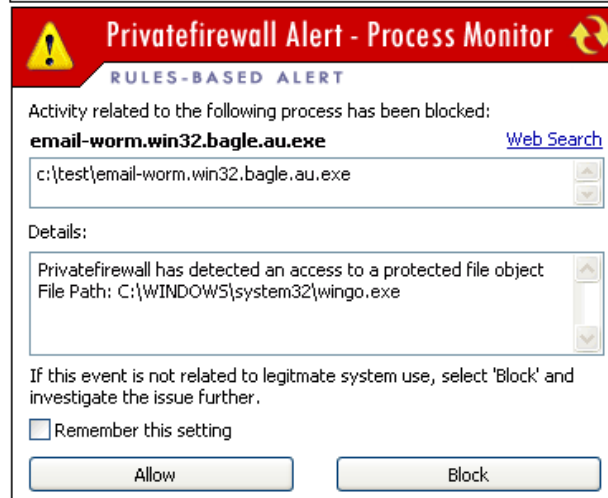
Details:


Privatefirewall has detected an attempt to control a service
Target Service:
Image Path:

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

Remember this setting

Allow Block



Privatefirewall Alert - Process Monitor 

RULES-BASED ALERT

Activity related to the following process has been blocked:
email-worm.win32.bagle.au.exe [Web Search](#)

c:\test\email-worm.win32.bagle.au.exe

Details:

Privatefirewall has detected an access to a protected file object
File Path: C:\WINDOWS\system32\wingo.exe

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

Remember this setting

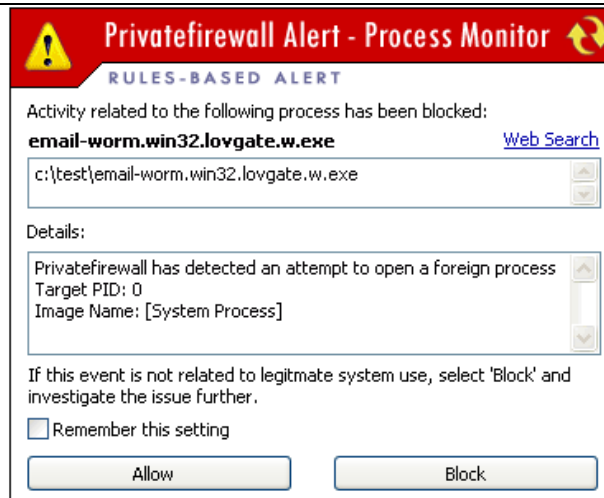
Allow Block


Attempt to access protected registry area, attempt to control windows service, and access protected object associated with windows executable **WINGO.EXE**

**Email-
Worm.Win32.LovGate.w**

It makes the \windows\Media folder accessible via the local network. The worm attempts to copy itself to all local network machines by using the Administrator account. The worm also sends itself using its own SMTP server. The worm harvests information about the victim machine, saves it in a file named c:\Netlog.txt and sends this file to the worm's author via email. It installs a backdoor on TCP port 6000 to receive commands. It launches an FTP server without login or password on a random port. The worm searches all accessible disks from C: to Z: for files with the extension .exe. It then renames them as *.zmx, ascribes the attribute 'hidden/ system' to these files, and copies itself to the original files under the original names (working in the same way as companion viruses do.)

This worm spreads via the Internet as an attachment to infected messages.



Privatefirewall Alert - Process Monitor 

RULES-BASED ALERT

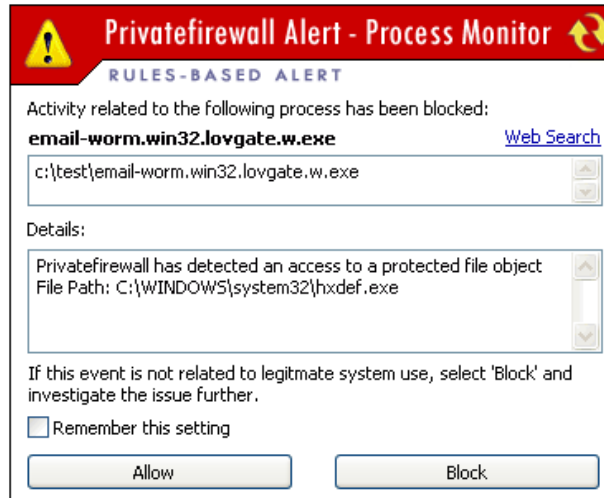
Activity related to the following process has been blocked:
email-worm.win32.lovgate.w.exe [Web Search](#)


c:\test\email-worm.win32.lovgate.w.exe

Details:
Privatefirewall has detected an attempt to open a foreign process
Target PID: 0
Image Name: [System Process]

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

Remember this setting



Privatefirewall Alert - Process Monitor 

RULES-BASED ALERT

Activity related to the following process has been blocked:
email-worm.win32.lovgate.w.exe [Web Search](#)

c:\test\email-worm.win32.lovgate.w.exe

Details:
Privatefirewall has detected an access to a protected file object
File Path: C:\WINDOWS\system32\hxdef.exe

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

Remember this setting



Privatefirewall Alert - Process Monitor 

RULES-BASED ALERT

Activity related to the following process has been blocked:
email-worm.win32.lovgate.w.exe [Web Search](#)

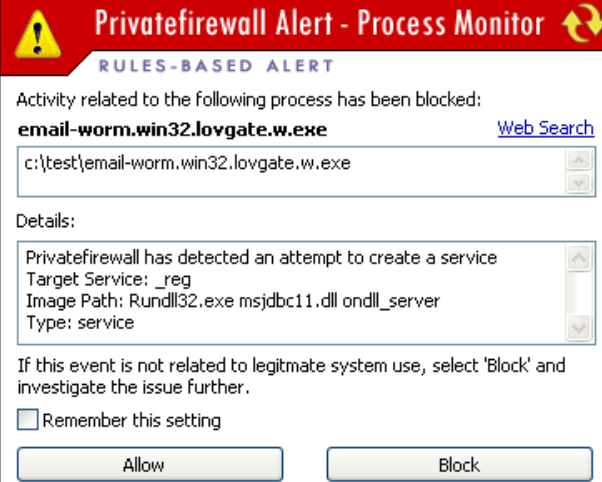

c:\test\email-worm.win32.lovgate.w.exe

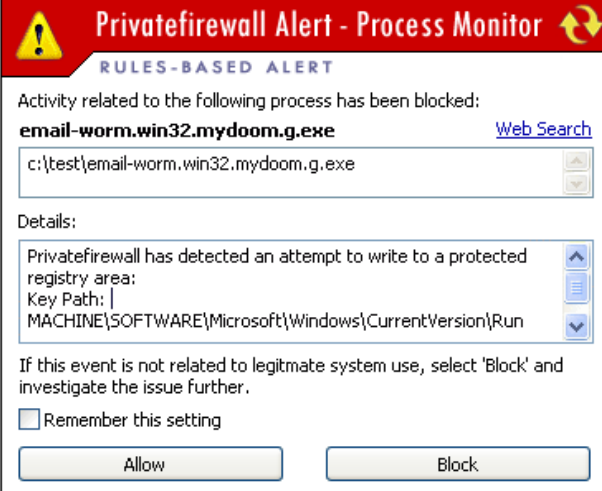

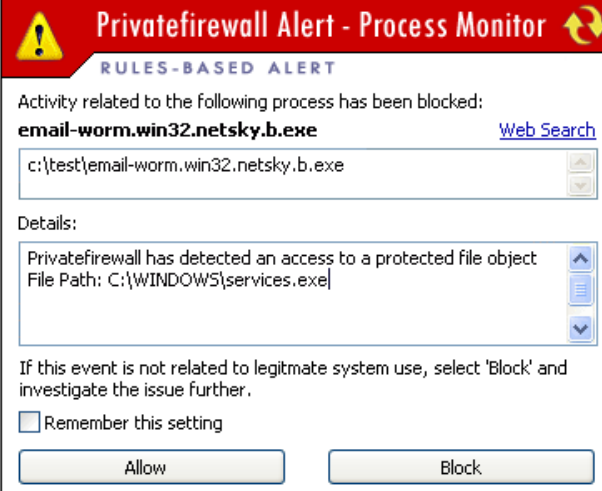

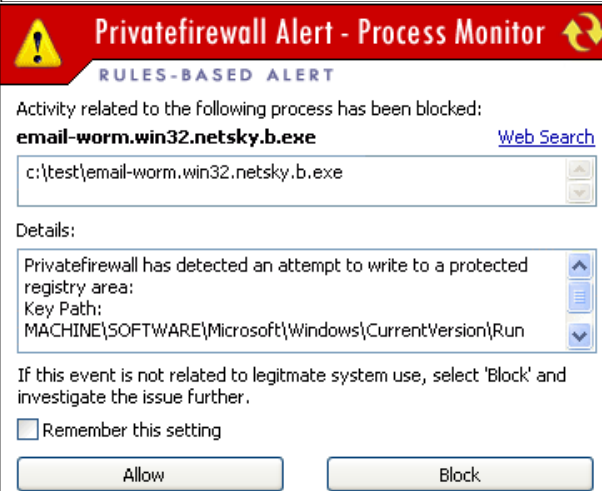

Details:
Privatefirewall has detected an attempt to write to a protected registry area:
Key Path: MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

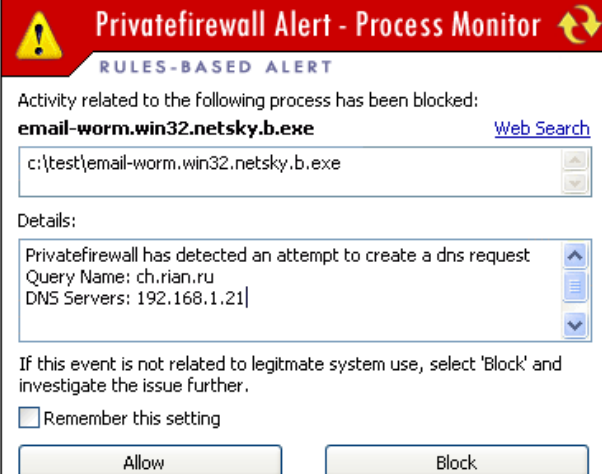
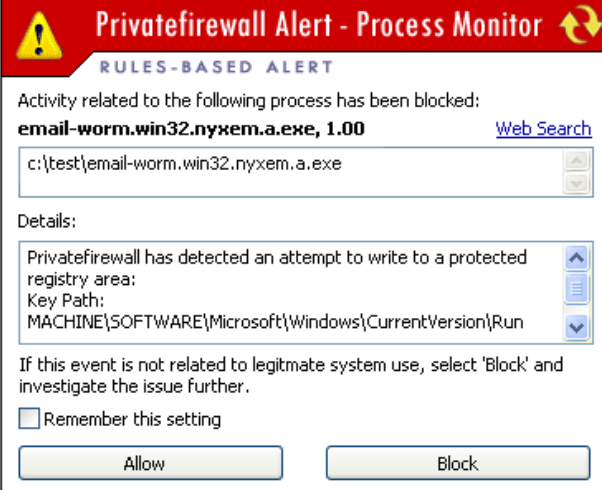
If this event is not related to legitimate system use, select 'Block' and investigate the issue further.

Remember this setting

Attempt to initiate foreign process, access protected file object, associated with **HXDEF.EXE**, access protected registry area, create a service target, **and DNS request**

				
<p>Email-Worm.Win32.Mydoom.g</p>	<p>Once the worm is launched, it may open Windows Notepad, which will display a random selection of characters. The worm includes a backdoor function, and is also coded to conduct a DoS attack on www.symantec.com and symantec.com. The worm opens TCP ports 80 and 1080 to receive commands. The backdoor component can act as a proxy server, and also download and launch files.</p>	<p>This worm spreads via the Internet as an attachment to infected messages.</p>		<p>Attempt to access protected file object and access protected registry area</p>

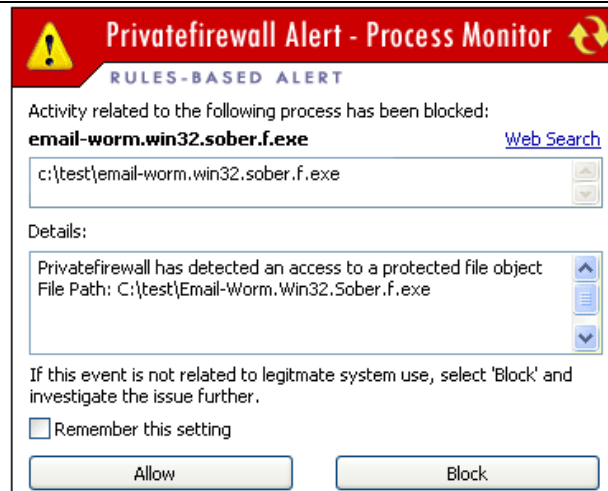
			 <p>Privatefirewall Alert - Process Monitor </p> <p>RULES-BASED ALERT</p> <p>Activity related to the following process has been blocked: email-worm.win32.mydoom.g.exe Web Search</p> <p>c:\test\email-worm.win32.mydoom.g.exe</p> <p>Details: Privatefirewall has detected an attempt to write to a protected registry area: Key Path: MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run</p> <p>If this event is not related to legitimate system use, select 'Block' and investigate the issue further. <input type="checkbox"/> Remember this setting</p> <p>Allow Block</p>	
<p>Email-Worm.Win32.NetSky.b</p>	<p>The worm creates a number of copies of itself in all sub-directories on disks c to Z which contain the word 'share' or 'sharing' in the directory name. The worm finds files with extensions adb, asp, dbx, doc, eml, htm, html, msg, oft, php, pl, rtf, sht, tbb, txt, uin, vbs and wab, searches them for email addresses and sends a copy of itself to the addresses found. The worm uses its own SMTP library to send messages.</p>	<p>(Also known as Moodown.b) This worm spreads via the Internet as a file attached to infected emails.</p>	 <p>Privatefirewall Alert - Process Monitor </p> <p>RULES-BASED ALERT</p> <p>Activity related to the following process has been blocked: email-worm.win32.netsky.b.exe Web Search</p> <p>c:\test\email-worm.win32.netsky.b.exe</p> <p>Details: Privatefirewall has detected an access to a protected file object File Path: C:\WINDOWS\services.exe</p> <p>If this event is not related to legitimate system use, select 'Block' and investigate the issue further. <input type="checkbox"/> Remember this setting</p> <p>Allow Block</p>  <p>Privatefirewall Alert - Process Monitor </p> <p>RULES-BASED ALERT</p> <p>Activity related to the following process has been blocked: email-worm.win32.netsky.b.exe Web Search</p> <p>c:\test\email-worm.win32.netsky.b.exe</p> <p>Details: Privatefirewall has detected an attempt to write to a protected registry area: Key Path: MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run</p> <p>If this event is not related to legitimate system use, select 'Block' and investigate the issue further. <input type="checkbox"/> Remember this setting</p> <p>Allow Block</p>	<p>Attempt to access protected file object and access protected registry area, and create a DNS request</p>


				
<p>Email-Worm.Win32.Nyxem.a</p>	<p>Once launched, the worm copies itself and its components to the Windows system directory. The name is chosen at random by the worm from the names of files which already exist. When launching, the worm launches Windows Media Player. The worm uses its own library (ossntp.dll, oswinsck.dll) to send messages via SMTP. The worm harvests email addresses from Yahoo and MSN Messenger, and also scans files with the extensions .htm and .dbx to harvest addresses. The worm attempts to prevent antivirus programs from launching. The worm attempts to conduct a DoS attack on www.nymex.com</p>	<p>This worm spreads via the Internet as an attachment to infected messages. It also spreads via Yahoo Pager and MSN Messenger.</p>		<p>Attempt to access protected file object, access protected registry area</p>

**Email-
Worm.Win32.Sober.f**

The worm is activated if the user opens the attached file. Once the worm is launched, it opens Notepad which will display the text contained in the original message. The worm creates several copies of itself and its additional files in the Windows system directory. It harvests email addresses, and sends email messages to these addresses by creating a direct connection to the SMTP server.

This worm spreads via email as a file attached to infected messages. It also spreads via file-sharing networks.



Privatefirewall Alert - Process Monitor 

RULES-BASED ALERT

Activity related to the following process has been blocked:
email-worm.win32.sober.f.exe [Web Search](#)

c:\test\email-worm.win32.sober.f.exe

Details:

Privatefirewall has detected an access to a protected file object
File Path: C:\test\Email-Worm.Win32.Sober.f.exe

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

Remember this setting



Privatefirewall Alert - Process Monitor 

RULES-BASED ALERT

Activity related to the following process has been blocked:
email-worm.win32.sober.f.exe [Web Search](#)

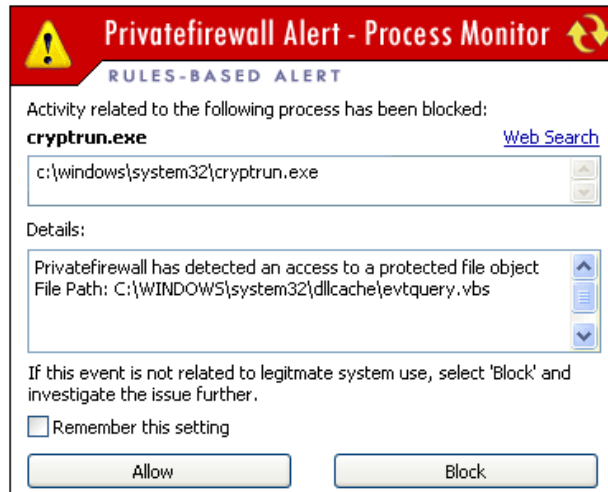
c:\test\email-worm.win32.sober.f.exe


Details:

Privatefirewall has detected an attempt to write to a protected registry area:
Key Path: USER\5-1-5-21-725345543-507921405-839522115-1004\Softwar

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

Remember this setting



Privatefirewall Alert - Process Monitor 

RULES-BASED ALERT

Activity related to the following process has been blocked:
cryptrun.exe [Web Search](#)

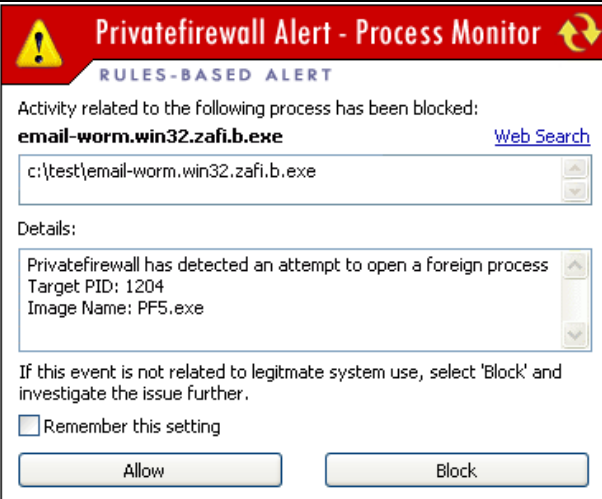

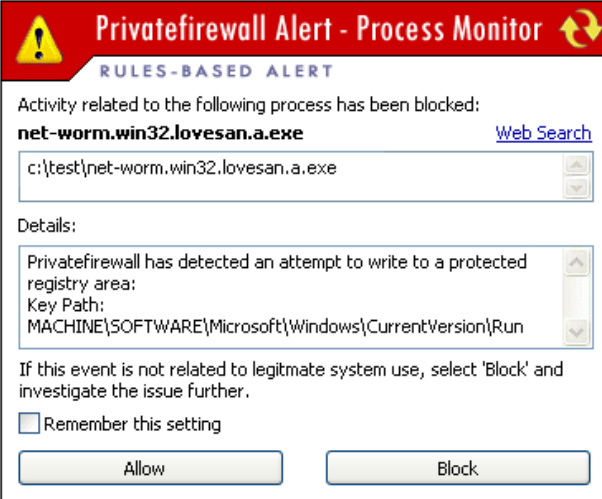
c:\windows\system32\cryptrun.exe

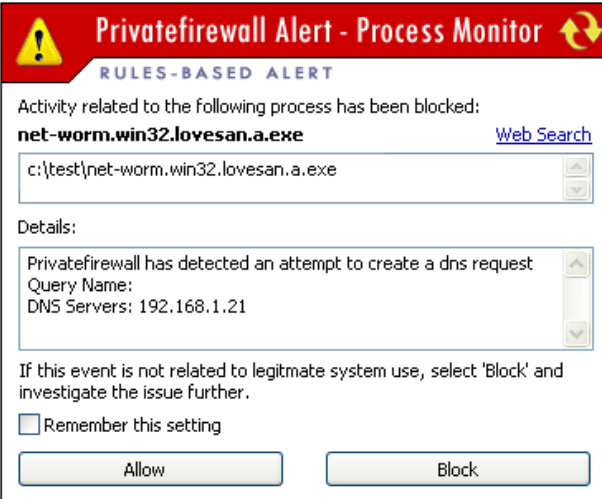
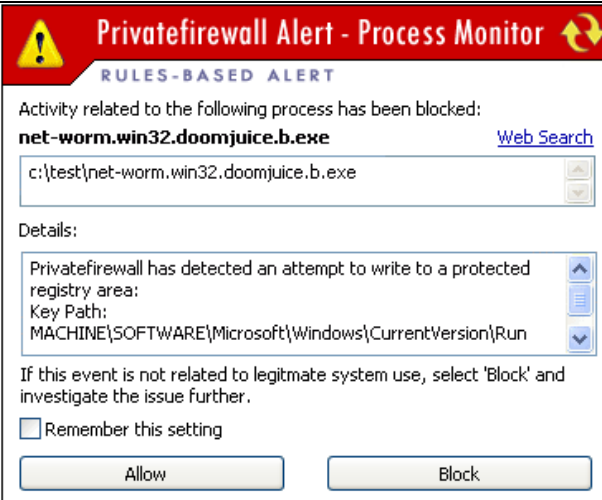
Details:

Privatefirewall has detected an access to a protected file object
File Path: C:\WINDOWS\system32\dlcache\evtquery.vbs

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

Remember this setting

<p>Email-Worm.Win32.Zafi.b</p>	<p>Once launched, the worm copies its file to the Windows system directory. The name of the file is randomly generated. It stops the windows critical processes and deletes the files from disk. It attempts to detect antivirus program files on the computer and overwrite them with a copy of itself. It also attempts to conduct DoS attacks on the following sites:www.2f.hu, www.parlament.hu, www.virusbuster.hu, www.virushirado.hu</p>	<p>This worm spreads via the Internet as an attachment to infected messages, and also via local and file-sharing networks.</p>	 	<p>Attempt to access protected file object</p>
<p>Net-Worm.Win32.Lovesan.a</p>	<p>Lovesan downloads and attempts to run a file named msblast.exe. The worm scans IP addresses, attempting to connect to 20 random IP addresses and infect any vulnerable machines. Lovesan sleeps for 1.8 seconds and scans the next 20 IP addresses. The worm sends a buffer-overrun request to vulnerable machines via TCP port 135. The newly infected machine then initiates the command</p>	<p>Lovesan is an Internet Worm which exploits the DCOM RPC vulnerability.</p>		<p>Attempt to access protected registry area, create DNS request and initiate outgoing TCP traffic (epmap)</p>

	<p>shell on TCP port 4444. Once a computer is infected the system sends an error message about RPC service failure and may reboot the machine.</p>		 <p>Privatefirewall Alert - Process Monitor RULES-BASED ALERT</p> <p>Activity related to the following process has been blocked: net-worm.win32.lovesan.a.exe Web Search</p> <p>c:\test\net-worm.win32.lovesan.a.exe</p> <p>Details: Privatefirewall has detected an attempt to create a dns request Query Name: DNS Servers: 192.168.1.21</p> <p>If this event is not related to legitimate system use, select 'Block' and investigate the issue further.</p> <p><input type="checkbox"/> Remember this setting</p> <p>Allow Block</p>	
<p>Net-Worm.Win32.Doomjuice .b</p>	<p>Once launched, the worm copies itself to the Windows system directory under the name regedit.exe and registers this file in the system registry auto-run key. To propagate, the worm utilizes computers infected by Mydoom.a and Mydoom.b The worm connects to TCP port 3127, which has been opened by shimgapi.dll, the backdoor component of Mydoom, to receive commands. If the infected computer answers the</p>	<p>This worm spreads via the Internet, using computers infected by I-Worm.Mydoom.a and I-Worm.Mydoom.b to propagate.</p>	 <p>Privatefirewall Alert - Process Monitor RULES-BASED ALERT</p> <p>Activity related to the following process has been blocked: net-worm.win32.doomjuice.b.exe Web Search</p> <p>c:\test\net-worm.win32.doomjuice.b.exe</p> <p>Details: Privatefirewall has detected an attempt to write to a protected registry area: Key Path: MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run</p> <p>If this event is not related to legitimate system use, select 'Block' and investigate the issue further.</p> <p><input type="checkbox"/> Remember this setting</p> <p>Allow Block</p>	<p>Attempt to access protected file object, access protected registry area, create a DNS request, and initiate outgoing TCP traffic.</p>

command, then Doomjuice establishes a connection and sends a copy of itself. The backdoor component of Mydoom accepts the file and executes it. The worm attempts to conduct a DoS attack on the www.microsoft.com site.

 **Privatefirewall Alert - Process Monitor** 

RULES-BASED ALERT

Activity related to the following process has been blocked:
net-worm.win32.doomjuice.b.exe [Web Search](#)



c:\test\net-worm.win32.doomjuice.b.exe

Details:

Privatefirewall has detected an access to a protected file object
File Path: C:\WINDOWS\system32\znhhy.exe

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

Remember this setting

 **Privatefirewall Alert - Process Monitor** 

RULES-BASED ALERT

Activity related to the following process has been blocked:
net-worm.win32.doomjuice.b.exe [Web Search](#)



c:\test\net-worm.win32.doomjuice.b.exe

Details:

Privatefirewall has detected an attempt to create a dns request
Query Name:
DNS Servers: 192.168.1.21

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

Remember this setting

 **Privatefirewall Alert - Outgoing Traffic** 

APPLICATION CONTROL ENGINE

Access to the Network/Internet has been blocked for:
Net-Worm.Win32.Doomjuice.b.exe [Web Search](#)

C:\test\Net-Worm.Win32.Doomjuice.b.exe

Details:

2/21/2006 1:38:18 PM PF has blocked outgoing TCP (6) packet
from 192.168.1.212:1355 to 189.199.53.0:3127

Remember this setting

**Net-
Worm.Win32.Mytob.bi**

Once launched, the worm copies itself to the Windows system directory. IT also registers itself in the Windows system registry, ensuring that the worm will be launched each time Windows is rebooted on the victim machine. Net-Worm.Win32.Mytob.bi opens a TCP port on the victim machine to contact to IRC channels and receive commands. This gives a remote malicious user full access to the victim machine via IRC channels, making it possible to receive information from the infected computer, download, launch and delete files. The worm also terminates processes connected with antivirus solutions, firewalls, and other security programs. The worm also modifies the %System%\drivers\etc\hosts file in order to block access to antivirus vendors' sites from the victim machine.

It spreads via the Internet as an attachment to infected messages, and includes a backdoor program which receives commands via IRC channels.

Privatefirewall Alert - Process Monitor

RULES-BASED ALERT

Activity related to the following process has been blocked:
net-worm.win32.mytob.bi.exe [Web Search](#)

c:\test\net-worm.win32.mytob.bi.exe

Details:

Privatefirewall has detected an access to a protected file object
File Path: C:\WINDOWS\system32\drivers\etc\hosts

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

Remember this setting

Privatefirewall Alert - Process Monitor

RULES-BASED ALERT

Activity related to the following process has been blocked:
net-worm.win32.mytob.bi.exe [Web Search](#)

c:\test\net-worm.win32.mytob.bi.exe

Details:

Privatefirewall has detected an attempt to write to a protected registry area:
Key Path: MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

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

Remember this setting

Privatefirewall Alert - Process Monitor

RULES-BASED ALERT

Activity related to the following process has been blocked:
net-worm.win32.mytob.bi.exe [Web Search](#)

c:\test\net-worm.win32.mytob.bi.exe

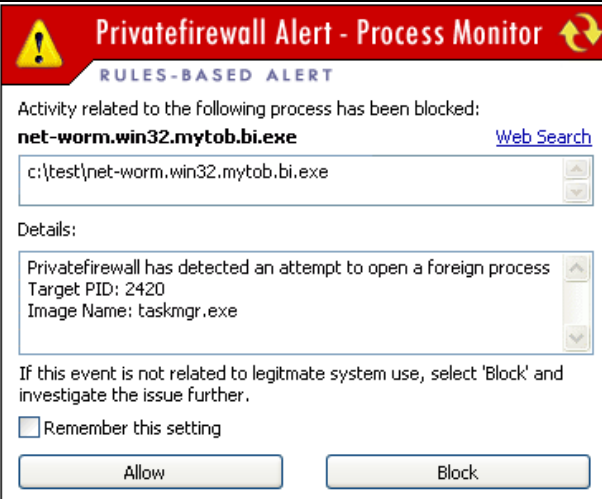

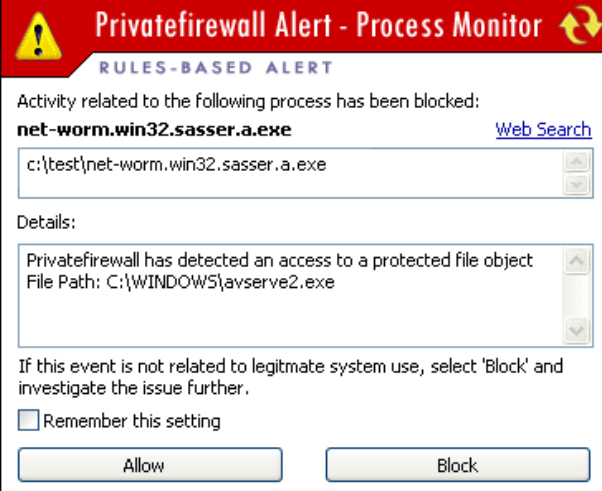

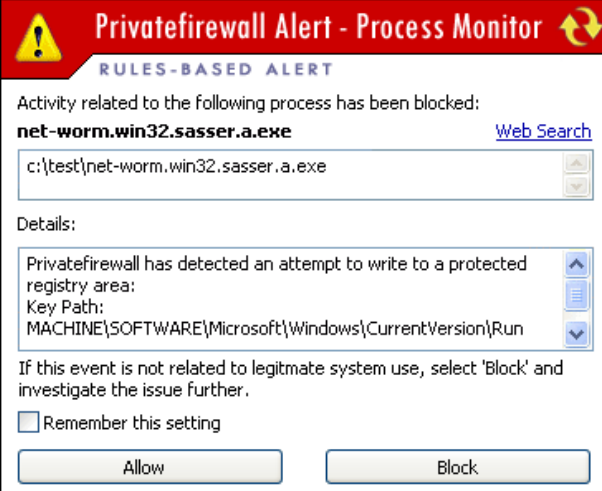

Details:

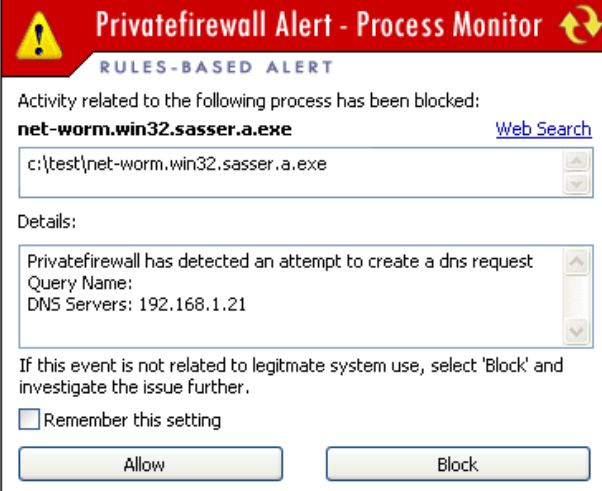
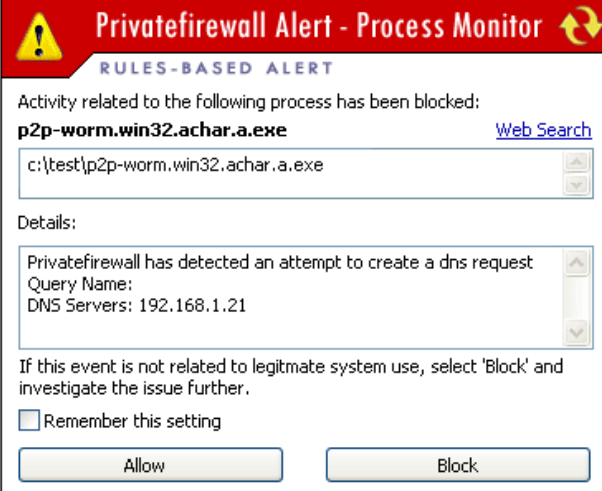

Privatefirewall has detected an attempt to create a dns request
Query Name: rian.ru
DNS Servers: 192.168.1.21




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

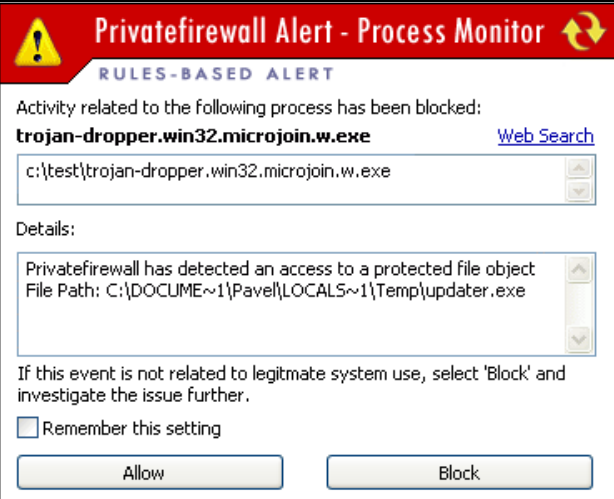
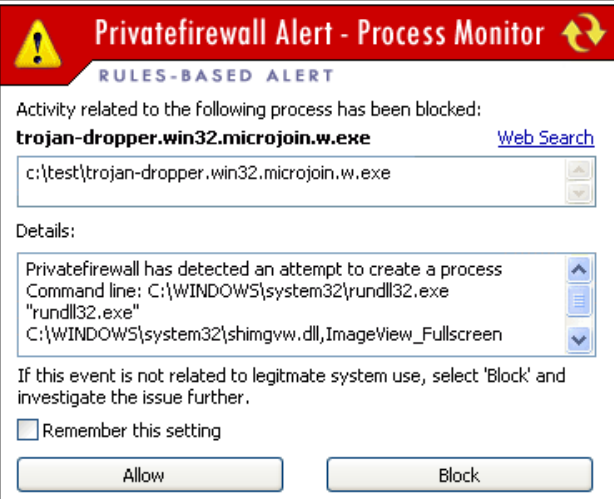

Remember this setting

Attempt to access protected file object, access protected registry area, create a DNS request, and open a foreign process

			 <p>Privatefirewall Alert - Process Monitor </p> <p>RULES-BASED ALERT</p> <p>Activity related to the following process has been blocked: net-worm.win32.mytob.bi.exe Web Search</p> <p>c:\test\net-worm.win32.mytob.bi.exe</p> <p>Details: Privatefirewall has detected an attempt to open a foreign process Target PID: 2420 Image Name: taskmgr.exe</p> <p>If this event is not related to legitimate system use, select 'Block' and investigate the issue further.</p> <input type="checkbox"/> Remember this setting <p>Allow Block</p>	
<p>Net-Worm.Win32.Sasser.a</p>	<p>Once launched, Sasser copies itself into the Windows root directory under the name avserve.exe and registers this file in the system registry autorun key. Sasser launches FTP server on TCP port 5554 and then launches 128 propagation routines. During this process, the worm attempts to initiate the AbortSystemShutdown process in order to forbid system reboot. Sasser initiates an IP-address scan in order to identify victim addresses and sends a request to TCP port 445. If any machines respond, Sasser exploits the LSASS vulnerability to launch a 'cmd.exe' command shell on TCP port 9996. After infection the victim machine generates an error message about a LSASS service failing, whereupon it may attempt to reboot.</p>	<p>Sasser is an Internet worm that exploits the MS Windows LSASS vulnerability.</p>	 <p>Privatefirewall Alert - Process Monitor </p> <p>RULES-BASED ALERT</p> <p>Activity related to the following process has been blocked: net-worm.win32.sasser.a.exe Web Search</p> <p>c:\test\net-worm.win32.sasser.a.exe</p> <p>Details: Privatefirewall has detected an access to a protected file object File Path: C:\WINDOWS\avserve2.exe</p> <p>If this event is not related to legitimate system use, select 'Block' and investigate the issue further.</p> <input type="checkbox"/> Remember this setting <p>Allow Block</p>  <p>Privatefirewall Alert - Process Monitor </p> <p>RULES-BASED ALERT</p> <p>Activity related to the following process has been blocked: net-worm.win32.sasser.a.exe Web Search</p> <p>c:\test\net-worm.win32.sasser.a.exe</p> <p>Details: Privatefirewall has detected an attempt to write to a protected registry area: Key Path: MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run</p> <p>If this event is not related to legitimate system use, select 'Block' and investigate the issue further.</p> <input type="checkbox"/> Remember this setting <p>Allow Block</p>	<p>Attempt to access protected file object, access protected registry area, and create a DNS request</p>

			 <p>Privatefirewall Alert - Process Monitor</p> <p>RULES-BASED ALERT</p> <p>Activity related to the following process has been blocked: net-worm.win32.sasser.a.exe Web Search</p> <p>c:\test\net-worm.win32.sasser.a.exe</p> <p>Details: Privatefirewall has detected an attempt to create a dns request Query Name: DNS Servers: 192.168.1.21</p> <p>If this event is not related to legitmate system use, select 'Block' and investigate the issue further.</p> <input type="checkbox"/> Remember this setting <p>Allow Block</p>	
<p>P2P- Worm.Win32.Achar.a</p>	<p>To infect Kazaa shared folder the worm reads its name from system registry and copies itself to the folder. The worm also tries to copy itself with the "CUCARACHA.exe" name to startup directories on remote computers.</p>	<p>This is a family of low-severity worms that replicate by making their copies in a Kazaa shared folder.</p>	 <p>Privatefirewall Alert - Process Monitor</p> <p>RULES-BASED ALERT</p> <p>Activity related to the following process has been blocked: p2p-worm.win32.achar.a.exe Web Search</p> <p>c:\test\p2p-worm.win32.achar.a.exe</p> <p>Details: Privatefirewall has detected an attempt to create a dns request Query Name: DNS Servers: 192.168.1.21</p> <p>If this event is not related to legitmate system use, select 'Block' and investigate the issue further.</p> <input type="checkbox"/> Remember this setting <p>Allow Block</p>	<p>Attempt to access protected file object, and create a DNS request</p>
			 <p>Privatefirewall Alert - Outgoing Traffic</p> <p>APPLICATION CONTROL ENGINE</p> <p>Access to the Network/Internet has been blocked for: Net-Worm.Win32.Sasser.a.exe Web Search</p> <p>C:\test\Net-Worm.Win32.Sasser.a.exe</p> <p>Details: 2/21/2006 1:45:37 PM PF has blocked outgoing TCP (6) packet from 192.168.1.212:2249 to 130.71.204.158:445 (microsoft-ds)</p> <input type="checkbox"/> Remember this setting <p>Allow Access Block Access</p>	

			 <p>Privatefirewall Alert - Process Monitor</p> <p>RULES-BASED ALERT</p> <p>Activity related to the following process has been blocked: p2p-worm.win32.achar.a.exe Web Search</p> <p>c:\test\p2p-worm.win32.achar.a.exe</p> <p>Details:</p> <p>Privatefirewall has detected an access to a protected file object File Path: \\180.87.55.1\c\Documents and Settings\All Users\Menu Inicio\CUCARACHA.exe</p> <p>If this event is not related to legitimate system use, select 'Block' and investigate the issue further.</p> <input type="checkbox"/> Remember this setting <p>Allow Block</p>	
<p>Trojan.Win32.StartPage.nk</p>	<p>This Trojan modifies the Start Page, Search Page, SearchURL, and SearchBar.</p>	<p>No known spreading routine.</p>	 <p>Privatefirewall Alert - Process Monitor</p> <p>RULES-BASED ALERT</p> <p>Activity related to the following process has been blocked: trojan.win32.startpage.nk.exe Web Search</p> <p>c:\test\trojan.win32.startpage.nk.exe</p> <p>Details:</p> <p>Privatefirewall has detected an access to a protected file object File Path: c:\windows\system32\elitevlt32.exe</p> <p>If this event is not related to legitimate system use, select 'Block' and investigate the issue further.</p> <input type="checkbox"/> Remember this setting <p>Allow Block</p>  <p>Privatefirewall Alert - Process Monitor</p> <p>RULES-BASED ALERT</p> <p>Activity related to the following process has been blocked: trojan.win32.startpage.nk.exe Web Search</p> <p>c:\test\trojan.win32.startpage.nk.exe</p> <p>Details:</p> <p>Privatefirewall has detected an attempt to create a process Command line: C:\WINDOWS\system32\cmd.exe "C:\WINDOWS\system32\cmd.exe" /c del C:\test\tROJAN~4.EXE >> NUL</p> <p>If this event is not related to legitimate system use, select 'Block' and investigate the issue further.</p> <input type="checkbox"/> Remember this setting <p>Allow Block</p>	<p>Attempt to access protected file object and create a process</p>

<p>Trojan-Dropper.Win32.Microjoin.w</p>	<p>Drops Trojan.LdPinch and displays a picture.</p>	<p>No known spreading routine.</p>	 	<p>Attempt to access protected file object and create a process</p>
<p>Trojan-PSW.Win32.LdPinch.gm</p>	<p>It tries to steal the following information: Email account information, passwords from Windows Commander, CuteFTP, WS_FTP, Outlook, Opera, Mozilla, BatMail, Trillian, ICQ, E Dialer, FAR Manager and sends it to author via email.</p>	<p>Have no known spreading routine.</p>		<p>Attempt to access protected file object, access protected registry area, and create a DNS request</p>

Privatefirewall Alert - Process Monitor 

RULES-BASED ALERT

Activity related to the following process has been blocked:
trojan-psw.win32.ldpinch.gm.exe [Web Search](#)


c:\test\trojan-psw.win32.ldpinch.gm.exe

Details:

Privatefirewall has detected an attempt to write to a protected registry area:
Key Path:
USER\5-1-5-21-725345543-507921405-839522115-1004\Softwar

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

Remember this setting

Privatefirewall Alert - Process Monitor 

RULES-BASED ALERT

Activity related to the following process has been blocked:
trojan-psw.win32.ldpinch.gm.exe [Web Search](#)


c:\test\trojan-psw.win32.ldpinch.gm.exe

Details:

Privatefirewall has detected an attempt to create a dns request:
Query Name:
DNS Servers: 192.168.1.21

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

Remember this setting

Privatefirewall Alert - Outgoing Traffic 

APPLICATION CONTROL ENGINE


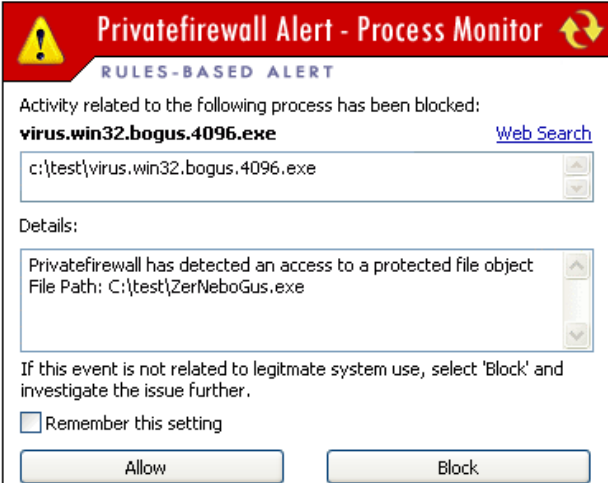
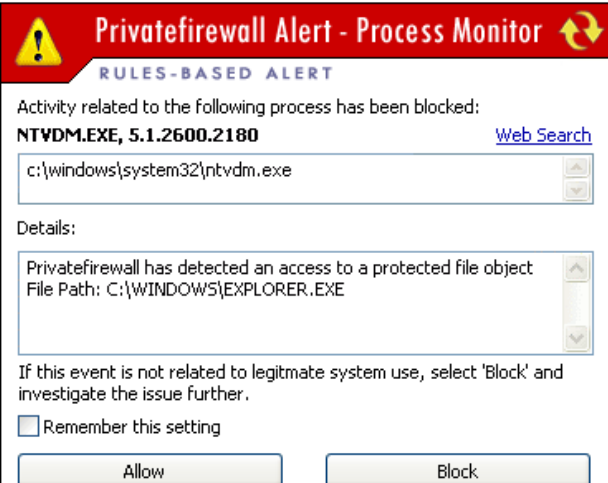
Access to the Network/Internet has been blocked for:
Trojan-PSW.Win32.LdPinch.gm.exe [Web Search](#)

C:\WINDOWS\Trojan-PSW.Win32.LdPinch.gm.exe

Details:

2/21/2006 1:51:36 PM PF has blocked outgoing TCP (6) packet from 192.168.1.212:2332 to 194.67.23.111:25 (smtp)

Remember this setting

<p>Trojan-PSW.Win32.PdPinch.gen</p>	<p>It steals confidential information from the victim machine, including files containing configuration details which contain passwords.</p>	<p>Have no known spreading routine.</p>	 <p>Privatefirewall Alert - Process Monitor</p> <p>RULES-BASED ALERT</p> <p>Activity related to the following process has been blocked: trojan-psw.win32.pdpinch.gen.exe Web Search</p> <p>c:\test\trojan-psw.win32.pdpinch.gen.exe</p> <p>Details: Privatefirewall has detected an attempt to open a foreign process Target PID: 0 Image Name: [System Process]</p> <p>If this event is not related to legitimate system use, select 'Block' and investigate the issue further.</p> <input type="checkbox"/> Remember this setting <p>Allow Block</p>	<p>Attempt to open a foreign process</p>
<p>Virus.Win32.Bogus.4096</p>	<p>It is a silly nonmemory resident depending Win32 virus. It gets the first .EXE file in the current directory, moves 4Kb of file header to the end of the file and overwrites file header with its own code. If the first file in directory is already infected, the virus does not infect more files. To run the host file the virus disinfects it to the temporary file with the "ZerNeboGus.exe" name.</p>	<p>Have no known spreading routine.</p>	 <p>Privatefirewall Alert - Process Monitor</p> <p>RULES-BASED ALERT</p> <p>Activity related to the following process has been blocked: virus.win32.bogus.4096.exe Web Search</p> <p>c:\test\virus.win32.bogus.4096.exe</p> <p>Details: Privatefirewall has detected an access to a protected file object File Path: C:\test\ZerNeboGus.exe</p> <p>If this event is not related to legitimate system use, select 'Block' and investigate the issue further.</p> <input type="checkbox"/> Remember this setting <p>Allow Block</p>	<p>Attempt to access protected file object</p>
<p>Virus.DOS.Trivial.Seneca.381</p>	<p>It is a very dangerous non-memory resident parasitic virus. Being executed it searches for .EXE files and overwrites them. On November, 25th it displays some text then erases the sectors of the current drive.</p>	<p>Have no known spreading routine.</p>	 <p>Privatefirewall Alert - Process Monitor</p> <p>RULES-BASED ALERT</p> <p>Activity related to the following process has been blocked: NTVDM.EXE, 5.1.2600.2180 Web Search</p> <p>c:\windows\system32\ntvdm.exe</p> <p>Details: Privatefirewall has detected an access to a protected file object File Path: C:\WINDOWS\EXPLORER.EXE</p> <p>If this event is not related to legitimate system use, select 'Block' and investigate the issue further.</p> <input type="checkbox"/> Remember this setting <p>Allow Block</p>	<p>Attempt to access protected file object</p>

<p>Virus.Win32.Perrun.a</p>	<p>Perrun is non-memory resident parasitic Win32 virus. When the virus runs it searches for all *.JPG files in the current directory and appends its code to the end of the files (resulting in EXE virus code at the end of affected JPEG files).</p>	<p>Have no known spreading routine.</p>	 <p>Privatefirewall Alert - Process Monitor </p> <p>RULES-BASED ALERT</p> <p>Activity related to the following process has been blocked: NTVDM.EXE, 5.1.2600.2180 Web Search</p> <p>c:\windows\system32\ntvdm.exe</p> <p>Details:</p> <p>Privatefirewall has detected an access to a protected file object File Path: C:\WINDOWS\EXPLORER.EXE</p> <p>If this event is not related to legitimate system use, select 'Block' and investigate the issue further.</p> <p><input type="checkbox"/> Remember this setting</p> <p><input type="button" value="Allow"/> <input type="button" value="Block"/></p>	<p>Attempt to access protected file object</p>
------------------------------------	--	---	---	--