

# Outpost Firewall Pro 2.5 vs Leak Tests

*This document describes how Outpost Firewall Pro 2.5 scores on the better-known leak tests*

One of the major areas of firewall protection is outbound filtering, which is used to control all outgoing activity and to block malicious programs such as Trojans, spyware, and adware when they try to connect to a remote address. Most firewall users are confident in their firewall and do not consider that its outbound filtering can be bypassed. To check the efficiency of this personal firewall feature several security experts created leak tests, which simulate and imitate Trojans, to demonstrate (without damaging to your data) that it is possible to bypass a firewall's protection. Leak tests are simply programs that show just how well protected a computer is in terms of its outgoing network connections.

As shown below, Outpost Firewall Pro 2.5 passes all known leak tests even with "out of the box" settings making your system effectively protected from the intrusion right after being installed.

## Threats and Methods of Penetration

There are several methods of penetration and each leak test uses one or more techniques to demonstrate a firewall's vulnerabilities.

### **Substitution**

This program technique tries to rename itself with the name of an existing trusted application and to put itself into the same folder as the trusted app. This bypasses those firewalls that rely on application filenames but not on application checksums.

### **Launcher**

This method accesses the Internet by launching a trusted application and giving it command line parameters. The firewall considers that this is the trusted application that requests access to the network and allows the connection.

Although this is not a firewall failure per se (detecting when a process requesting network access is launched by another process), Outpost Firewall Pro 2.5 correctly handles these situations and prevents unauthorized activity of malicious processes trying to access the network using trusted applications.

### **DLL injection**

This method uses a trusted process to load a malicious DLL file. After it's loaded, the DLL code becomes a part of the trusted process and can transmit any private data over the network while the firewall attributes the activity to the trusted process. This technique is often used by Trojans.

### **Timing attack**

When detecting an unauthorized network request, most firewalls freeze the requesting process and prompt the user whether or not to block the request. To freeze the process, the PID (process identifier) is required. Programs that use this timing attack technique transmit the data erratically, changing the PID after each portion of data is sent.

### **Default rule using**

Many firewalls have a set of pre-defined default rules designed so the firewall does not totally block all access to the network after it is installed. Malicious programs can take advantage of these rules to bypass the firewall.

### **Direct network interface reaching**

All network traffic in Windows operating systems, by default, use the Winsock TCP/IP stack layer. But some programs can use the lower layers of a Windows network stack and even communicate directly with a network interface and thus bypass the firewall.

### **Process memory injection**

This method of attack is one of the hardest to detect. A process generally consists of many threads, which speed up process execution. A malicious program can inject a new thread that executes its own code into the threads of a trusted process or, which is even harder to detect, use an existing thread and modify its code to access the Internet. No DLL is loaded, which makes this kind of attack very hard to detect.

### **Recursive request**

Some malware use a system service to perform network access instead of attacking or modifying a trusted application.

# Outpost Firewall Pro 2.5 Security Features

This document uses information from [www.firewallleaktester.com](http://www.firewallleaktester.com):

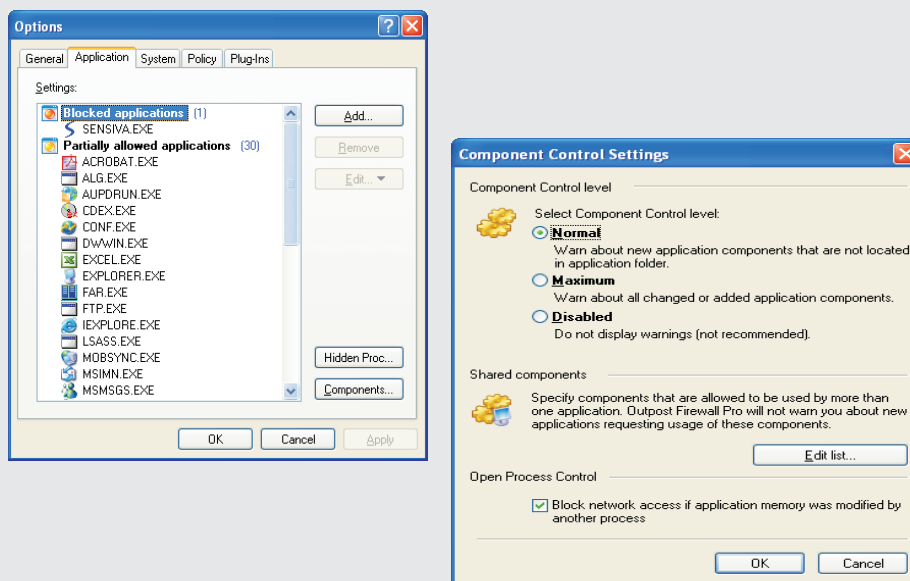
Providing network security is the core function of any firewall. Firewall programming has to stay a step ahead of possible new dangers so users can be confident that their systems are well protected. Outpost Firewall Pro 2.5 is a fortress with an unsurpassed record of withstanding new attacks.

The following Outpost Firewall Pro 2.5 features provide overwhelming protection against every attack technique, showing no weakness to each leak test making it a rock solid defense for your system.

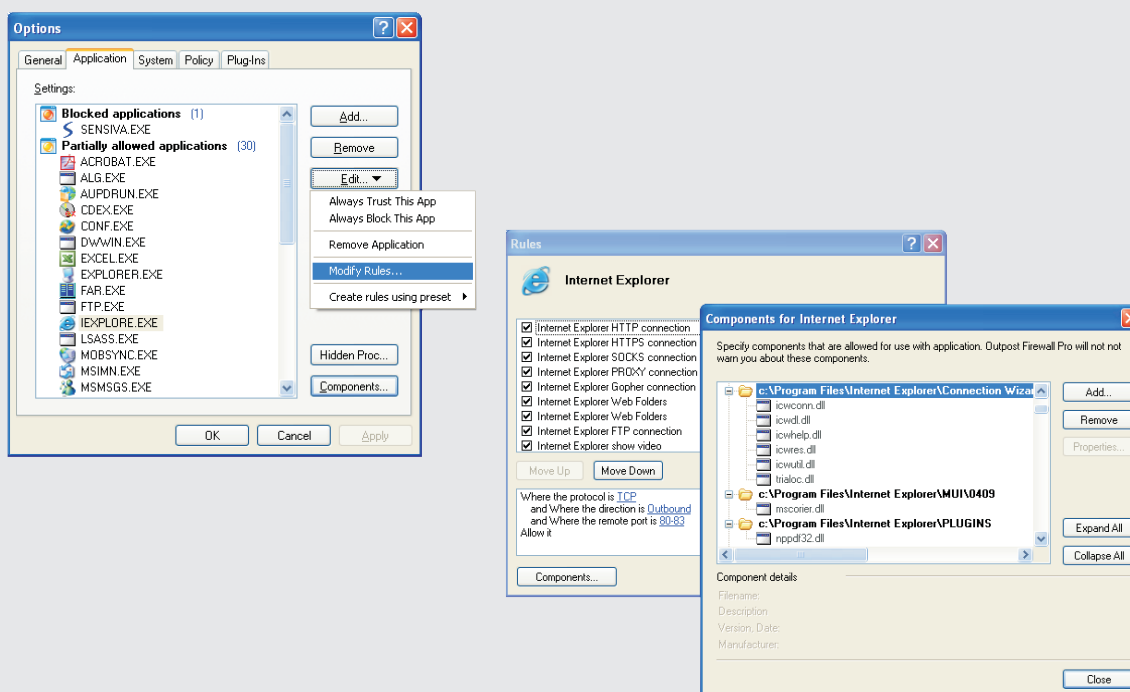
By employing technologies of Component Control, Hidden Process Control, and Open Process Control Outpost Firewall Pro 2.5 does not allow malicious applications to be activated as parts of legitimate programs and thus fully protects you from Trojans, spyware and other dangers.

## Component Control

Outpost Firewall Pro 2.5 not only monitors applications, but it also monitors each component of each application. When a module of an application is changed and that application tries to establish a connection, Outpost Firewall Pro 2.5 will ask you whether it should be allowed. The purpose of this Component Control is to make sure that components are not fake or malicious. Some Trojan horses can be inserted as modules of legitimate applications (your browser, for example, has many separate parts) and thus gain the privileges needed to go online. Outpost Firewall Pro 2.5 allows you to choose the Component Control level you want by clicking the Components button on the Applications tab of the Options dialog window:



You can also view the components Outpost Firewall Pro 2.5 monitors for each application by selecting the application from the list, selecting Edit > Modify Rules and clicking the Components button:



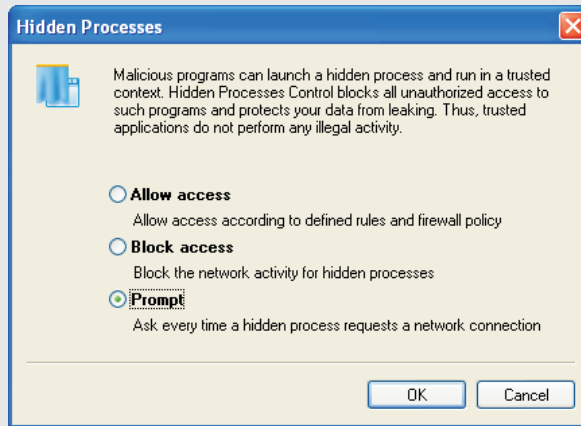
### Hidden Process Control

Several network-enabled applications do not directly access the network. Instead they spawn child processes that act on their behalf in a hidden window. This allows these applications to bypass traditional firewalls because the process is not treated as a part of the application, so firewall security restrictions do not apply to that process. Moreover, the process is hidden from the user so it is not possible to track what actions it does perform.

On one hand, this technology is used by ordinary applications (like Microsoft Internet Explorer) to perform routine maintenance operations (like update checks) in a more user-friendly manner; on the other hand, a malware program can take advantage of this technique to send out a user's private information or perform other covert activities.

Outpost Firewall Pro 2.5 lets you control hidden processes as well as processes that are ran on behalf of a trusted application, so they cannot perform inappropriate activity.

To configure how Outpost Firewall Pro 2.5 should treat such processes, open the Application tab of the Options dialog, click Hidden Proc, and select the desired policy for hidden processes:

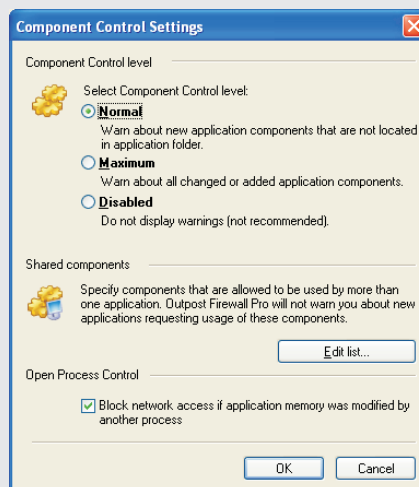


### Open Process Control

Several Trojan horses and viruses use sophisticated techniques that let them alter the code of trusted applications running in memory and so bypass your system's security perimeter to perform their malicious activities. This is known as code injection or copycat vulnerability.

Outpost Firewall Pro 2.5 controls these functions that are used to inject malicious code into a trusted application's memory space and so prevents rogue processes from employing this maneuver.

To enable process memory control, open the Component Control Settings dialog and select Block network access if application memory was modified by another process:



## Outpost Firewall Pro 2.5 vs. Leak Tests

This section contains a description of each of the better-known leak tests and Outpost Firewall's behavior in its blocking.

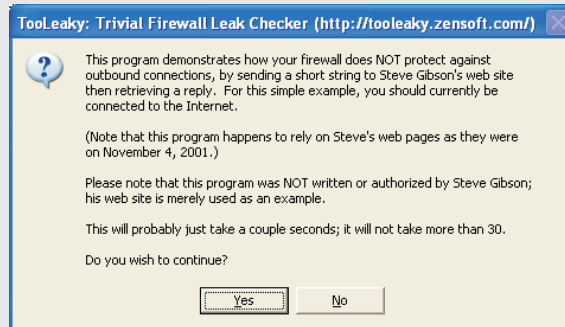
### TooLeaky by Bob Sundling

<http://www.tooleaky.zensoft.com> Launcher

Tooleaky opens your default web browser with the following command line:

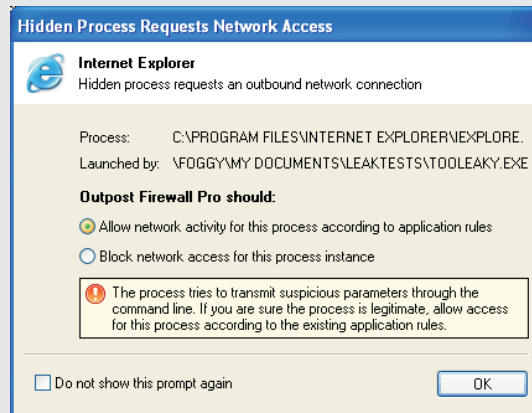
```
ieexplore.exe http://grc.com/lt/leaktest.htm?PersonalInfoGoesHere
```

The launched window is hidden. If the web browser is allowed to access HTTP port 80, all data will be able to be transmitted to any remote address. This information could be a password or credit card number sent by a very real malicious program.



If the test succeeds, it means your firewall has failed; it doesn't check applications that launch other apps.

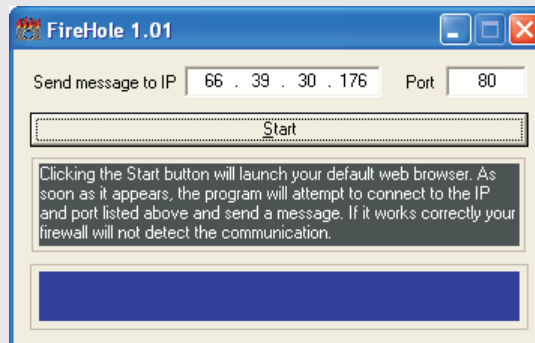
Outpost Firewall Pro 2.5 detects this activity and displays a dialog box prompting you to decide if the application should be allowed to access the Internet:



### FireHole by Robin Keir

<http://www.keir.net/firehole.html> Launcher, DLL injection

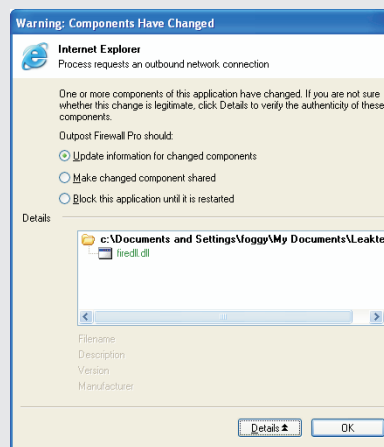
FireHole uses the default web browser to transmit data to a remote address. To do this, it installs a DLL file (with an intercept function built-in) onto the user's computer. This DLL loads itself into the same process space as a trusted application, so FireHole can access the Internet silently.



If the test succeeds, it means your firewall doesn't control applications that try to access the network by launching another app, and is also vulnerable to DLL injection.

If the test fails, it means your firewall controls process spawning, but this does not always mean that your firewall is invulnerable to DLL injection.

Outpost Firewall's Component Control technology detects if some application tries to modify a trusted application (such as Internet Explorer):



### WallBreaker by Guillaume Kaddouch

<http://www.firewallleaktester.com/> Launcher

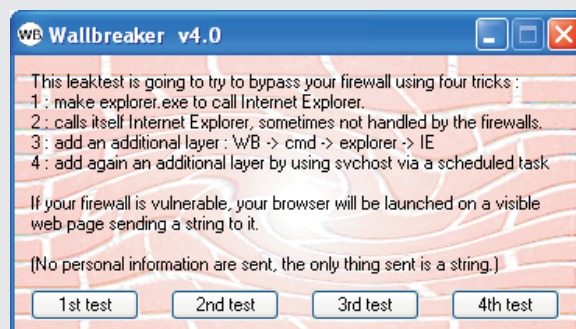
This leak test reveals the level of your firewall's launch checking capabilities. It consists of four independent tests.

The first test uses explorer.exe to launch iexplore.exe and then to access the Internet, so, it looks like a Windows application that legitimately launches another app, rather than WallBreaker that launched it. Some firewalls can detect applications trying to directly access the Internet or applications launching other ones to access the Internet, but they cannot detect WallBreaker, which launches an application that launches another app.

The second test simply launches Internet Explorer directly, but in a way that is not handled by some firewalls.

The third test is a variant of the first test. It launches cmd.exe first, which then launches explorer.exe, and finally iexplore.exe: Wallbreaker -> cmd -> explorer -> iexplore (Win 2000/XP only). It shows that a malicious program can try to hide by adding layers before accessing the Internet.

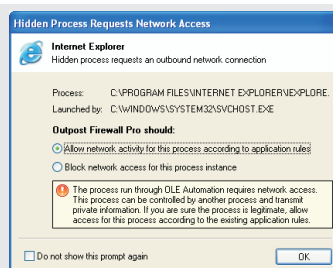
The fourth test is an extension of the third one. Wallbreaker sets a scheduled task by using Windows Task Scheduler (AT.exe) which in turn will execute the task via svchost: Wallbreaker -> AT -> svchost -> cmd -> explorer -> iexplore (Win 2000/XP only). This test creates a batch file with a random filename in his directory; it should be manually deleted by the user at the end of the test. In order for this test to work, the Windows Task Scheduler service must be started (keep in mind that a real Trojan could do it by itself).



If the test succeeds, i.e. your firewall does not warn you that WallBreaker.exe is trying to access the Internet; your firewall lacks this launch checking capability.

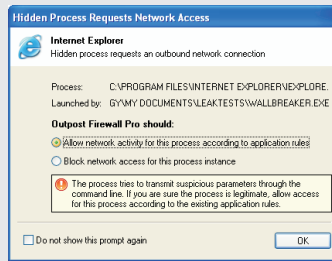
Outpost Firewall Pro 2.5 detects every situation where a process launches other applications in order to access the network whether they run through OLE Automation or use other technologies.

#### First test:



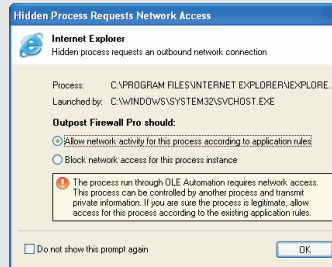
The explorer.exe uses svchost.exe to launch iexplore.exe and Outpost Firewall Pro 2.5 detects this.

## Second test:



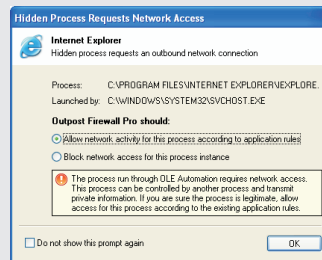
In this test Outpost Firewall Pro 2.5 detects WallBreaker.exe launching *ieplorer.exe* and transmitting a URL to it.

## Third test:



As in the first test case, explorer.exe launches *ieplorer.exe* through svchost.exe giving it a URL as a parameter.

## Fourth test



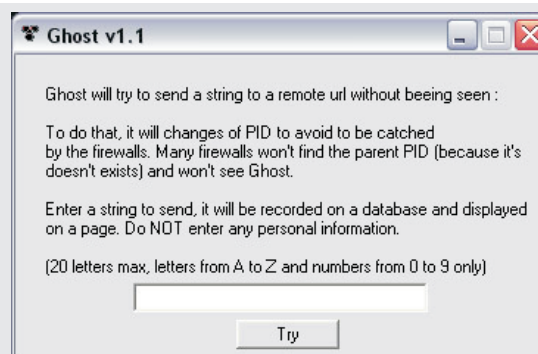
The same as in the third test.

## Ghost by Guillaume Kaddouch

<http://www.firewallleaktester.com/> Launcher, Timing attack

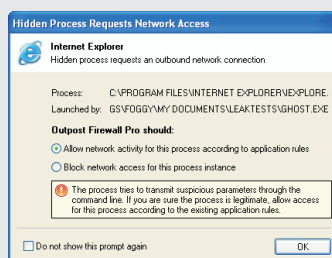
This test reveals whether your firewall's "parent/child network access monitoring" detects in time that an executable is launching another app to access the Internet.

Generally, when an application accesses the Internet, a firewall uses the Windows API to retrieve the parent's (the executable which launched the trusted application) PID and name and freezes it to ask you what it should do (whether to allow or deny the communication). To prevent being seen, Ghostonce it has been given the information to send to the default browser changes the PID by shutting itself down and restarting to continue to send data. It just tries to reach a web page and send a string to it. The page reached could receive your credit card number, for example.



If *Ghost.exe* is seen and is apparently frozen but the page is loaded, it means that your firewall's "parent/child network access monitoring" is good, but it checks too late. If no information can be sent, and no page is loaded at all, and *Ghost.exe* is detected by the firewall, you have a strong "parent/child network access monitor".

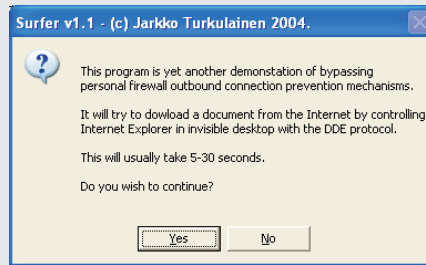
Outpost Firewall Pro 2.5 correctly detects the parent process names and prevents the sending of *any* information.



## Surfer by Jarkko Turkulainen Launcher

This test reveals whether your firewall checks the Direct Data Exchange (DDE) inter-process protocol and if its parent/child monitoring is strong enough.

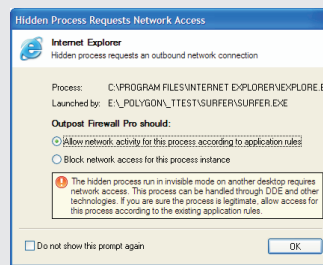
Many firewalls now catch the direct ShellExecute or CreateProcess while calling Internet Explorer and giving it parameters. To avoid that, Surfer creates a hidden desktop and launches IE inside it with no URL, therefore with no network access. It then launches another instance of itself and closes the first one. Then it uses the DDE protocol to provide parameters to IE and not via a direct call while launching IE.



If the test succeeds, it means your firewall does not check the DDE inter-process protocol or that its parent/child monitoring is too weak.

(Note that DDE could be used on an already running IE instance. It would just be less stealthy this way, but possible.)

Outpost Firewall Pro 2.5 correctly detects situations when a process is run in another desktop and blocks such activity.



## LeakTest by Steve Gibson

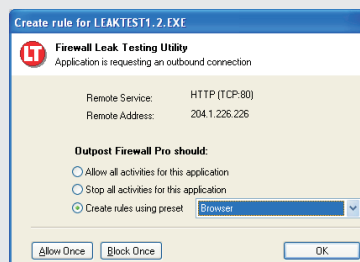
<http://www.grc.com/lt/leaktest.htm> Substitution

This is one of the first leak tests. It is based on the fact that some firewalls trust only trusted applications that are defined by the user. The test demonstrates that renaming a malicious program to the name of an authorized application allows the malware to bypass a firewall. Recent versions of personal firewalls include an application checksum and warn the user if it has been modified.



LeakTest attempts to establish a standard TCP connection to HTTP port 80 of the main grc.com web server at Gibson Research Corporation. After achieving a connection, data transfer permission is verified and the connection is terminated. If the test succeeds, it means your firewall trusts your applications by their names instead of an encrypted fingerprint.

Outpost Firewall Pro 2.5 validates the application checksum, detects unauthorized activity and requests if it should allow the application to access the network:



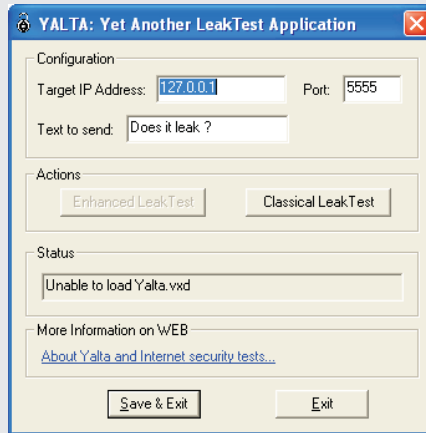
## YALTA by Soft4Ever

[http://www.soft4ever.com/security\\_test/En/index.htm](http://www.soft4ever.com/security_test/En/index.htm)

Default rule using, Direct network interface reaching

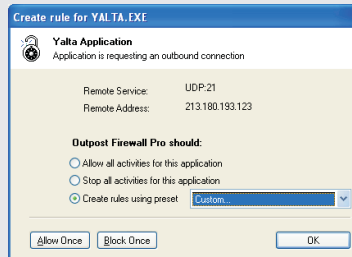
Testing with YALTA, you see how Trojans can try to transmit data from your computer to the Internet. This checks if your personal firewall can detect these.

YALTA consists of two tests: a classical test, and an advanced test. The classical test tries to send UDP packets to generally allowed ports like 53 (DNS), 21(FTP), etc. The advanced test uses a driver to send packets directly to the network interface below the TCP/IP layer (Windows 9x/Me only).



If the test succeeds, it means your firewall allows many kinds of traffic on pre-configured ports.

Outpost Firewall Pro 2.5 detects unauthorized outbound connections and can prevent them:

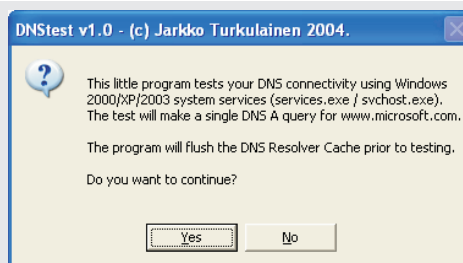


## DNSstester by Jarkko Turkulainen

<http://www.klake.org/~jt/dnshell/> Recursive request

By default on all NT type operating systems since Windows 2000, a Windows service DNS Client is running and handles all DNS requests. Thus, all DNS requests coming from applications are transmitted to the DNS Client service (svchost.exe under Windows XP) that will perform the DNS request.

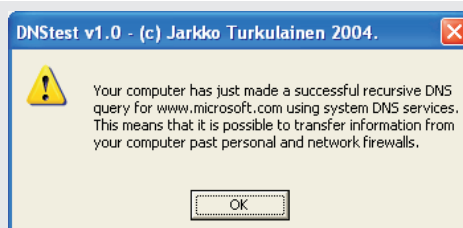
This behavior can be used to transmit data to a remote computer by crafting a special DNS request without the firewall noticing it. Indeed, the DNS Client service must be allowed to access the Internet. DNSstester uses this kind of DNS recursive request to bypass your firewall.



If the test succeeds, it means your firewall checks DNS requests too late (when they're about to go out the computer) so it just sees the DNS Client service and not the leak test process.

If the test fails this test your DNS Client service is probably disabled.

No personal firewall, including Outpost Firewall Pro 2.5 passes this test, but this is not a concern since this technique has never been used by any spyware or Trojan program.



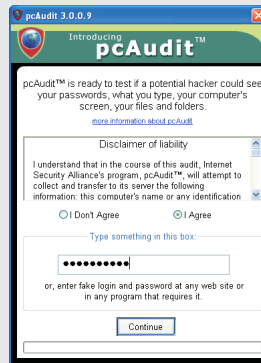
Nevertheless, to strengthen the security of your system, you can disable the DNS Client service by using the Services snap-in. In this case the technique will fail. In this case, however, you should create a rule for each application that requires DNS access.

## pcAudit by Internet Security Alliance

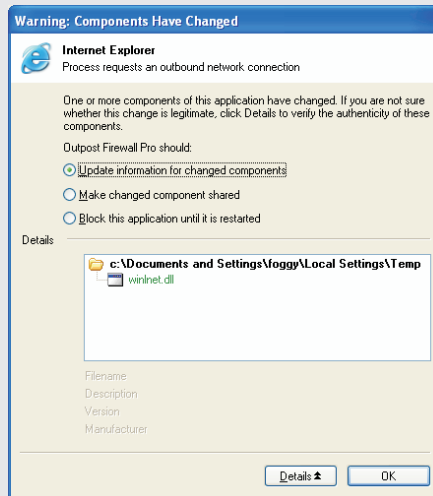
<http://www.pcinternetpatrol.com/> DLL injection

PCAudit uses DLL injection to insert its code (as a DLL) into an authorized application instead of launching it directly. If the trusted application has full access, PCAudit will freely go through.

To test PCAudit correctly, answer "Always" if your firewall warns you that explorer.exe tries to access the Internet. Then try again and if your firewall does not show you an alert, it means that it is vulnerable to DLL injection.



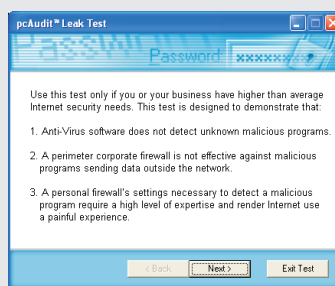
Outpost Firewall's Component Control blocks all such unauthorized activity:



## pcAudit2 by Internet Security Alliance

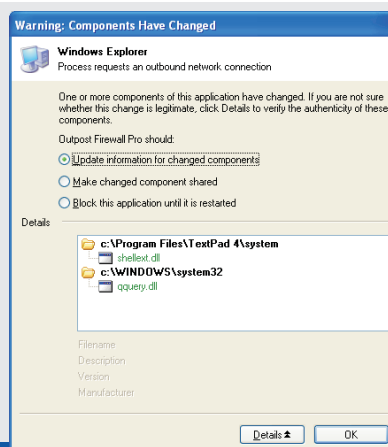
<http://www.pcinternetpatrol.com/> DLL injection

PCAudit V2 uses a different way than its previous version to bypass DLL protection on a personal firewall, which can successfully block the first version of PCAudit.



If the test succeeds, it means that either your firewall is vulnerable to DLL injection or has a DLL injection protection feature but it's not adequate.

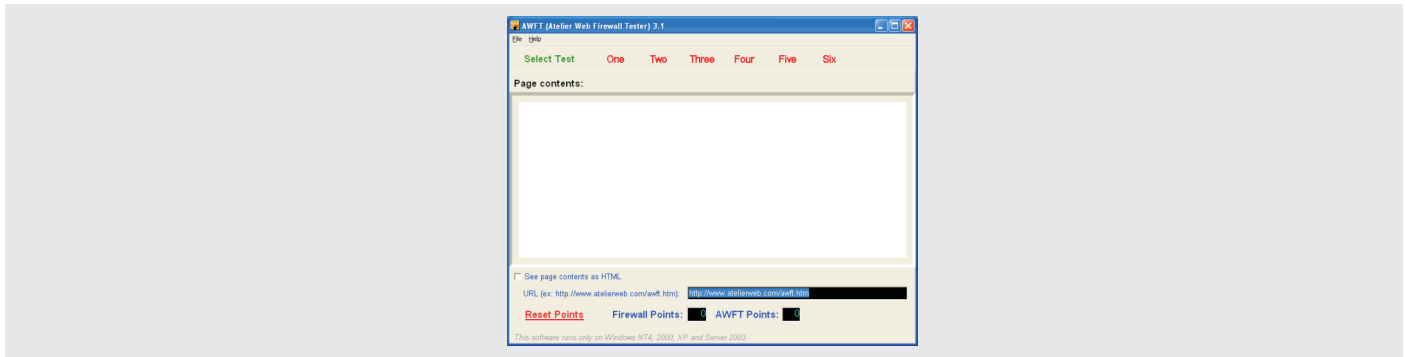
Outpost Firewall Pro 2.5 is undaunted by this form of attack and remains on guard protecting your system:



## Atelier Web Firewall Tester (AWFT) 3.1

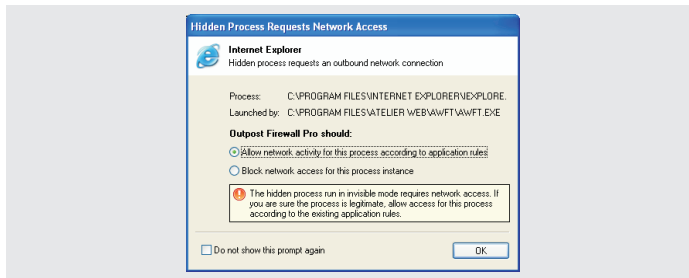
<http://www.atelierweb.com/awft/> Process injection

AWFT offers six tests that enable you to give a score (max 10) to your firewall.

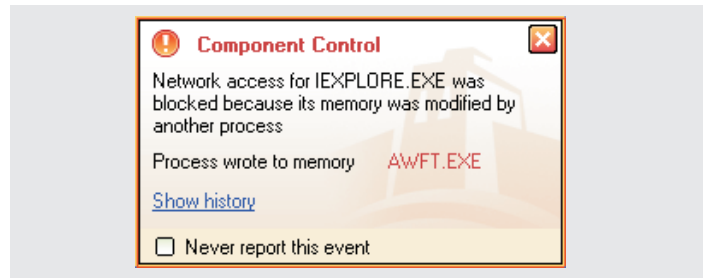


As shown below, Outpost Firewall Pro 2.5 takes the full 10 points.

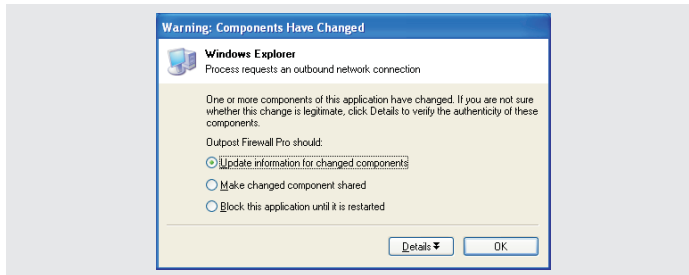
1. The first test attempts to load a copy of the default browser and patch it in memory before it executes.



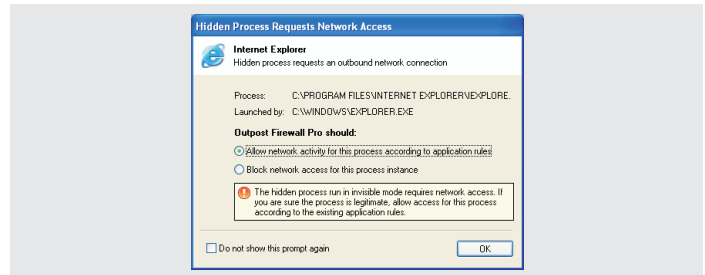
2. The first test attempts to load a copy of the default browser and patch it in memory before it executes.



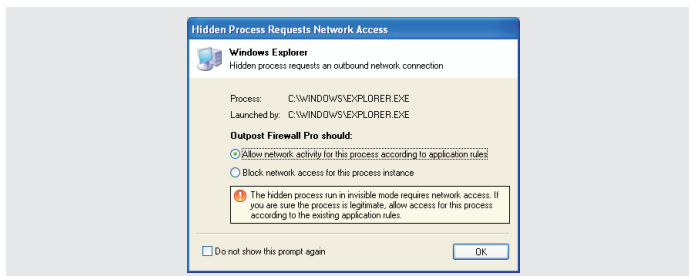
3. The third creates a thread on Windows Explorer.



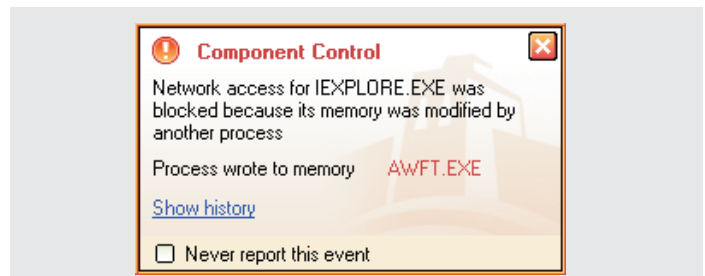
4. The fourth attempts to load a copy of the default browser from within Windows Explorer and patch it in memory before execution. It defeats firewalls that require authorization for an application to load another one (Windows Explorer is normally authorized). This test usually succeeds, unless the default browser is blocked from accessing the Internet.



5. The fifth test performs a heuristic search for proxies and other software authorized to access the Internet on port 80, loads a copy and patches it in memory before execution from within a thread on Windows Explorer. This is a very difficult test for most personal firewalls.



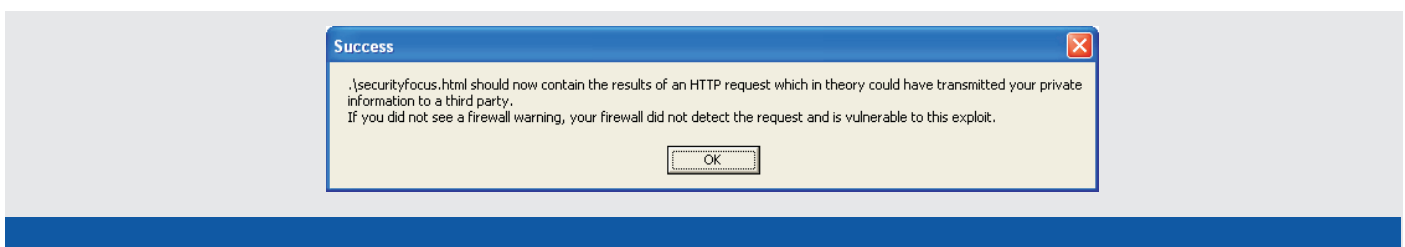
6. The sixth performs a heuristic search for proxies and other software authorized to access the Internet on port 80, requests the user to select one of them, then creates a thread on the selected process. This is another difficult nut to crack for personal firewalls.



## Thermite by Oliver Lavery

Download link: <http://www.firewallleaktester.com/leaks/thermite.exe> Process memory injection

Thermite, unlike other leak tests that inject their code into another process via DLL's, injects its code directly into the target process, by creating an additional malicious thread within that process. It is totally invisible to some personal firewalls.



If the test succeeds, it means your firewall is vulnerable to process memory injection.

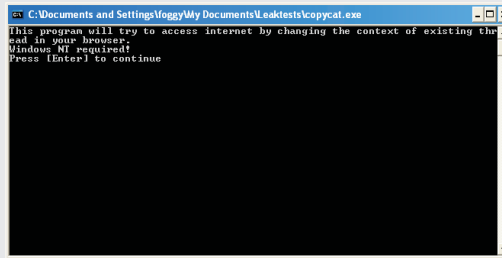
Outpost Firewall's Component Control feature detects such code injection:



### CopyCat

Download link: <http://mc.webm.ru/copycat.exe> Process memory injection

Like Thermite, CopyCat uses direct code injection (without creating an additional thread) into a web browser to prevent being caught by the firewall.



If the test succeeds, it means your firewall is vulnerable to process memory injection.

Outpost Firewall's Component Control feature detects such code injection:



## Conclusion

Leak	TestTechnique	OFP 2.5	OFP 2.1	Outpost Free 1.0	Windows XP Firewall (Sp2)
TooLeaky	Launcher	+	+	-	-
FireHole	Launcher, DLL injection	+	+	-	-
WallBreaker	Launcher	+	-	-	-
Ghost	Launcher, Timing attack	+	-	-	-
Surfer	Launcher	+	-	-	-
LeakTest	Substitution	+	+	+	-
YALTA	Default rule using, Direct network interface reaching	+	-	-	-
DNSStester	Recursive request	?	?	?	?
pcAudit	DLL injection	+	+	-	-
pcAudit2	DLL injection	+	-	-	-
Atelier Web Firewall Tester (AWFT)	Process injection	+ (10/10)	- (5/10)	- (0/10)	- (0/10)
Thermite	Process memory injection	+	-	-	-
CopyCat	Process memory injection	+	-	-	-

As shown above, Outpost Firewall Pro 2.5 passes all known leak tests. With Outpost Firewall, you can be certain that you are protected and need not worry about anyone being able to download or steal your personal information. However, you should keep in mind that progress does not stand still and new techniques can appear that will bypass your strongest protection. That's why it is always very strongly recommended that you keep your firewall software up to date so it addresses the most recent threats and dangers.

? To strengthen the security of your system, you can disable the DNS Client service by using the Services snap-in. In this case the technique will fail. However, you should create a rule for each application that requires DNS access.