



Information Leak Prevention in Outpost Firewall Pro 4.0

A Guide to Leak Tests

Table of contents

Document overview.....	3
Document design	3
Security is a multi-layered concern	3
Tools used to test the firewall's vigilance.....	5
New data protection functionality in Outpost Firewall Pro 4.0	6
Leak tests overview.....	6
Ways to leak information	6
Now it's time for the leak tests themselves	8
Leak test #1 "Firewall Leakage Tester"	9
Leak test #2 "TooLeaky"	10
Leak test #3 "WallBreaker"	11
Leak test #4 "Ghost"	12
Leak test #5 "YALTA"	13
Leak test #6 "DNSTester"	14
Leak test #7 "FireHole"	15
Leak test #8 "pcAudit"	16
Leak test #9 "Comodo Parent Injection Leak Test".....	17
Leak test #11 "Copycat"	19
Leak test #12 "Atelier Web Firewall Tester"	20
Leak test #13 "Surfer"	21
Leak test #14 "PCFlank Leaktest"	22
Leak test #15 "Breakout"	23
Leak test #16 "MBtest"	24
Leak test #17 "OutBound"	25
Leak test #18 "Jumper"	26
A little background from Agnitum	27
Conclusion.....	27
About Agnitum.....	27
Contacts.....	27

Document overview

Outpost Firewall Pro 4.0 is the first personal firewall to offer anti-leak technology that passes all known leak-tests and is specifically designed to prevent malware programs from transmitting information out of a protected computer by hijacking a trusted application's access permissions.

This document focuses on the all-encompassing protection provided by Outpost Firewall Pro 4.0 to prevent personal and confidential information from leaking out of your PC into the hands of hackers and cyber criminals. Real-world examples show that Outpost Firewall Pro 4.0 passes all recognized third-party leak tests, providing significant additional security for Internet-connected PC users.

Document design

This document contains all the information home computer users need to understand system security, particularly firewalls, and how third-party tools are used to measure the reliability of firewalls in protecting users against information leakage.

The document is divided into three parts:

1. The first part provides an overview of the current security situation for Windows-based computers, the role and functionality of personal firewalls, and how Outpost Firewall Pro differs from other personal firewalls.
2. At the heart of the document are the results of a series of leak tests applied to Outpost Firewall Pro, which are designed to verify the firewall's outbound filtering capabilities. Each set of test results is accompanied by graphical explanations and a short commentary written in everyday, non-technical language.
3. The final part of the document is a short interview with Agnitum's Chief Software Architect Alexey Belkin, who shares his views on what influenced his decision to incorporate this strong anti-leak protection into Outpost Firewall Pro 4.0.

Security is a multi-layered concern

We all have valuable information stored on our PCs, so it's important to consider how to protect that information reliably. The Internet is rife with malware designed to steal personal information—like passwords, bank account details, and other confidential data without the user's knowledge—and 'phone home' that information to hackers and other cyber criminals.

The vulnerability of this information means it is vital computer users be able to control how and what information is allowed to be transmitted off the computer; they should be able to safeguard outbound connections so that no unauthorized data transfers can be made.

While anti-virus and anti-spyware programs can detect and remove malware programs downloaded from the Internet to a PC, a firewall serves a broader purpose. Firewalls prevent malicious programs from connecting to the Internet, serving as a virtual checkpoint for data in transit and permitting only authorized connections. Even if a virus or spyware has found its way onto the user's computer, the firewall can prevent that piece of malware from communicating or propagating out of the infected machine. Both anti-virus and anti-spyware depend to an extent on timely signature updates to recognize new threat patterns, so the malware creators are always in the driver's seat. The firewall is there to protect computers from damage by new malware threats while the anti-virus and anti-spyware vendors are preparing their updates.

Windows XP, especially with Service Pack 2 applied, provides fairly robust protection—the security upgrade has helped eliminate many of the loopholes previously exploited by malware to compromise systems, and its built-in firewall has been upgraded to better address new threats. Unfortunately, these implementations are not enough to counter the security holes in the operating system itself.

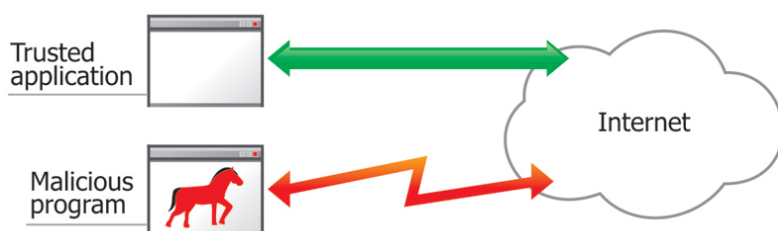
Firstly, the Windows XP firewall lacks protection for outbound connections—every outgoing data transfer is presumed safe and allowed by default—which is not always a safe assumption to make, as has been corroborated by the recent surge in spyware, backdoor programs, botnet activity, and other threats to

the security of information stored on Windows XP systems.

Secondly, Windows XP is designed and constructed in such a way that it allows one program installed on the computer to unrestrictedly communicate, exchange data and share internal components with other programs, assuming total legitimacy. For example, by clicking a hyperlink in e-mail, the default browser is started and the specified link opened; this happens automatically, with no need to launch the browser manually and enter the URL. Of course, this makes work easier, but at the same time, it lessens system security—a malware program can call and execute a legitimate application in exactly the same way, with no questions asked. Many third-party firewalls, as well as the Windows XP-bundled firewall, cannot detect such stealthy behavior and allow malware to use the computer's Internet connectivity.

Below are three scenarios showing the level of protection a computer would have with different firewall configurations:

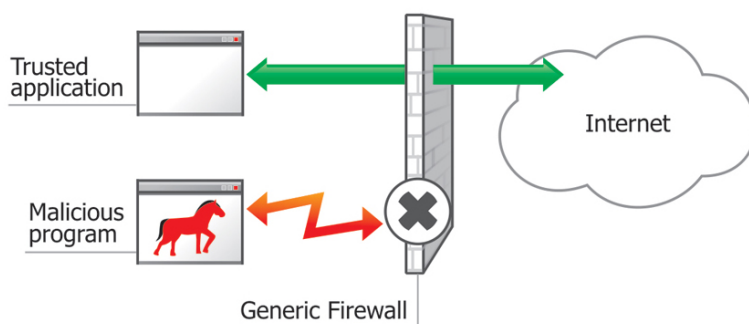
1. No firewall



Network and Internet access is allowed without restriction. Legitimate (green arrows) and unauthorized (red arrows) data are both permitted to enter and leave the computer freely. The computer's connections (ports) are exposed to any type of inbound or outbound access.

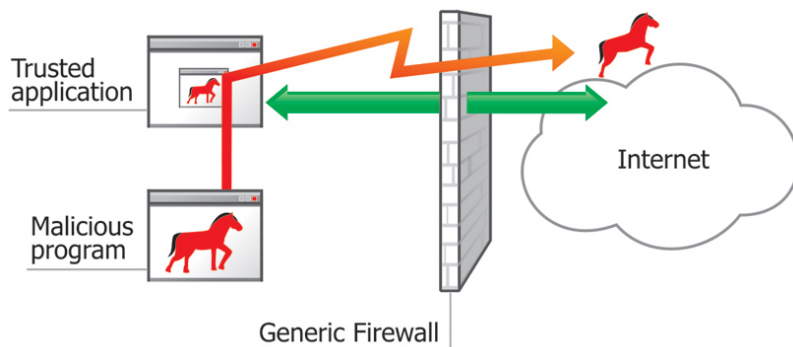
2. Windows XP or other basic firewall

a) Malicious programs cannot phone home data directly



This type of firewall performs basic filtering of outbound traffic; for example, it would detect and prevent attempts by malicious programs, such as Trojan horses, to phone home unauthorized information to a hacker. However, it would be unable to detect if that same malicious program infiltrated a trusted application and sent data off the computer using the latter's access permissions (see b) below).

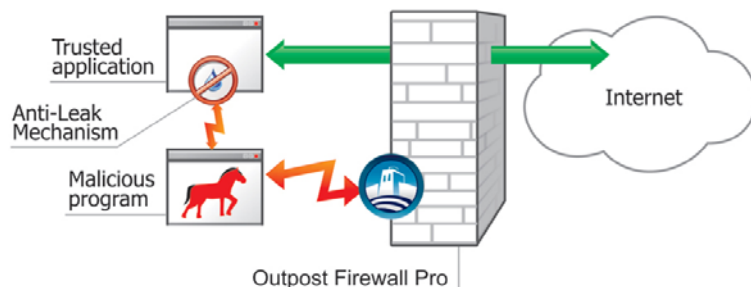
b) Malicious program succeeds in transmitting data by hijacking a trusted application's permissions



If the direct route is blocked by the firewall, the malicious program will next try to hijack a trusted application and use its credentials to transmit data off the machine, 'spoofing' the firewall.

Generic firewalls are unable to detect inappropriate inter-program communications and so would permit the malicious program to connect to the designated hacker site, resulting in personal information being compromised.

3. Outpost Firewall Pro



Outpost Firewall Pro's advanced anti-leak controls detect and prevent not just attempts by malware applications to send data off the machine directly. Outpost Firewall Pro v4.0 also monitors inter-application activity, ensuring that malware cannot use legitimate applications' credentials to transmit data off the PC.

Together, these two functions deliver multi-layered protection against malicious leakage of personal information.

Later, you'll find information on the kinds of techniques used by hackers to try to sneak data past the firewall's outbound defenses and how Outpost 4.0 protects users against each and every one of them.

Tools used to test the firewall's vigilance

As mentioned earlier, firewalls should be able to monitor programs for outbound activity. Even if a program tries to masquerade as another application that's been pre-configured with the firewall as "trusted", a competent firewall should be able to detect such application hijacking and prevent data from being transmitted off the PC in this way.

The information security community has developed special tools to test firewalls' ability to recognize unauthorized program interactivity and prevent malware programs from connecting to the network using legitimate programs' IDs. Called "leak tests", these software tools simulate an attempt by malware to send data off a PC so that the user can see how their firewall might respond to such a threat.

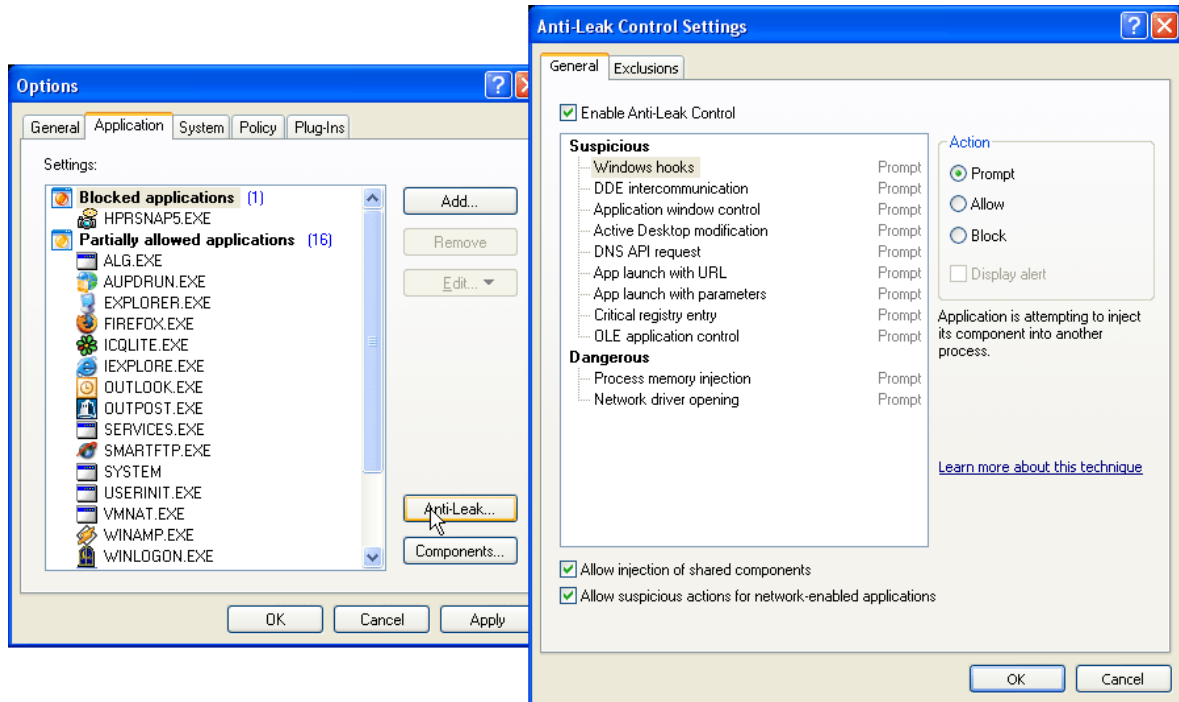
Leak tests use a variety of techniques and mechanisms to test a firewall's ability to prevent unauthorized outbound data transmissions; they are legitimate utilities that send only user-permitted information to isolated test locations and cannot damage the system.

Some people say that leak tests are not real-life situations and so are only proof-of-concept lab examples. However, because the techniques they use can and have been used by actual malware programs, they serve as a valuable indicator of a firewall's real ability to deal with outbound attacks.

New data protection functionality in Outpost Firewall Pro 4.0

Outpost 4.0 offers a number of improvements designed to make data theft a thing of the past, including a total of twelve new anti-leak features.

On the Application tab in Outpost's Options window, a new "Anti-Leak" box has been added where you can adjust the level of outbound protection against unauthorized behavior by applications:



Later, you'll see how these new additions work in the context of various leak tests to deliver Outpost's essential multi-layered protection to your PC.

Leak tests overview

A wealth of information on leak tests can be found at [Firewall Leak Tester](#) and [PC Flank](#). The number of leak tests is growing all the time, as are their proficiency and sophistication in the use of new techniques to try to get past the firewall. Firewall software developers such as Agnitum are constantly testing their products against current leak tests, in much the same way that a new car model's handling and performance is tested at a racetrack before going out to dealerships.

Although being able to pass all current leak tests is not a 100 percent guarantee that your firewall is bulletproof (there can be no guarantees in security), it is a good sign that it will be able to withstand determined attempts to steal data. As can be seen from the sites noted above, no single firewall has yet been able to pass all existing leak tests—until now. Outpost Firewall Pro v4.0 passes every single test without hesitation—a solid indication of its ability to keep hackers at bay.

But first, let's review the ways in which hackers might attempt to steal information from your PC.

Ways to leak information

As leak tests are based on various techniques (or a combination of them) to get information past the firewall's outbound defenses, this section provides a review of existing techniques and goes on to review all the leak tests in detail, noting in each instance how Outpost recognizes and counters the simulated attacks.

Leak technique #1 "Filename Substitution"

This approach is one of the easiest kinds of outbound attacks to beat. It involves a program renaming

itself to have the same name as that of a legitimate program on the computer and accessing the Internet while posing as a good program.

Leak technique #2 “Application launch with URL”

Programs using this technique start a separate Internet-accessing program (usually a web browser) with the URL of the site it is programmed to connect to. The process may occur in a hidden window to hide the activity from the user.

Leak technique #3 “Manipulation with trusted rules”

A rarely used but potent technique that involves one program exploiting the way the firewall processes access permission rules within the system. To do this, the test attempts to access ports labeled as trusted with the firewall and transmit unauthorized traffic through them.

Leak technique #4 “Spoofed DNS request”

DNS address resolution is used to direct an Internet-enabled application to a corresponding numeric IP address relating to the target remote server. It converts a user-supplied hostname address (e.g., www.agnitum.com) to an IP address so that the machine can understand the command and access the necessary site (e.g., 67.15.103.130). The technique of spoofed DNS request means that under the guise of a normal DNS request, sensitive data is communicated to a hijacked or illegal DNS server.

Leak technique #5 “Component injection”

This technique is used when a malware program launches another application on a computer and injects its internal component or a .DLL file into the target process. The injected component then requests the captured application to access the network, thus attempting to spoof the firewall.

Leak technique #6 “Process injection”

Similar to the process of injecting a component into a trusted program, a malware application can inject its entire contents into the memory block of a trusted application, opening up a new thread of the parent process and accessing the network with the trusted program’s credentials.

Leak technique #7 “DDE intercommunication”

This technique is used by one program to send commands to another (usually a browser) for the latter to process. Using the DDE procedure call, programs can manage and share content with each other. The DDE technique of application control in a leak test is used to check whether the firewall can recognize when one program uses DDE interaction to control the activity of an Internet-enabled application.

Leak technique #8 “Using OLE to control applications”

A relatively new idea, this approach uses the technique of OLE inter-program control (a short form of the Object Linking and Embedding command) in leak tests. OLE is a Windows mechanism that allows one program to manage the behavior of another program.

Leak technique #9 “Controlling applications’ windows through Windows messages”

One application can control other windows’ content and commands through Windows messages. Some leak tests use this technique to control the activity of web-enabled applications and access the network through them.

Leak technique #10 “Direct network interface access”

When the principle of direct network interface access is used, the test creates an additional network layer by injecting a corresponding device driver into the system and sends/receives traffic through this layer, bypassing the standard communication channels monitored by the firewall. This technique enables the leak test (or any other application) to send and receive data, complicating the process of data filtering through the firewall. It is a little complex under the Windows XP environment, as it requires some skill on the tester’s part to tweak the system configuration, but is a good test of a firewall’s robustness and flexibility.

Leak technique #11 “Access through Windows Active Desktop modification”

Leak tests can create an HTML page pointing to a certain website and set it as a Windows Active Desktop (AD). When the AD is turned on, it is permitted to go to the website address contained in the HTML

page, acting on behalf of the system and thus bypassing firewall's sensors.

Leak technique #12 "Modification of system registry"


The registry is a universal repository of system settings and program configurations. Modifying its content can lead to application errors or even system failure. Leak tests using this technique make small modifications to the registry elements, enabling an unverified process to unrestrictedly access the network, in spite of the presence of a firewall, by adding its components to the applications and acting on their behalf.

Now it's time for the leak tests themselves

Now we're going to put all the leak tests under the microscope, one by one, and examine how Outpost Firewall Pro 4.0 reacts. The leak tests are arranged in order of the technique they use, and a short commentary accompanies the results of each test.

Currently, there are eighteen leak tests and we've tested Outpost against all of them. Let's get started.

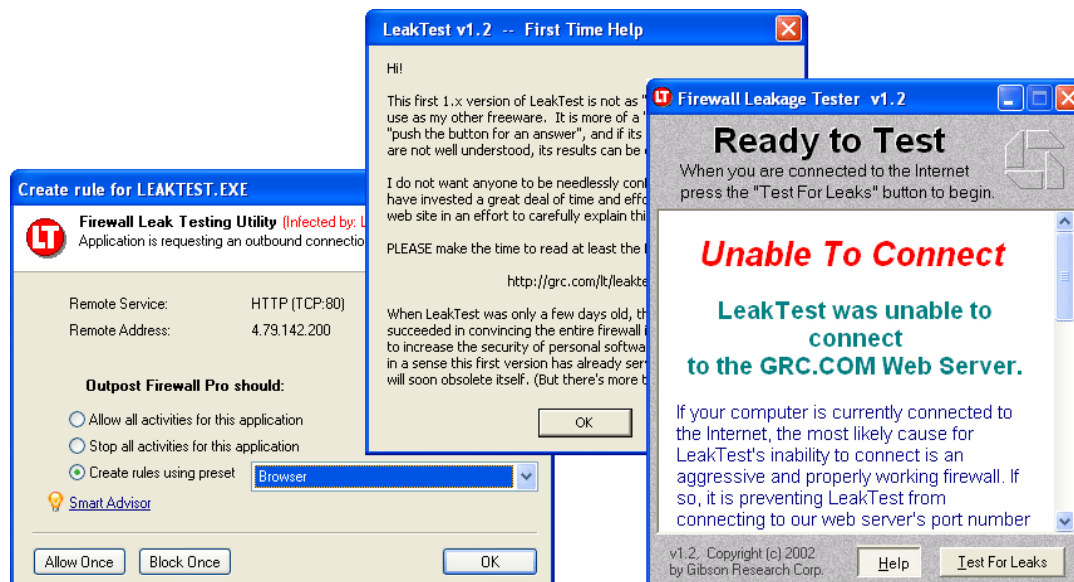
Leak test #1 "Firewall Leakage Tester"

Name/instant download link	Bypass technique used	Leaktest info/homepage	Outpost function used
Firewall Leakage Tester (Leak Test)	Filename substitution	 LeakTest.exe Firewall Leak Testing Utility Gibson Research Corp.	Fingerprint verification

This is an easy-to-pass leak test that uses the **filename substitution** technique to test the firewall.

The test tries to rename itself as one of the authorized programs on a computer (e.g., Internet Explorer) and establish an outbound connection with a remote server under the guise of that name. This test would defeat firewalls that rely solely on the file name to identify an application and do not perform a more thorough evaluation (e.g., fingerprint verification). Although it's a fairly easy test, some firewalls do fail it.

Here's how Outpost responds:





Outpost looks beyond a program's name to its unique identifiers or fingerprints. SHA256 is used to identify applications through updated presets, and MD5 identification is implemented to identify applications in active program rulesets, blocking the disguised program from connecting.

What this means for the user is that any malicious or unwanted application soliciting outbound access by trying to impersonate a legitimate application will be detected by Outpost and the user will be prompted to allow or disallow the connection.

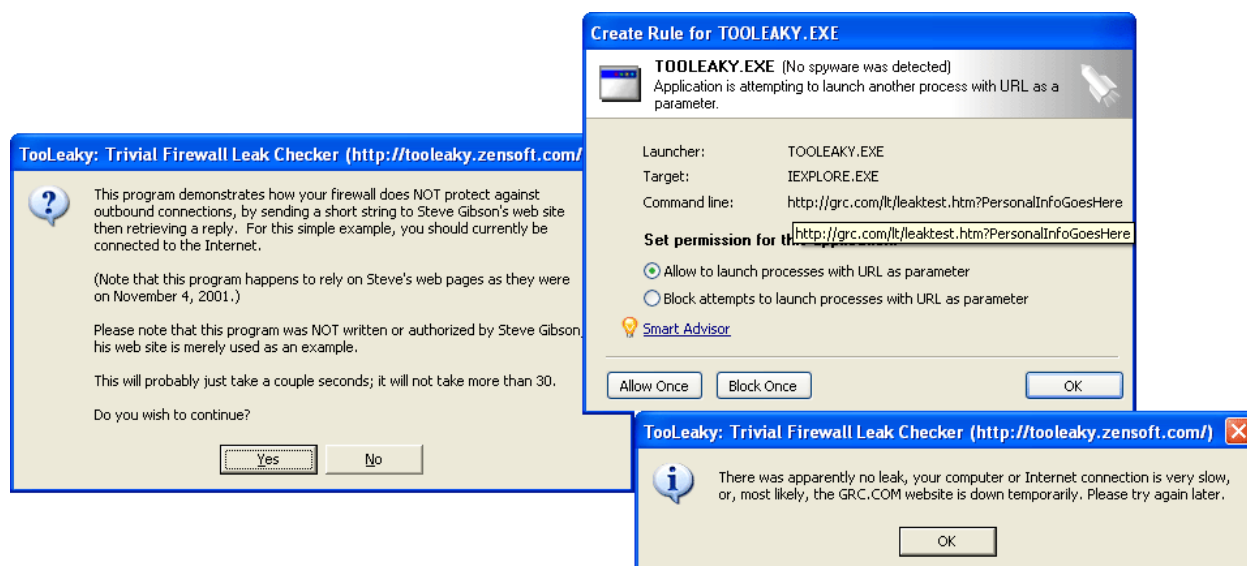


Leak test #2 "TooLeaky"

Name/instant download link	Bypass technique used	Leak test info/homepage	Outpost function used
TooLeaky	Application launch with a URL	 tooleaky.exe	"App launch with URL" 

This leak test is a slightly more advanced version of the previous test, in that it launches the default web browser with a pre-configured web address in a hidden window in an attempt to make the firewall believe a legitimate action is taking place. Firewalls that trust an application by default without looking beyond to who actually launched it in the first place and what additional connection parameters are supplied would fail this test.

Here's how Outpost responds:



The screenshot displays three overlapping windows from the Outpost Firewall Pro interface:

- Top Window: Create Rule for TOOLEAKY.EXE**
 - Title: TOOLEAKY.EXE (No spyware was detected)
 - Description: Application is attempting to launch another process with URL as a parameter.
 - Launcher: TOOLEAKY.EXE
 - Target: IEXPLORE.EXE
 - Command line: http://grc.com/lt/leaktest.htm?PersonalInfoGoesHere
 - Set permission for the rule:
 - Allow to launch processes with URL as parameter
 - Block attempts to launch processes with URL as parameter
 - Buttons: Allow Once, Block Once, OK
- Bottom-Left Window: TooLeaky: Trivial Firewall Leak Checker (http://tooleaky.zensoft.com/)**
 - Content: This program demonstrates how your firewall does NOT protect against outbound connections, by sending a short string to Steve Gibson's web site then retrieving a reply. For this simple example, you should currently be connected to the Internet. (Note that this program happens to rely on Steve's web pages as they were on November 4, 2001.) Please note that this program was NOT written or authorized by Steve Gibson, his web site is merely used as an example. This will probably just take a couple seconds; it will not take more than 30. Do you wish to continue?
 - Buttons: Yes, No
- Bottom-Right Window: TooLeaky: Trivial Firewall Leak Checker (http://tooleaky.zensoft.com/)**
 - Content: There was apparently no leak, your computer or Internet connection is very slow, or, most likely, the GRC.COM website is down temporarily. Please try again later.
 - Button: OK

Outpost's "App launch with URL" anti-leak control detects when an application attempts to start a program with a target URL and will prompt the user to decide whether or not to allow such activity for a particular program.

What this means for the user is that Outpost watches every program started on a computer and controls permissions for starting Internet-accessing programs, regardless of whether the program request is legitimate.

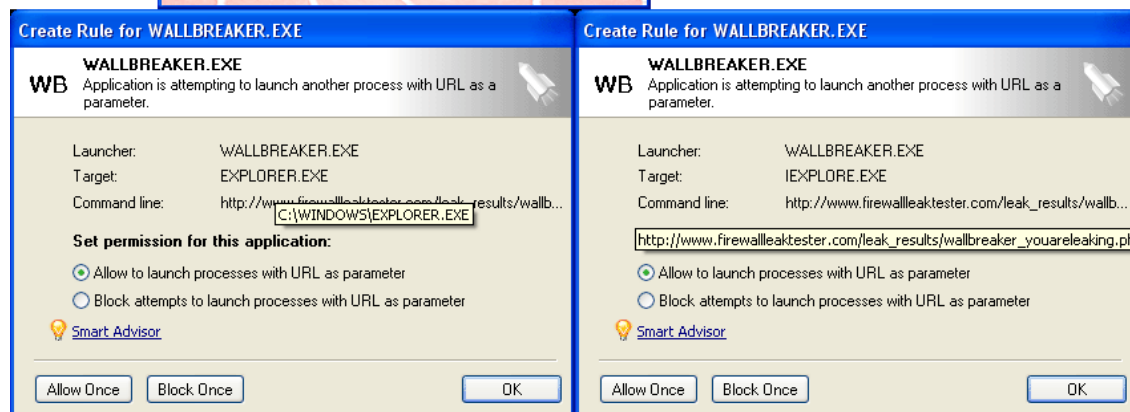
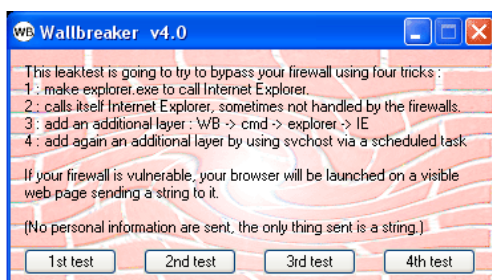
PASSED

Leak test #3 "WallBreaker"

Name/instant download link	Bypass technique used	Leak test info/homepage	Outpost function used
WallBreaker	Application launch with a URL	 WallBreaker.exe	"App launch with URL" 

WallBreaker comprises several tests that use a variety of techniques to test the firewall's outbound strength. It attempts to obscure a program launch sequence and hide the identity of the originating application in a chain of program launch events. The goal is to sufficiently confuse the firewall with layered program call commands so that the firewall loses track of who actually started the trusted program. It also launches a trusted program with a pre-defined command in its address bar in a hidden window.


Here's how Outpost responds:



Outpost Firewall Pro easily detects all attempts by the WallBreaker tests to spoof the firewall, effectively protecting the computer against these types of launching techniques.



Leak test #4 "Ghost"

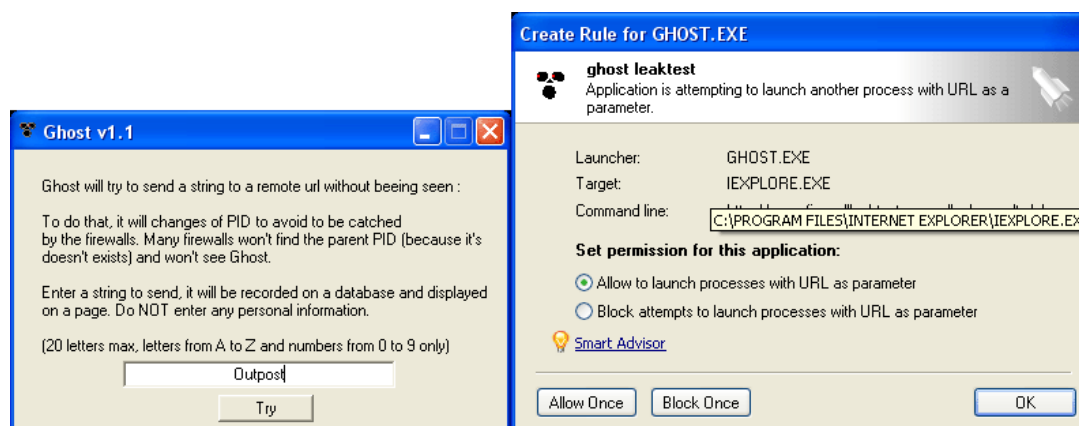
Name/instant download link	Bypass technique used	Leak test info/homepage	Outpost function used
Ghost	Application launch with a URL	 Ghost.exe ghost leaktest gkweb	"App launch with URL" 

The Ghost leak test uses the launcher techniques in conjunction with the URL address and Process Identifier (PID) manipulation.

The PID is a unique identifier assigned to each process or program started on a Windows-based computer, which the system uses to recognize active running tasks.

The Ghost leak test continually changes its PID by opening and closing itself multiple times in rapid succession. The goal is to overwhelm the firewall with different PID numbers for the same application, with the intention of preventing the firewall from being able to recognize the original process.


Here's how Outpost responds:



What this means for the user is that Outpost can detect if an application tries to change its PID number and disorient the firewall. Outpost will simply ask the user if it is OK to allow an application that is constantly changing its identity to access the Internet, either directly or through an external Internet-enabled program.

PASSED

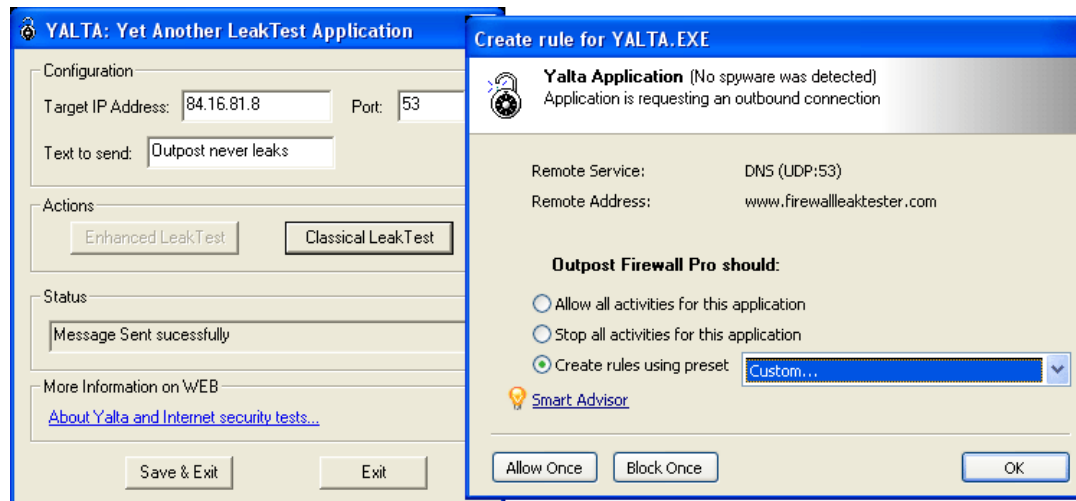
Leak test #5 "YALTA"

Name/instant download link	Bypass technique used	Leaktest info/homepage	Outpost function used
YALTA (Yet Another Leak Test Application)	Manipulation with trusted rules	 Yalta.exe Yalta Application Soft4Ever	Global rules & per-application access

Yalta is a very crafty test—it checks whether the firewall is able to detect legitimate-seeming connection activity initiated by an unauthorized program. To do this, it attempts to transmit data using a common UDP access protocol through port 21 (usually used for FTP traffic), to make the firewall believe data is being transmitted legitimately. There is also an advanced test (not available on Windows XP systems) that creates a new network driver and attempts to transmit data through it, bypassing the standard TCP/IP stack monitored by a firewall.

Firewalls that do not identify the initiator of a permitted connection and check only whether the activity the program is performing fits a general pattern of acceptable behavior will fail this test.

Here's how Outpost responds:



The above screenshots show that Outpost verifies an application's permissions before allowing it to perform a generally allowed action and alerts the user when suspect behavior is detected.

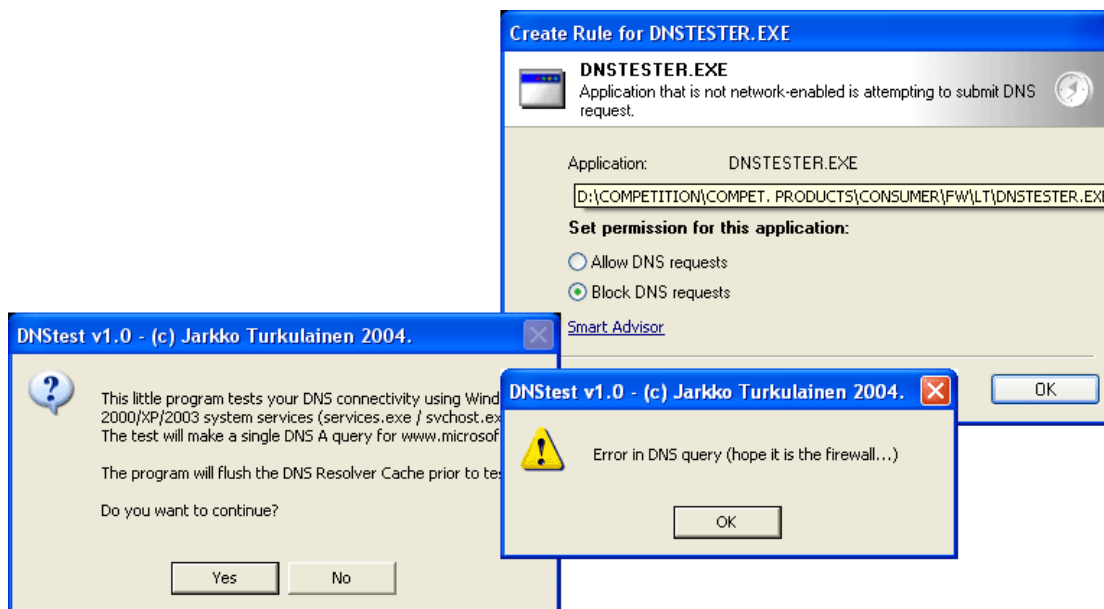
PASSED

Leak test #6 "DNSTester"

Name/instant download link	Bypass technique used	Leaktest info/homepage	Outpost function used
DNSTester	Spoofed DNS request	 dnstester.exe	"DNS API request" 

DNSTester uses recursive DNS requests to attempt to send data through the firewall undetected. By spoofing a DNS request in this way, DNSTester mimics the approach used by malicious programs to extract sensitive data from a system through illegitimate requests to the DNS Client Service (svchost.exe). The role of the DNS Client Service is to retrieve the resolved DNS addresses supplied by the DNS server, so that applications can quickly find the correct remote hosts on the Internet.

Here's how Outpost responds:



Outpost verifies applications' permissions to access the DNS Client Service and prompts the user for a decision if a noncompliant request is detected, protecting users against DNS service exploitation.

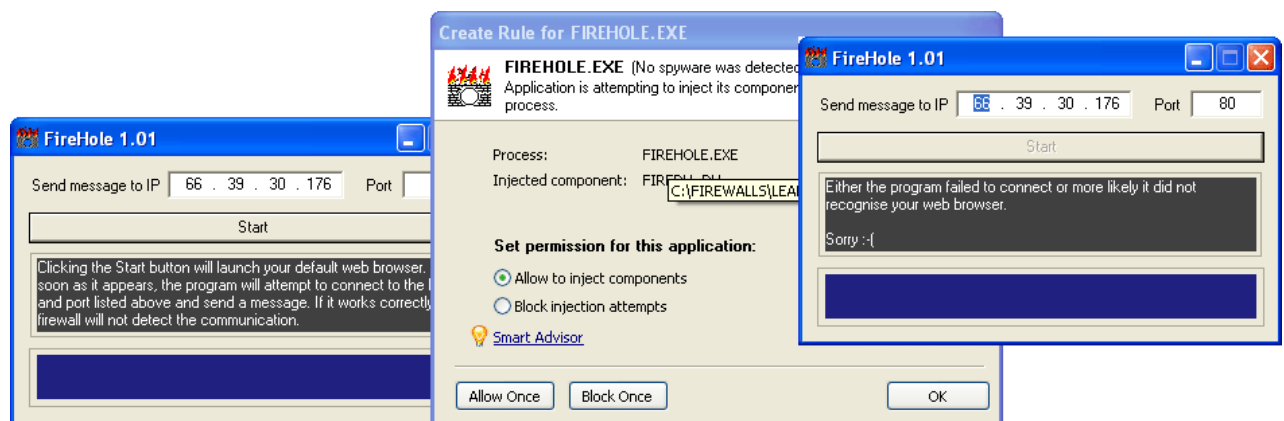
PASSED

Leak test #7 "FireHole"

Name/instant download link	Bypass technique used	Leak test info/homepage	Outpost function used
FireHole	Component injection	 firehole.exe	"Windows hooks" 

This leak test launches the default web browser and injects a small file—an executable with a DLL extension (also known as a “component” to the main application)—into the browser, which then commands the browser to connect to a malicious remote server. This technique is known as “component injection” and will not be detected by firewalls that do not monitor the internal modules of an application and what they are connecting to.



Here’s how Outpost responds:



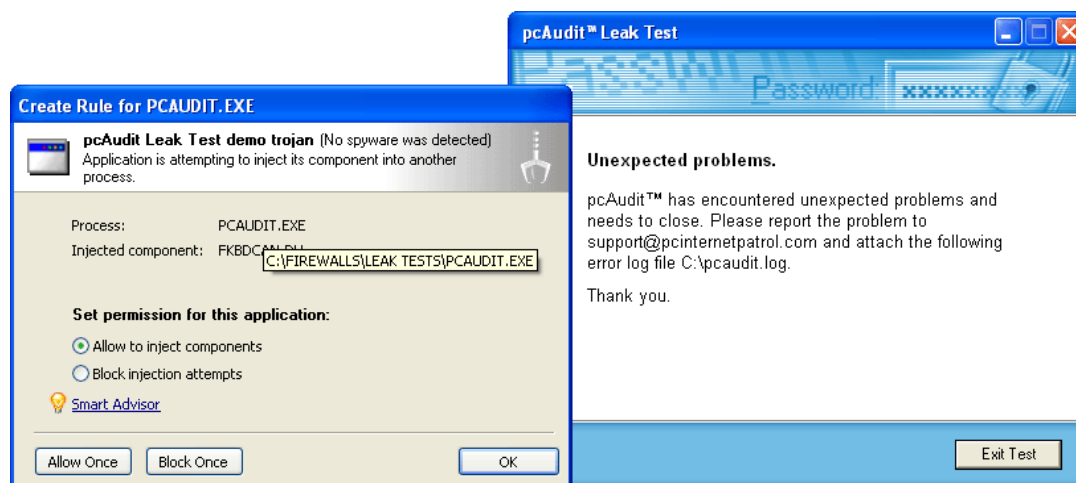
When Outpost detects an attempt by one application to inject a code snippet into another process and through it access the network, the user will be notified and prompted for a decision on whether to allow the process.

PASSED

Leak test #8 "pcAudit"

Name/instant download link	Bypass technique used	Leak test info/homepage	Outpost function used
pcAudit	Component injection	 pcaudit.exe pcAudit Leak Test demo trojan Internet Security Alliance, LLC	"Windows hooks" 



The pcAudit leak test uses the same principle as the FireHole program on the previous page—injecting a component into the memory space of a trusted program. pcAudit displays a very informative and easy-to-understand results page when the test is completed with a negative result (failed): the user's desktop is displayed, along with recently entered text and key data about the host computer. When Outpost is running, the response is even simpler:



This means that Outpost has successfully prevented the pcAudit leak test from sending data off the user's computer.

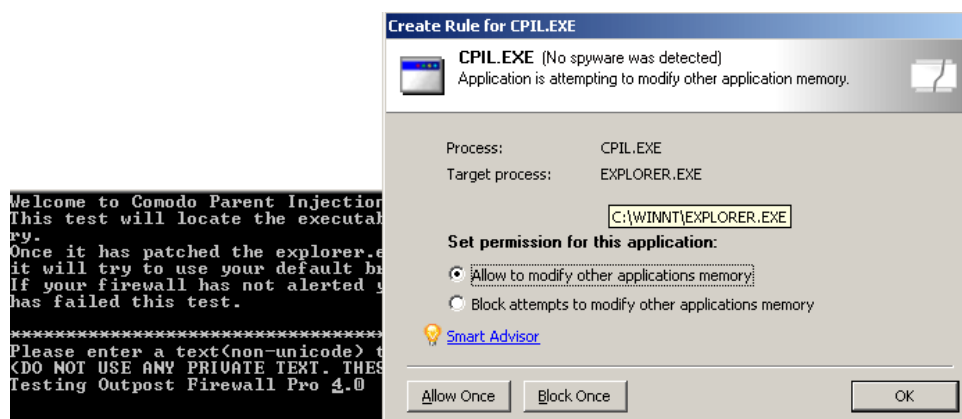
PASSED

Leak test #9 "Comodo Parent Injection Leak Test"

Name/instant download link	Bypass technique used	Leak test info/homepage	Outpost function used
Comodo Parent Injection Leak Test (CPIL)	Process injection	 cpil.exe	"Process memory injection" 

The Comodo leak test is a new program that uses the technique of component injection into Windows Explorer (explore.exe) to access the network on behalf of Explorer. The test works only under Windows 2000 OS and is not compatible with Windows XP SP2.



Here's how Outpost responds:



Outpost users running Windows 2000 can thus be assured that Outpost reliably passes the Comodo Parent Injection leak test.

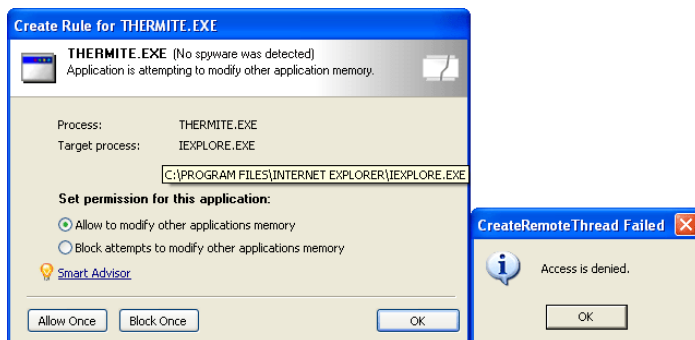


Leak test #10 "Thermite"

Name/instant download link	Bypass technique used	Leak test info/homepage	Outpost function used
Thermite	Process injection	 thermite.exe	"Process memory injection" 

The Thermite leak test uses a sophisticated hacker technique to attempt to bypass firewall protection. It injects its entire code directly into the memory of another process, making a new thread of the parent process and using that process to transmit data past the firewall. The assumption is that the firewall won't notice that an authorized program has been hijacked by malware code.



Here's how Outpost responds:



Because of the way in which Outpost monitors how programs interact on a computer, it can detect if one program is attempting to take control over another program and access the network using its credentials. In such instances, the user will be prompted to allow or disallow the action.

PASSED

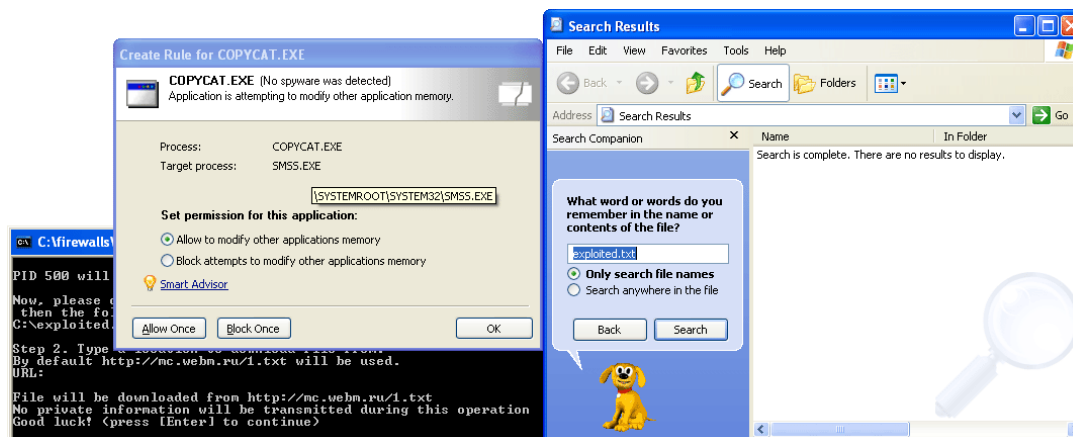
Leak test #11 "Copycat"

Name/instant download link	Bypass technique used	Leak test info/homepage	Outpost function used
Copycat	Process injection	 copycat.exe	"Process memory injection" 

The Copycat leak test is based on the same principle as Thermite—direct injection of foreign code into the resident memory of an authorized process. This test differs in that it doesn't create a new thread of the parent process but instead operates directly using the name of the hijacked process.

If this test succeeds, your firewall is vulnerable to hacking by process injection.



Here's how Outpost responds:



Outpost prevents Copycat from implanting itself into the memory block of an internal Windows program, illustrating its ability to monitor local program and process interaction on the user's system.

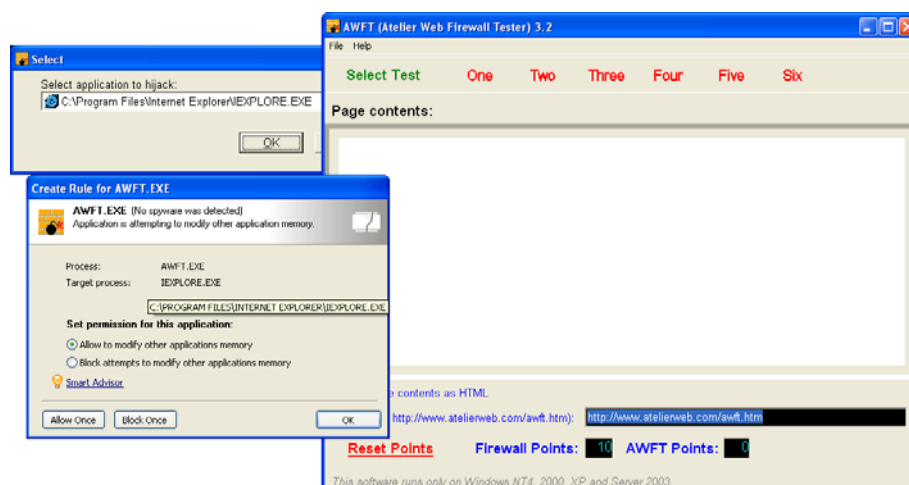
PASSED

Leak test #12 "Atelier Web Firewall Tester"

Name/instant download link	Bypass technique used	Leak test info/homepage	Outpost function used
Atelier Web Firewall Tester (AWFT)	Process injection	 awft.exe	"Process memory injection" 

The AWFT test comprises a suite of six tests in one program. It is a very complex test, combining multiple techniques designed to defeat firewalls: direct process injection into the memory of a trusted process, launching the default browser and modifying its memory block, creating an additional thread in the memory space of a trusted process, and other techniques.



Here's how Outpost responds:



The maximum score—indicating the best firewall—is ten. This is what Outpost Firewall Pro 4.0 scores, indicating that it provides maximum protection against information leaks.

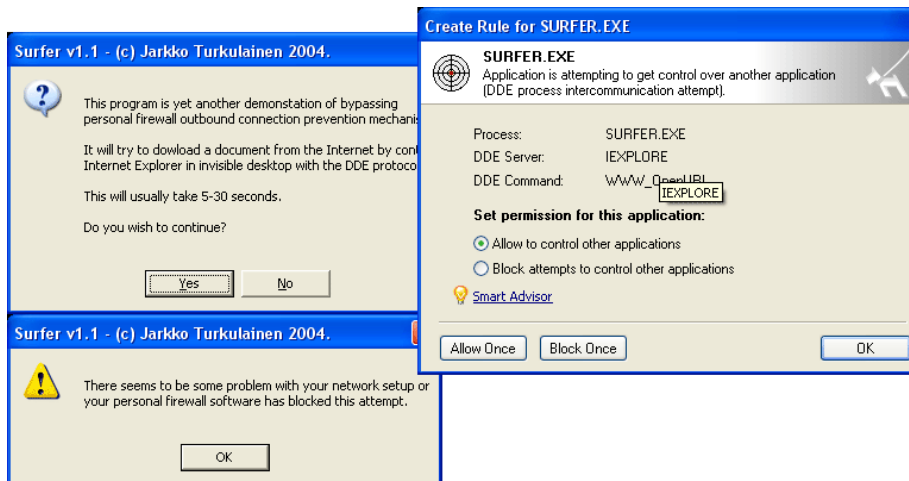


Leak test #13 "Surfer"

Name/instant download link	Bypass technique used	Leak test info/homepage	Outpost function used
Surfer	DDE inter-communication	 surfer.exe	"DDE intercommunication" 

The Surfer test aims to bypass a firewall using the technique of DDE (Direct Data Exchange) control to control the actions of a trusted application. The test launches the default web browser with a URL parameter through the DDE interface.



Here's how Outpost responds:



Because Outpost controls the commands an application receives through the DDE interface, it can protect the user's system by determining if the activity is legitimate.

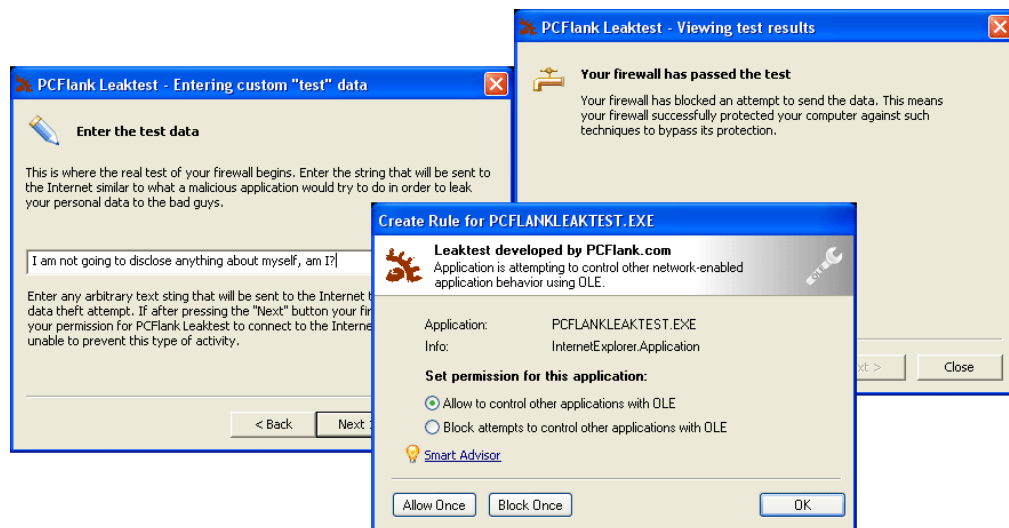


Leak test #14 "PCFlank Leaktest"

Name/instant download link	Bypass technique used	Leak test info/homepage	Outpost function used
PCFlank Leaktest	Application control through OLE automation	 PCFlankLeaktest.exe Leaktest developed by PCFlank PCFlank.com	"OLE application control" 

The PCFlank Leaktest uses OLE (Object Linking and Embedding) intercommunication to exchange data and commands between applications. The test uses the OLE model to manipulate IE activity and send specified data to the authors' test location.





Here's how Outpost responds:



Outpost can detect OLE communications and prompts the user to allow or disallow the application (in this case the PCFlank leak test) control over the other application's activity. A "no" response blocks the transmission and protects the user's data.

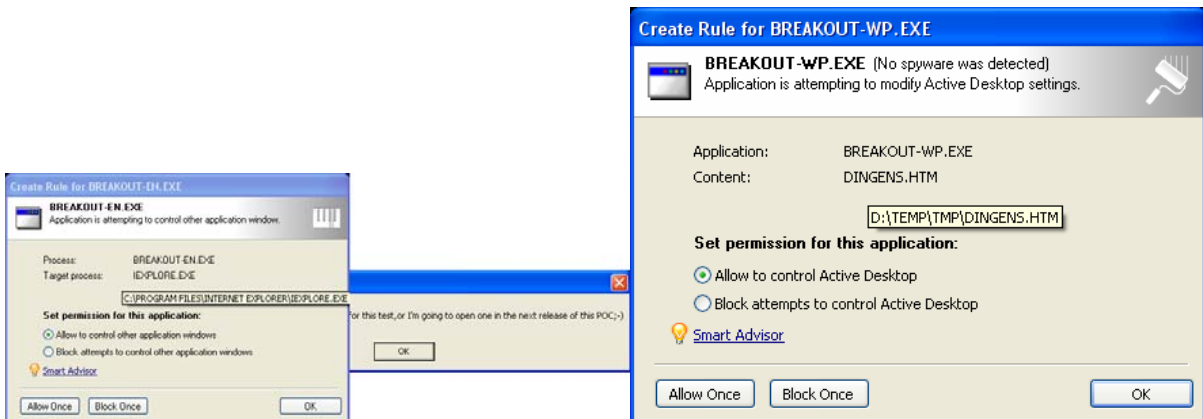


Leak test #15 "Breakout"

Name/instant download link	Bypass technique used	Leak test info/homepage	Outpost function used
Breakout	Windows messages	 breakout-en.exe	"Application window control" 
Breakout	Active Desktop modification	 breakout-wp.exe	

The Breakout test launches Internet Explorer in the background and attempts to control its behavior using "SendMessage API" inter-process communication, which enables one program to control another program's activity in a hidden mode. The same technique is used for the test to make Windows Active Desktop display a locally created HTML page and set it as desktop wallpaper. Any firewall that does not control how Internet-connecting applications interpret commands from other programs under Windows would fail this test.



Here's how Outpost responds:



As soon as it detects an attempt to use hidden windows, Outpost alerts the user.



Leak test #16 "MBtest"

Name/instant download link	Bypass technique used	Leak test info/homepage	Outpost function used
MBtest	Direct network interface access	 mbtest.exe	"Network driver opening" 

The MBtest leak test creates a flood of erratic packets and sends them off to the network adapter, bypassing the standard TCP/IP stack monitored by the firewall in an attempt to evade leak prevention techniques.



Here's how Outpost responds:



Outpost Firewall detects when an application is attempting to send data directly to a network adapter and alerts the user.

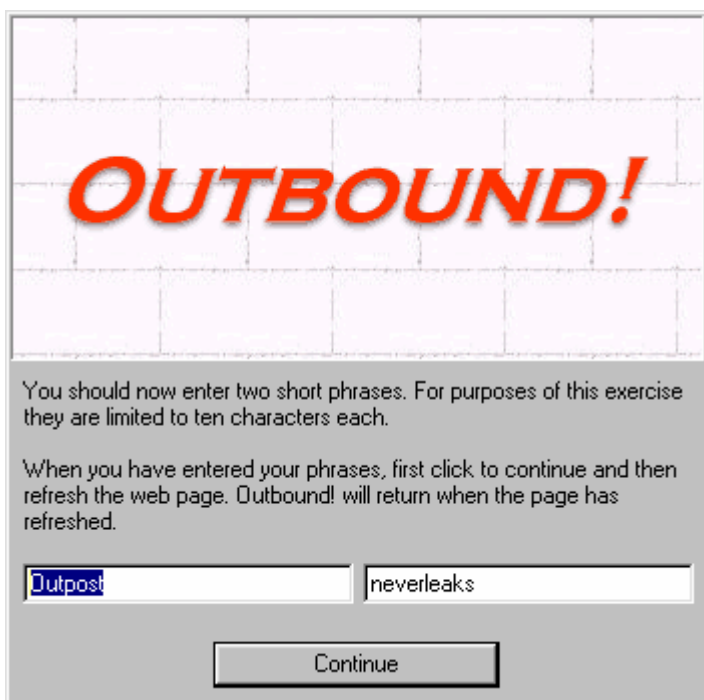
PASSED

Leak test #17 "OutBound"

Name/instant download link	Bypass technique used	Leak test info/homepage	Outpost function used
OutBound	Direct network interface access	 outbound.exe	"Network driver opening" 

OutBound is an older leak test, requiring Windows 98 to run, along with the installation of several older device drivers. However, since Outpost still supports older operating systems such as Windows 98 (unlike Microsoft), it was important for us to pass this test.

As with the previous test using the same technique, OutBound tries to send out information by opening the network driver and dispatching data through that channel. However, in our tests, it appears that this leak test no longer functions correctly; the test code did not execute correctly and the information was never transmitted. We believe this failure to execute was caused by Outpost, although we can't actually prove it.



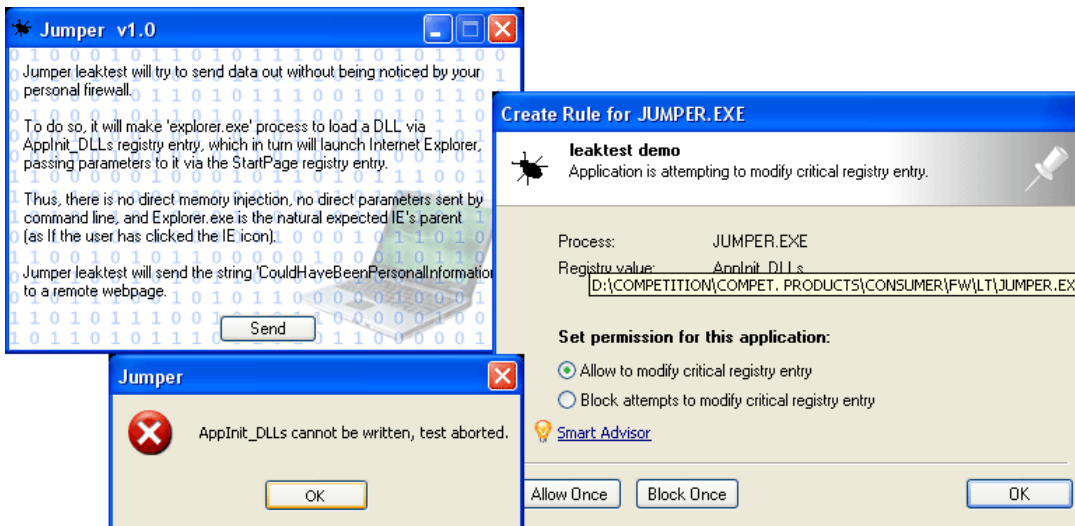
Leak test #18 "Jumper"

Name/instant download link	Bypass technique used	Leak test info/homepage	Outpost function used
Jumper	Modification of system registry	 jumper.exe leaktest demo http://www.firewallleaktester..	"Critical registry entry" 

The Jumper test uses both the Launcher and Registry Modification techniques to bypass the firewall's sensors.

By tampering with the registry, the test tricks Windows into loading the Jumper's DLL the next time Windows Explorer is launched. Then the malicious DLL modifies the registry entry for the browser's start page so that, next time it is started, it can transfer sensitive data contained in a URL address.

Here's how Outpost responds:



Because Outpost monitors critical system areas of the computer, unauthorized attempts to write to the registry ensure that malicious modifications cannot be made.

PASSED

A little background from Agnitum

Alexey Belkin, Agnitum Chief Software Architect, shares his thoughts on the addition of anti-leak components to Outpost.



“There will always be a tradeoff between security and usability. Take a regular door lock, for example. Some people will be content to live with an ordinary, factory-installed lock, while others feel safer with a stronger, more extensive system of locks that requires several keys. The latter approach takes more time, but your house will be more secure.

“The same approach can be applied to firewalls—some provide basic protection against unsophisticated threats but at the same time are easy to use, while others will be stronger, but may take some time and effort to configure correctly.

“We designed Outpost to be as strong as possible to protect users against a wide range of malware attacks and hacker intrusions. Although Outpost will ask more questions than you would normally see in a basic firewall for an initial period of use, it does, as can be seen from these test results, provide best-of-breed protection against all known methods of information leakage. We contend that the need to provide bulletproof protection is more important than the minor irritation of a few additional prompts in the first few days of use. We take data protection seriously, and we believe you should, too.

“We have provided a way for users to reduce the number of questions from the firewall. In the “anti-leak” section of the software, we have created an Exclusions tab which can be used to adjust the level of anti-leak protection as it relates to each Internet-enabled application on the user’s computer.”

Conclusion

As can be seen from this analysis, Outpost Firewall Pro 4.0 passes all currently available leak tests, providing independent proof that the software offers the highest level of protection.

In summary:

- Leak tests serve as an independent, safe way to measure a firewall’s outbound protection quality for program-specific access;
- There are eighteen currently known leak tests, based on more than a dozen program interactivity techniques;
- Outpost Firewall Pro 4.0 passes all current leak tests, providing robust protection against malware seeking to establish unauthorized connections and leak confidential information.

Plus, powerful filters ensure that protected information can never leave the computer, deterring even the most lethal hacker attacks.

The new version of Outpost Firewall Pro will safeguard users’ Internet and network connections, no matter what direction malware evolution may take.

About Agnitum

Founded in 1999, Agnitum Ltd. (www.agnitum.com) is committed to delivering and supporting high-quality, easy to use security software. The company’s products are Outpost Firewall Pro, securing personal and family desktops, and Outpost Network Security, ensuring reliable endpoint protection and performance for small business networks. Users can download a free evaluation copy of Outpost Firewall Pro from the company’s website.

Contacts

Agnitum Ltd.
Bolshoy Sampsonievskiy 60, Liter "A"
St.Petersburg, Russia, 194044

Tel: +7-(812)-3365246
Fax: +7-(812)-3365244
E-mail: pr@agnitum.com, www.agnitum.com