C·O·M·O·D·O

Creating Trust Online™

Comodo Firewall Whitepaper

Comodo Firewall 2.3 vs. The Leak Tests

Table of Contents

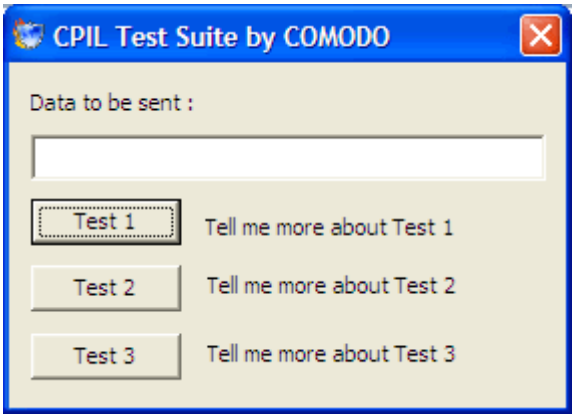
Part One:

What is Firewall Leak Testing?

Everyday, Internet users are exposed to malware programs without their knowledge. Personal firewalls form the first line of the defense to answer to these threats. Network filtering and outbound application connection filtering are the two essential components that a robust and secure personal firewall must have, that most of the personal firewalls currently in the market claim to provide in some form.

Leak tests are small, non-destructive, programs designed by security experts that deliberately attempt to bypass a firewall's outgoing security measures. The rationale behind them is painfully simple: “If this test can get past your computer’s security defenses, then so can a hacker.” Explicitly designed to help identify a firewall’s security flaws, leak tests provide the invaluable function of informing the user whether or not their firewall is providing adequate protection. The tests pose no real threat to the security of a computer as they are harmless simulations of the attack techniques typically used by spyware and Trojan horse programs. There are many leak-testing programs available – each one designed to exploit a particular flaw and each using a particular attack technique to break a firewall’s standard protection mechanisms.

Although the implementation varies from leak test to leak test, all attempt to transmit some random, non-confidential data to an outside website without the knowledge of the user.



For example, in the Comodo suite of leak tests, the user is encouraged to type some random text into the space marked 'Data to be sent’ before clicking one of the ‘Test’ buttons.

For a Personal Firewall to pass a leak test, it must detect and prevent it from making a connection to the internet. Secondly, it should inform the user that this connection attempt is being made – usually by presenting a pop-up alert with the connection details.

By purposeful design, leak test programs employ very advanced techniques to conceal their malicious activities so that they bypass the outbound defenses of a personal firewall. These techniques are commonly known as “leak” techniques.

1.1 “Leak” Techniques

There are many techniques that leak tests employ to break personal firewalls’ standard protection mechanisms.

Credits for this section: The broad format used to identify ‘Trojans that use this technique’ and ‘Leak Tests that emulate this technique’ is inspired by that used at http://www.firewallleaktester.com/malwares.htm . The naming convention for all leak test

techniques, apart from 'Unhooking', is that used on Firewall Leak Tester (http://www.firewallleaktester.com/categories.htm). The malware listed as examples of a particular technique, apart from 'Unhooking, are quoted from http://www.firewallleaktester.com/malwares.htm.

Credit for 'Unhooking' as a name; for development as a leak-testing technique and the named 'Trojans that use this technique'/Leak Tests that emulate this technique' goes to Matousec. Transparent Security. (www.matousec.com)

1.1.1 Unhooking

Personal firewalls commonly use so called hooks to implement their protection mechanisms. There exist two major types of hooks – kernel mode hooks and user mode hooks. If the self-protection mechanisms are not implemented well by the firewall it may be possible to unhook its hooks. As a result, some or all protection mechanisms of the firewall are disabled.

Trojans that use this technique:
Unknown
Leak Tests that emulate this technique:
FPR

1.1.2 Substitution

This technique tries to present itself as a trusted application by renaming itself to a commonly known, safe application such as iexplore.exe. As a result, firewalls that do not verify application signatures fail to detect such attempts.

Trojans that use this technique
W32.Welchia.Worm, The Beast
Leak Tests that emulate this technique
LeakTest 1.2

1.1.3 Launching (Parent Substitution)

With this technique, a program launches a trusted program by modifying its startup parameters such as command line parameters, to access the Internet. This type of penetration bypasses the firewalls that do not apply parent process checking before granting the internet access.

Trojans that use this technique
W32.Vivael@MM
Leak Tests that emulate this technique
Tooleaky, FireHole, WallBreaker, Ghost, Surfer, Jumper, CPIL, CPIL2, CPIL3

1.1.4 DLL Injection

Being one of the most commonly used techniques by Trojans, this method tries to load a DLL file into the process space of a trusted application. When a DLL is loaded into a trusted process, it acts as the part of that process and consequently gains the same access rights from the firewall as the trusted process itself. Firewalls that do not have an application component monitoring feature fail to detect such attacks.

Trojans that use this technique
The Beast, Proxy-Thunker, W32/Bobax.worm.a

Leak Tests that emulate this technique
PCAudit, FireHole, PCAudit v2, Jumper, CPIL3

1.1.5 Process Injection

This technique is the most advanced and difficult to detect penetration case that most of the personal firewalls still fail to detect although it is used by Trojans in the wild. The attacker program injects its code into process space of a trusted application and becomes a part of it.

Trojans that use this technique
Flux trojan
Leak Tests that emulate this technique
Thermite, CopyCat, CPIL

1.1.6 Default Rules

When a personal firewall is installed, by default, it tries to allow some vital specific traffic such as DHCP, DNS, netbios etc. not to interrupt the useful network activity. Doing so blindly may cause malicious programs to exploit these rules to access the Internet.

Trojans that use this technique
Unknown
Leak Tests that emulate this technique
Yalta

1.1.7 Race Conditions

While filtering the Internet access requests per application, personal firewalls need the process identifier (pid) of a process to perform its internal calculations. Attacker programs may try to exploit this fact by changing their process identifiers before personal firewalls detect them. A robust personal firewall should detect such attempts and behave accordingly.

Trojans that use this technique
Unknown
Leak Tests that emulate this technique
Ghost

1.1.8 Own Protocol Driver

All network traffic in Windows operating systems are generated by TCP/IP protocol driver and its services. But some Trojans can make use of their own protocol drivers to bypass the packet filtering mechanism provided by personal firewalls.

Trojans that use this technique
Unknown
Leak Tests that emulate this technique
Outbound, Yalta (test avancй), MBtest

1.1.9 Recursive Requests

Some system services provide interfaces to applications for common networking operations such as DNS, Netbios etc. Since using these interfaces is a legitimate behavior, a Trojan can exploit such opportunities to connect to the Internet.

Trojans that use this technique
Unknown
Leak Tests that emulate this technique
DNSTester, BITSTester

1.1.10 Windows Messages

Windows operating system provides inter process communication mechanism through window handles. By specially creating a window message, a Trojan can manipulate an application's behavior to connect to the Internet.

Trojans that use this technique
Unknown
Leak Tests that emulate this technique
Breakout1, zabypass

1.1.11 OLE Automation

Windows operating system also provides inter process communication mechanism through COM interfaces. By using a COM interface hosted by a server application, a Trojan can hijack the application to connect to the Internet.

Trojans that use this technique
Unknown
Leak Tests that emulate this technique
PCFlank, osfwbypassdemo

Part Two:
Comodo Firewall 2.3 vs. the Leak Tests

It is very important to test any firewall with its "out of the box" settings. A firewall may claim to provide the protection against leaking attempts while it fails to catch some of them with its default settings. Due to the fact that very few of the firewall users are able to know the correct configuration settings suitable for their system; and/or the required configuration settings are too noisy i.e. generating too many needlessly alarming alerts, users actually do not / can not have enough protection.

Another important issue is the proper detection of the leaking attempt and informing the user about the real attempt instead of something related but not meaningful to the user. For example, while detecting a DLL injection attack, a firewall can inform the user that an unknown component has been detected, but the user probably sees lots of such alerts with the legitimate components and he may not be able to see the difference between them. So it is very crucial to tell the user

the details about the attempt. A good firewall should inform the user if this unknown component is a result of DLL injection or not.

In this section, we will demonstrate how Comodo Firewall behaves against the leak tests according to the criteria we summarized above.

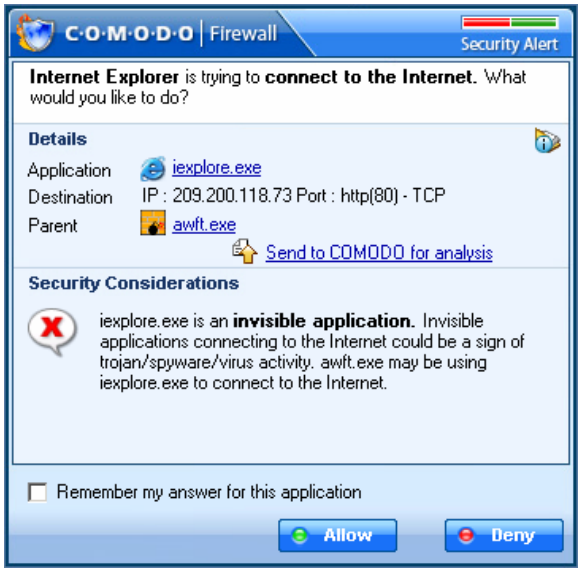
2.1 Comodo Firewall vs. Atelier Web Firewall Tester 3.2

Author: Josй Pascoa
Website: http://www.atelierweb.com/awft/
Category: Process Injection, Parent Substitution, DLL Injection
Criteria: Comodo Firewall with default settings

Atelier Web Firewall Tester contains 6 very effective leak tests each of which is used to calculate a grade over 10, for the personal firewall tested. Comodo Firewall **received 10/10** from these tests with its “out of the box” settings. For more information about each of these tests, please check the site at www.firewallleaktester.com .

2.1.1 Comodo Firewall vs. Atelier Test 1

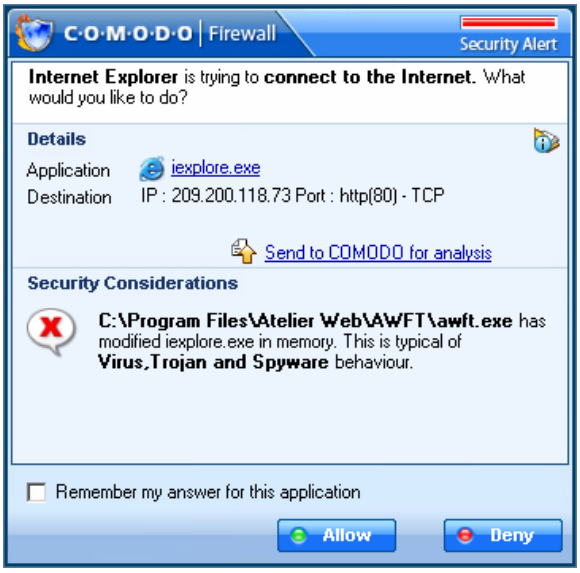
Test 1 attempts to load a copy of the default browser and patch it in memory before it executes.



Test Result: Comodo Firewall successfully **passed** this test with its “out of the box” settings.

2.1.2 Comodo Firewall vs. Atelier Test 2

Test 2 attempts to create a thread on a loaded copy of the default browser.



Test Result: Comodo Firewall successfully **passed** this test with its “out of the box” settings.

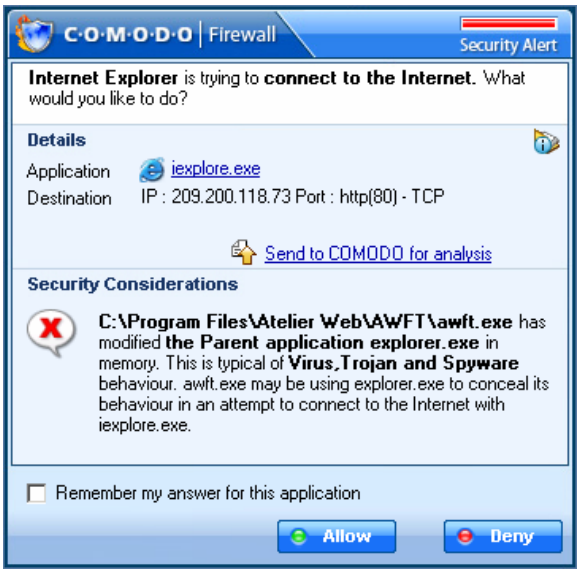
2.1.3 Comodo Firewall vs. Atelier Test 3

Test 3 attempts to create a thread on Windows Explorer

Test Result: Comodo Firewall successfully **passed** this test with its “out of the box” settings.

2.1.4 Comodo Firewall vs. Atelier Test 4

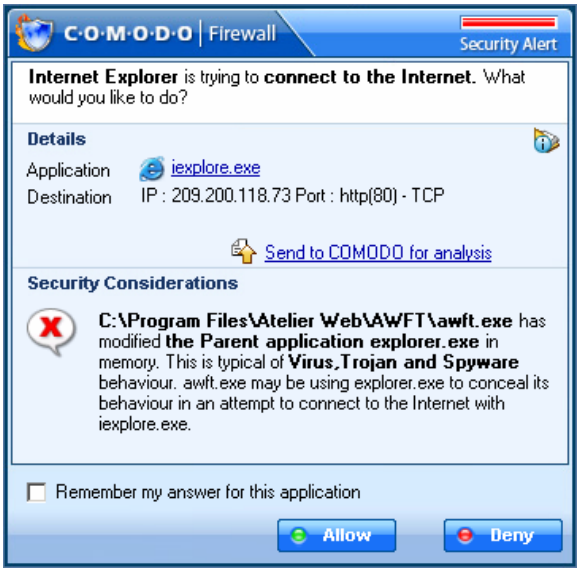
Test 4 attempts to load a copy of the default browser from within a thread in Windows Explorer and patch it in memory before execution. This attack regularly beats most personal firewalls which require authorization for an application to load another one (succeeding on Technique 1) - Windows Explorer is normally authorized.



Test Result: Comodo Firewall successfully **passed** this test with its “out of the box” settings.

2.1.5 Comodo Firewall vs. Atelier Test 5

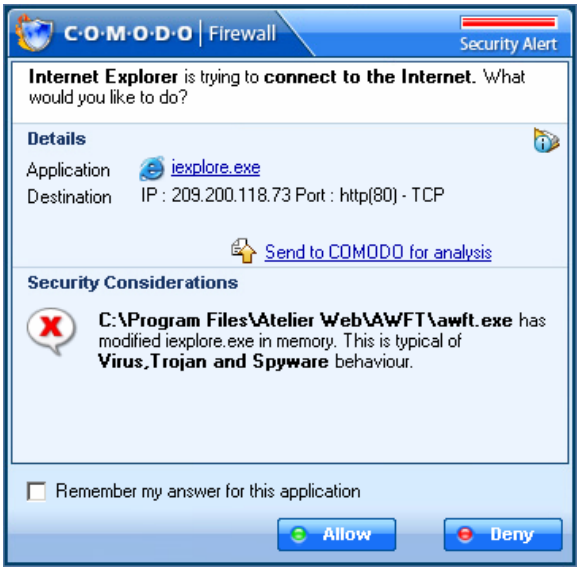
Test 5 performs a heuristic search for proxies and other software authorized to access the Internet on port 80. Then it loads a copy of this software and patches it in memory before execution from within a thread on Windows Explorer. This is a very difficult challenge for most personal firewalls!



Test Result: Comodo Firewall successfully **passed** this test with its “out of the box” settings.

2.1.6 Comodo Firewall vs. Atelier Test 6

Performs a heuristic search for proxies and other software authorized to access the Internet on port 80 then requests the user to select one of them. It then creates a thread on the select process.

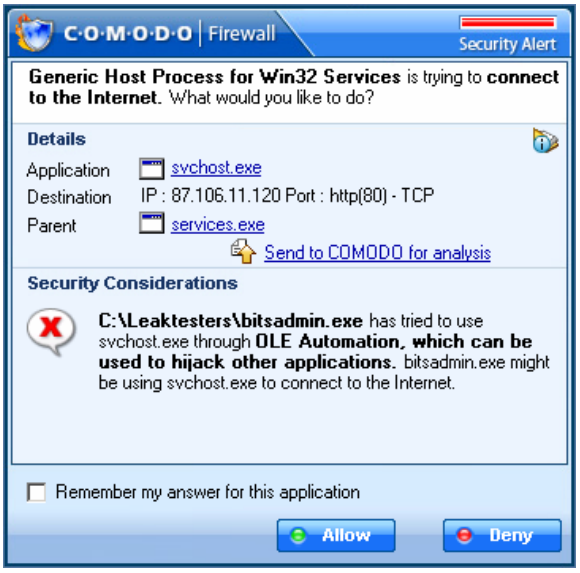


Test Result: Comodo Firewall successfully **passed** this test with its "out of the box" settings.

2.2 Comodo Firewall vs. BITSTester

Author: Guillaume Kaddouch
Website: http://www.firewallleaktester.com
Category: DLL Injection, Launcher
Criteria: Comodo Firewall with default settings

Since XP there have been Background Intelligent Transfer Service (BITS) installed in the Windows OS by default. Using a tool called BITSadmin from the Microsoft Windows XP Service Pack 2 Support Tools it is possible to control this service and order it to connect to a specific URL and download a file from the Internet. BITStester is a batch script that performs necessary steps to download a file.

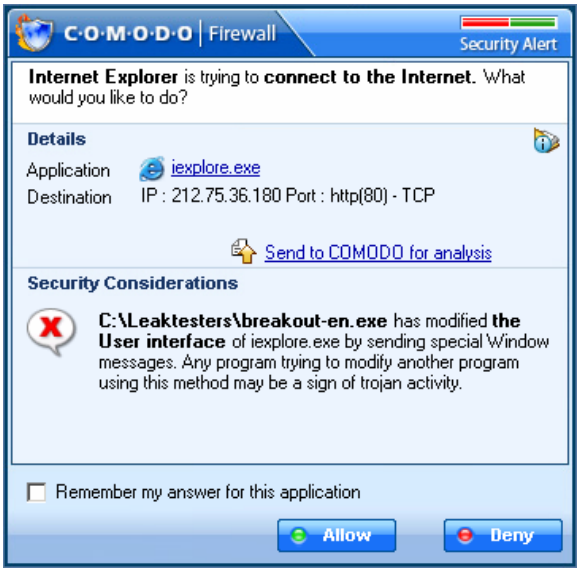


Test Result: Comodo Firewall successfully **passed** this test with its "out of the box" settings.

2.3 Comodo Firewall vs. Breakout - 1

Author: Volker Birk
Website: http://www.dingens.org/
Category: Windows Messaging
Criteria: Comodo Firewall with default settings

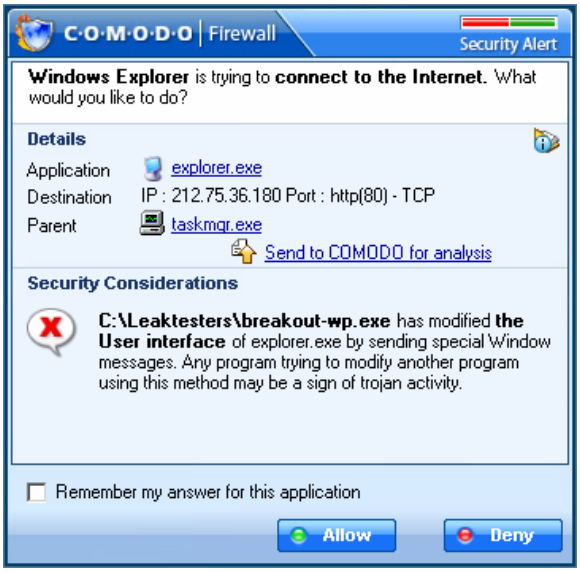
Breakout uses Windows Messages to control the Internet browser. It has two implementations, one for Internet Explorer and one for Mozilla or Firefox browsers. Using messages it is able to redirect the browser to the given location.



Test Result: Comodo Firewall successfully **passed** Breakout -

1 with its “out of the box” settings.

2.4 Comodo Firewall vs. Breakout - 2



Author: Volker Birk
Website: http://www.dingens.org/
Category: OLE Automation
Criteria: Comodo Firewall with default settings

Breakout creates HTML page on the local disk that points to the Internet server. Then, it enables Windows Active Desktop and set that HTML page to be the desktop wallpaper. As a result, Windows Explorer connects to the given URL.

Test Result: Comodo Firewall successfully **passed** Breakout - 2 with its “out of the box” settings.

2.5 Comodo Firewall vs. CopyCat

Author: Unknown
Website: http://mc.webm.ru/
Category: Process Injection
Criteria: Comodo Firewall with default settings

CopyCat uses Windows API SetThreadContext to take control over the thread of the trusted process. This technique was invisible to personal firewalls for a long time and even today many firewalls are not able to handle it.

Test Result: Comodo Firewall successfully **passed** this test with its “out of the box” settings. According to the site www.firewallleaktester.com, most of the personal firewalls in the market today failed to detect this leak test.

2.6 Exclusive! Comodo Firewall vs. CPIL Test Suite

Author: Comodo
Website: www.personalfirewall.comodo.com
Category: Process Injection
Criteria: Comodo Firewall with default settings

CPIL test locates the executable file called explorer.exe and patch its memory loading its own DLL. Then, it tries to use the default browser to transfer the data from your computer to the Internet server.

CPILSuite, devised by our own firewall developers, includes 3 advanced firewall leak tests. While this document was being written, Comodo Firewall was the only firewall that could pass all of the tests properly.

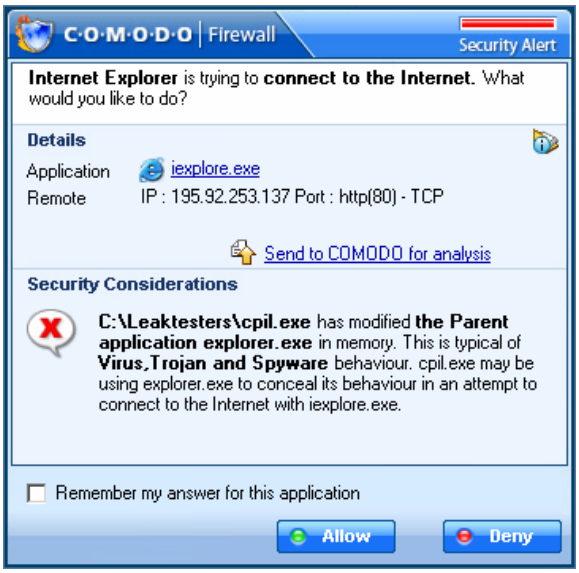
The CPIL suite contains three separate tests especially developed by Comodo engineers to test a firewall's protection against parent injection leak attacks. Each of the three tests involves the user typing some random text into a text box which CPIL will attempt to transmit to the Comodo servers.

Test Result: Comodo Firewall successfully **passed** this test with its "out of the box" settings.

2.6.1 Comodo Firewall vs. CPIL 1

Attempts to disable firewall hooks by directly accessing the physical memory and then modifies explorer.exe to bypass the firewall by running iexplore.exe with a command line address.

Test Result: Comodo Firewall successfully **passed** this test with its "out of the box" settings.



2.6.2 Comodo Firewall vs. CPIL 2

Attempts to inject cpil2.dll into explorer.exe by using Windows accessibility API and then tries to bypass the firewall by running iexplore.exe with a command line address. At the time of writing (11th Oct 2006) Comodo **Firewall was the only firewall that could detect this attempt properly.**

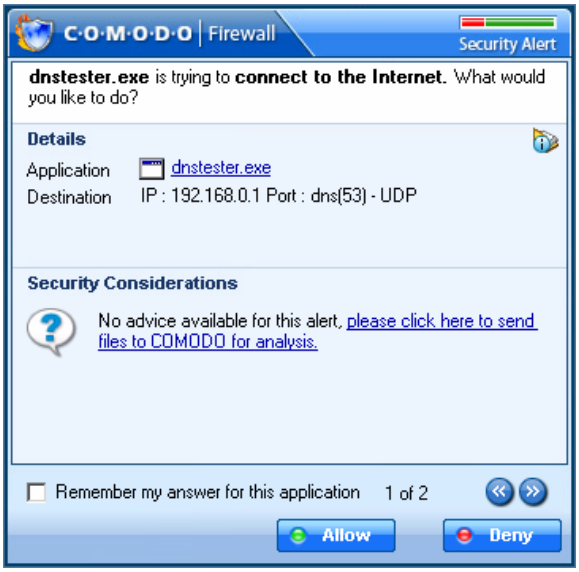
Test Result: Comodo Firewall successfully **passed** this test with its "out of the box" settings.

2.6.3 Comodo Firewall vs. CPIL 3

Attempts to inject cpil3.dll into explorer.exe by using Windows accessibility API and then tries to bypass the firewall by running iexplore.exe and modifying iexplore.exe with DDE communication. At the time of writing (11th Oct 2006) Comodo **Firewall was the only firewall that could detect this attempt properly.**

Test Result: Comodo Firewall successfully **passed** this test with its "out of the box" settings.

2.7 Comodo Firewall vs. DNStester



Author: Jarkko Turkulainen
Website: http://www.klake.org/~jt/dnshell/
Category: Substitution
Criteria: Comodo Firewall with default settings

DNStester uses Windows DNS API functions to make a recursive DNS query to the Internet server. DNS packets can be used to transfer extra data and this is why they should be controlled by firewalls as any other packets.

Test Result: Comodo Firewall successfully **passed** this test with its "out of the box" settings.

2.8 Comodo Firewall vs. Firehole

Author: Robin Keir
Website: http://keir.net/firehole.html
Category: Parent Substitution, DLL Injection
Criteria: Comodo Firewall with default settings

FireHole attempts to launch the default browser and then it uses Windows API SetWindowsHookEx to inject its own DLL into the browser's process. From inside of the browser it then establish the Internet connection.

Test Result: Comodo Firewall successfully **passed** this test with its "out of the box" settings. The firewall catches this leak attempt with 3 of its security components. Application monitor detects the parent change, component monitor detects the unknown library, and application behavior analysis reveals the details about the request. ***Unlike other firewalls, Comodo Firewall detects DLL injections even if Component Monitor is in learning mode.***

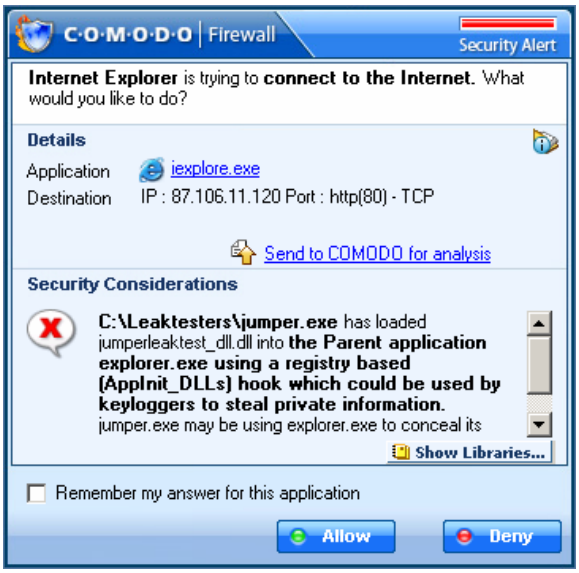
2.9 Comodo Firewall vs. Ghost

Author: Guillaume Kaddouch
Website: http://www.firewallleaktester.com/
Category: Parent Substitution, Race Conditions
Criteria: Comodo Firewall with default settings

Ghost tries to confuse firewalls by shutting down its own process and restarting itself. The reason for this is to change its Process Identifier (PID) such that the firewall is not able to identify its new process correctly. Then, it sends the information via the default browser to the Internet server.

Test Result: Comodo Firewall successfully **passed** this test with its "out of the box" settings.

2.10 Comodo Firewall vs. Jumper

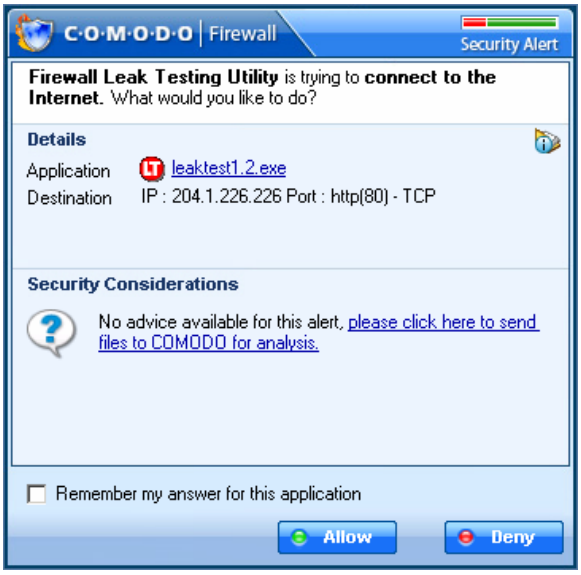


Author: Guillaume Kaddouch
Website: http://www.firewallleaktester.com
Category: DLL Injection, Launcher
Criteria: Comodo Firewall with default settings

Jumper attempts to infect Windows Explorer with its own DLL. At first, it tries to modify the registry value AppInit_DLLs and then it terminates Windows Explorer. When the Windows Explorer is run again it loads DLLs specified in AppInit_DLLs to its process. Jumper's DLL running from the Windows Explorer process launch Internet Explorer and controls its behavior to connect to the Internet server.

Test Result: Comodo Firewall successfully **passed** this test with its "out of the box" settings.

2.11 Comodo Firewall vs. LeakTest 1.2

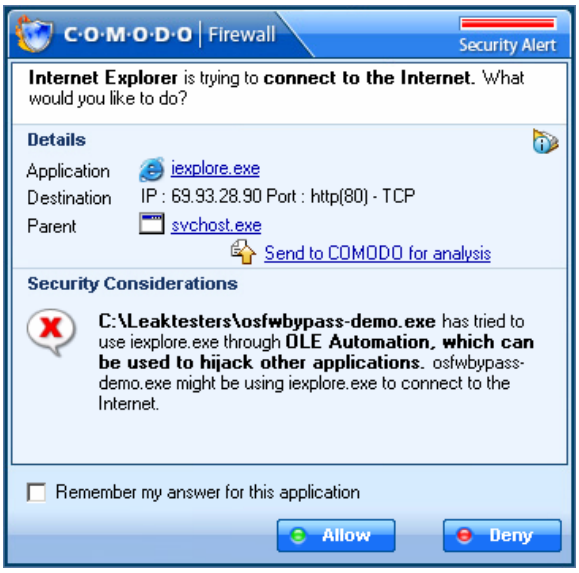


Author: Steve Gibson (Gibson Research Corporation)
Website: http://grc.com/lt/leaktest.htm
Category: Substitution
Criteria: Comodo Firewall with default settings

LeakTest is the oldest leak test program implemented to bypass stone-age firewalls that rely only on the name of the executable module when identifying applications.

Test Result: Comodo Firewall successfully **passed** this test with its "out of the box" settings.

2.12 Comodo Firewall vs. OSfwbypass



Author: Debasis Mohanty (a.k.a. Tr0y)
Website: http://www.hackingspirits.com/
Category: DLL Injection, Launcher
Criteria: Comodo Firewall with default settings

Using OLE automation OSfwbypass tries to load HTML page with Javascript into Internet Explorer. Javascript simply redirects Internet Explorer to the Internet server.

Test Result: Comodo Firewall successfully **passed** this test with its "out of the box" settings.

2.13 Comodo Firewall vs. Outbound and MBTest

Author: HackBusters, Unknown
Website: http://www.firewallleaktester.com/
Category: Own Protocol Driver
Criteria: Comodo Firewall with protocol driver protection activated

Comodo Firewall has an optional but disabled by default, feature called '**Monitor other NDIS protocols than TCP/IP'**. If this feature is activated in the 'Advanced/ Miscellaneous' section, it detects such leaking attempts.

This feature is disabled by default for 3 reasons:

- We are unaware of any Trojan which employ this technique.
- It may slow down operating systems networking unnecessarily.
- By default, Comodo Firewall already detects known Trojans with protocol driver level communication capabilities without this option is enabled e.g. ntrootkit.

Test Result: Comodo Firewall successfully **passed** this test with the **Monitor other NDIS protocols than TCP/IP** option enabled.

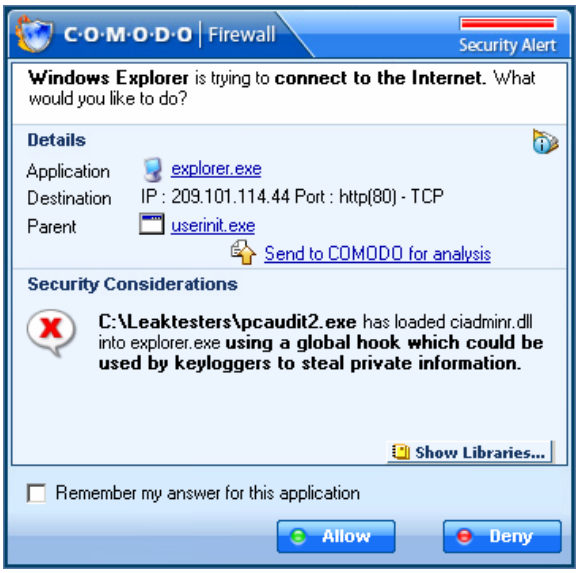
2.14 Comodo Firewall vs. PCAudit

Author: Internet Security Alliance
Website: http://www.pcinternetpatrol.com/
Category: DLL Injection
Criteria: Comodo Firewall with default settings

PCAudit implements typical DLL injection technique. It tries to load library into trusted process to be able to establish the Internet connection without any alerts from the firewall.

Test Result: Comodo Firewall successfully **passed** this test with its "out of the box" settings. This test is a demonstration of DLL injection attack***. Unlike other personal firewalls, Comodo Firewall detects DLL injections even if Component Monitor is in learning mode.***

2.15 Comodo Firewall vs. PCAudit 2



Author: Internet Security Alliance
Website: http://www.pcinternetpatrol.com/
Category: DLL Injection
Criteria: Comodo Firewall with default settings

Like PCAudit, its newer version called PCAudit2 attempts to load its own DLL to other processes to bypass the protection of firewalls from the trusted process.

Test Result: Comodo Firewall successfully **passed** this test with its "out of the box" settings. This test is a demonstration of DLL injection attack***. Unlike other firewalls, Comodo Firewall 2.3 detects DLL injections even if Component Monitor is in learning mode.***

2.16 Comodo Firewall vs. PCFlank

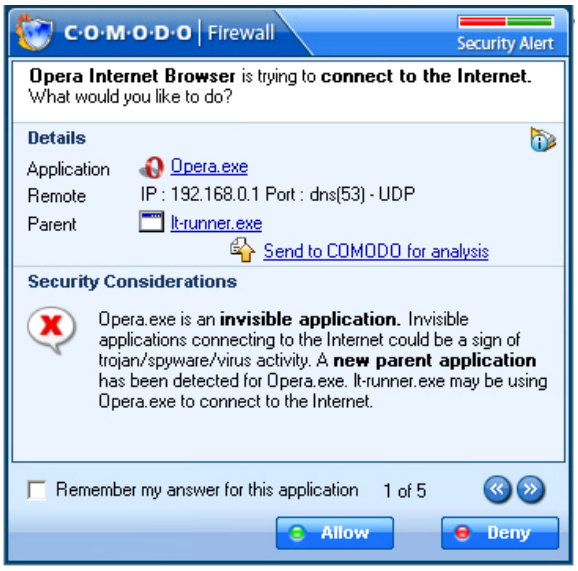
Author: PCFlank
Website: http://www.pcflank.com
Category: DLL Injection, Launcher
Criteria: Comodo Firewall with default settings

PCFlank attempts to control running instance of Internet Explorer using OLE automation to transfer information to the Internet server.

Test Result: Comodo Firewall successfully **passed** this test with its "out of the box" settings.

2.17 Comodo Firewall vs. Runner

Author: Matousec – Transparent Security
Website: http://www.matousec.com
Category: Substitution
Criteria: Comodo Firewall with default settings



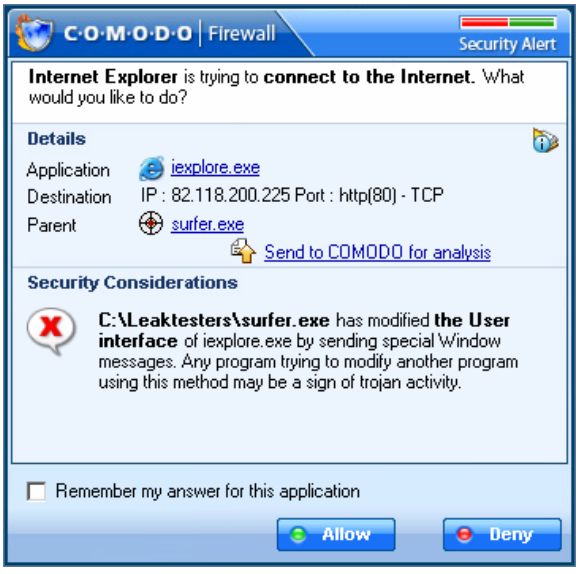
The Runner finds the default browser's executable and renames it. Then it copies itself to the file of the original default browser's executable. It runs this copy, renames it, copies the original executable of the default browser back and then it tries to establish an Internet connection.

Firewalls that are not able to handle this trick either do not verify the integrity of the default browser, or their verification occurs when the privileged action is executed instead of the moment of the fake executable execution.

Test Result: Comodo Firewall successfully **passed** this test with its “out of the box” settings.

2.18 Comodo Firewall vs. Surfer

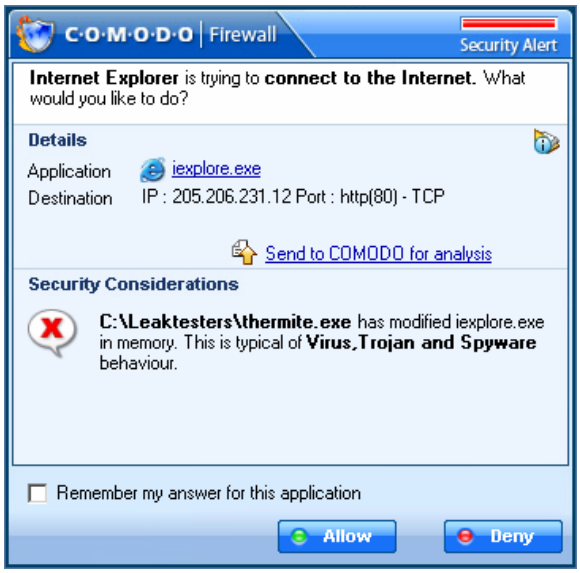
Author: Jarkko Turkulainen
Website: http://www.firewallleaktester.com/
Category: Parent Substitution
Criteria: Comodo Firewall with default settings



Surfer creates hidden desktop and runs Internet Explorer on it, then it uses Direct Data Exchange (DDE) to control its behavior and transfer data to the Internet server.

Test Result: Comodo Firewall successfully **passed** this test with its “out of the box” settings.

2.19 Comodo Firewall vs. Thermite



Author: Oliver Lavery
Website: http://www.firewallleaktester.com/
Category: Process Injection
Criteria: Comodo Firewall with default settings

Thermite attempts to find running instance of Internet Explorer, inject tiny infection code and create a remote thread in it. From the Internet Explorer process it then tries to establish socket connections and transfer information to the Internet server.

Test Result: Comodo Firewall successfully **passed** this test with its "out of the box" settings. According to the site www.firewallleaktester.com, most of the personal firewalls in the market today failed to detect this leak test.

2.20 Comodo Firewall vs. Tooleaky

Author: Bob Sundling
Website: http://tooleaky.zensoft.com/
Category: Parent Substitution
Criteria: Comodo Firewall with default settings

TooLeaky attempts to launch hidden instance of Internet Explorer with the URL in the command line parameter. Personal data may be transferred in the URL to the Internet server.

Test Result: Comodo Firewall successfully **passed** this test with its "out of the box" settings. Tooleaky.exe tries to launch internet explorer invisibly to transmit data. As seen in the screenshot, the firewall reveals everything about the leak in security considerations section.

2.21 Comodo Firewall vs. WallBreaker

Author: Guillaume Kaddouch
Website: http://www.firewallleaktester.com/
Category: Parent Substitution
Criteria: Comodo Firewall with "Do not show alerts for the applications certified by COMODO" option disabled

Note: The WallBreaker tests contain **4** types of breaching attempts.

2.21.1 Comodo Firewall vs. WallBreaker Tests 1, 3, 4

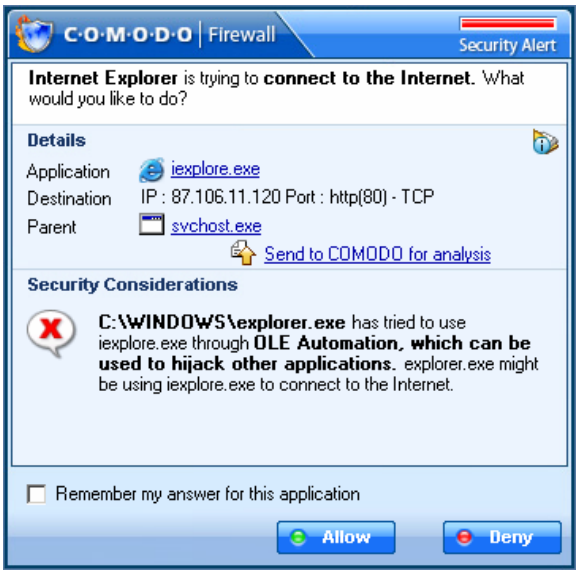
WallBreaker test 1, 3 and 4 attempt to load a copy of the default browser by using various techniques which require DDE (COM communication) Passing this test requires the 'Automatically approve safe applications' option to be disabled.

Test Result: Comodo Firewall successfully **passed** this test.

2.21.2 Comodo Firewall vs. WallBreaker Test 2

WallBreaker test 2 attempts to load iexplore.exe itself.

Test Result: Comodo Firewall successfully **passed** this test.



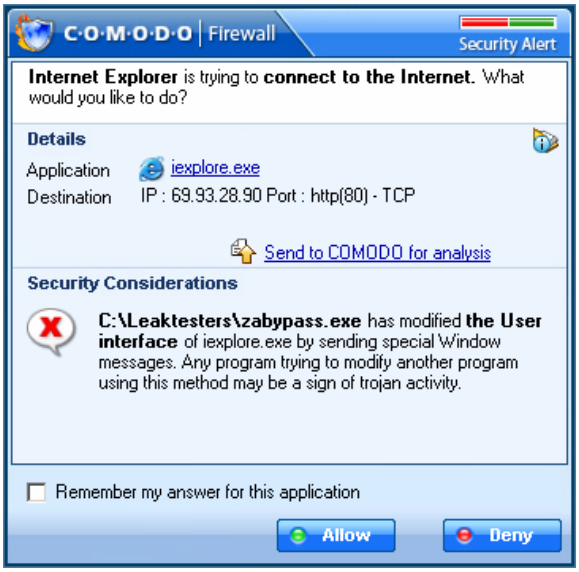
2.22 Comodo Firewall vs. Yalta

Author: Soft4ever
Website: http://www.soft4ever.com/security_test/En/index.htm/
Category: Default Rules, Own Protocol Driver
Criteria: Comodo Firewall with default settings

YALTA attempts to send UDP packet to a specific IP address and port. Some firewalls may not control connections to ports of specific services like DNS and trust connections that use these ports.

Test Result: Comodo Firewall successfully **passed** classical Yalta test with its "out of the box" settings. The Yalta Enhanced test works only in Windows 9X/Me systems and, as Comodo Firewall does not support those systems, the test is not applicable.

2.23 Comodo Firewall vs. ZABypass



Author: Debasis Mohanty (a.k.a. Tr0y)
Website: http://www.hackingspirits.com/
Category: DLL Injection, Launcher
Criteria: Comodo Firewall with default settings

ZAbypass was implemented to bypass old versions of ZoneAlarm PRO but it works against many other firewalls today. It uses Direct Data Exchange (DDE) to communicate with Internet Explorer and transfer data between its process and the Internet server.

Test Result: Comodo Firewall successfully **passed** this test with its “out of the box” settings.

About Comodo

Comodo is a leading global provider of Identity and Trust Assurance services on the Internet, with over 200,000 customers worldwide. Headquartered in Jersey City, NJ with global offices in the UK, Ukraine and India, the company offers businesses and consumers the intelligent security, authentication and assurance services necessary to ensure trust in online transactions.

As a leading Certification Authority, and in combination with the Digital Trust Lab (DTL), Comodo helps enterprises address digital ecommerce and infrastructure needs with reliable, third generation solutions that improve customer relationships, enhance customer trust and create efficiencies across digital ecommerce operations. Comodo's solutions include SSL certificates, integrated Web hosting management solutions, web content authentication, infrastructure services, digital e-commerce services, digital certification, identity assurance, customer privacy and vulnerability management solutions.

For additional information on Comodo – Creating Trust Online ™

www.comodo.com

To download Comodo Firewall, please visit http://personalfirewall.comodo.com

Comodo

US Headquarters,
525 Washington Blvd.,
Jersey City, NJ 07310
Tel : +1.888.COMODO.1
email : sales@comodo.com

Comodo Group Inc.,

3rd Floor, Office Village,
Exchange Quay, Trafford Road,
Salford, Manchester M5 3EQ,
United Kingdom.
Tel Sales: +44 (0) 161 874 7070
Fax Sales: +44 (0) 161 877 7025
email : sales@comodo.com

www.comodo.com