

Help! There's an Intruder in my Computer

By June Campbell

Help! There's an Intruder in my Computer

June Campbell
campbelj@nightcats.com

Business Writing by Nightcats Multimedia <http://www.nightcats.com>

Do you have passwords, love letters, naughty pictures or sensitive business information stored on your computer's hard drive? If you have a continuous Internet connection such as cable, xDSL, ISDN or other, you should know that it's almost embarrassingly easy for a hacker to break into a networked computer.

Once in, they can use your private information any way they see fit. As well as getting your personal documents, the hacker can damage your system files or install software on your disk that allows your computer to be used in Denial of Service attacks and other destructive activities.

Similarly, the hacker can activate your interior microphone or interior video recorder without your knowledge. This lets them record and distribute sound and video files of the conversations and activities taking place in your work area.

How Hackers Do It

Every Internet-connected computer has a unique set of identifying numbers called an IP address. Using special software applications, hackers send out probes over the Internet looking for live IP addresses. If they locate your computer, they look for "holes" or vulnerabilities that leave your system insecure.

For example, a computer is likely to have multiple applications (email, web browser, etc.) running on the same IP address. Each application is assigned a number called a "port" that uniquely identifies that service on a computer. Ports that allow an application to send or receive information from the Net must be "open". In some unprotected systems, even ports that are not in use have been left open -- practically inviting attack! When hackers discover an unprotected, open port, they can use that opening to gain access to your system.

An unprotected broadband connection is easiest to hack because both the connection and the IP address remain constant. If a hacker or a "script kiddie" finds your computer once, they can readily find it again. (Script kiddie is a derogatory name used by professional hackers to describe simple scripts used by young and inexperienced hackers).

The threat is less severe for persons connecting to the Internet via dial-up modems. Dial-ups usually connect with a different IP address each log-on. Therefore, if hackers have found a system once, the changing IP address will make it difficult (not impossible) to find it again.

However, if a trojan horse or back door program has been installed on a system, the trojan horse

could "phone home" with the IP address each time an Internet connection is made.

Back door programs allow remote users to control a system without the owner's knowledge. They are installed on computers by hackers, or sometimes come secretly bundled with software applications that the user installs. Well-known back door programs for Windows computers include BackOriface, NetBus and SubSeven.

Firewalls: Your First Level of Security

Firewalls are software applications or hardware devices that you install on your system. They are designed to prevent unauthorized access to or from a private network that is connected to the Internet. When a firewall is installed, all incoming or outgoing messages pass through the firewall. Those that do not meet the specified security criteria are blocked.

Most home firewalls are software applications.

How Firewalls Work

There are various types of firewalls, and they work through different processes. However, the following is true for most of the home or personal firewall software that is used today.

Information over the Internet is sent in "packets" of data. These packets travel from a source machine to a destination machine -- which could be two feet away or two continents away. Each packet of data contains the IP address and port number of the originating machine.

The firewall software inspects every packet of data that arrives at the computer -- BEFORE that data is allowed entry into the system and before it connects with an "open" port. The beauty of a firewall lies in its ability to be selective about what it accepts and what it blocks.

The firewall has the ability to refuse any suspect data. If the incoming data is ignored and not allowed in, that port will effectively disappear on the Internet and hackers cannot find it or connect through it. In other words, instead of receiving a signal that a port is open, the hackers receive nothing back and have no way of connecting.

Several firewall applications are available to the small business operator or the home computer user. Before changing firewalls or installing one for the first time, it's wise to check out the comparative testing that has been done on these applications.

Persons already running a firewall could test its effectiveness by trying the Shields and Ports test available at Gibson's Research Corporation (GRC) web site, or by downloading and running the LeakTest software available on site at <http://www.grc.com> .

GRC's Steve Gibson has some surprising test results posted in conjunction with LeakTest's personal firewall scoreboard at <http://grc.com/lt/scoreboard.htm> .

The best-rated one is free. Not only did Zone Lab's Zone Alarm (<http://www.zonelabs.com>) score best in Gibson's testing, but the firewall has been recognized for excellence by CNET, PC World, PC Magazine and Home Office Computing.

Other well-known firewalls include McAfee firewall at www.mcafee.com , Sygate Personal FW at www.sygate.com , Symantec/Norton at www.symantec.com and Tiny Personal FW at www.tinysoftware.com

Now, the bad news.

A firewall protects you from open ports, but it does not protect you from data coming and going through ports that you allow. Malicious code can invade your system from email attachments or by visiting a hostile web site. And remember -- even well trusted web sites can suddenly be hostile if hackers have added malicious code without the site administrator's knowledge.

Test your security against malicious code at Finjan Software's web site. Many of you will be dismayed to find that your supposedly secure system is vulnerable.

<http://www.finjan.com>

Malicious code blocking software such as Finjan's Surf n' Guard analyzes incoming data and decides whether the code could be harmful. ZDNet recommends that code-blocking software be used in addition to firewall and your antivirus software.

Too Late?

What if you think you've been hacked? Call your computer guru to help, or check out the information at sites like HackFix.

<http://www.hackfix.org>

=====
How to Write Business Plans, Business Proposals,
JV Contracts, Human Resource Package, More!
No-cost ebook "Beginners Guide to Ecommerce".
Business Writing by Nightcats Multimedia Productions

<http://www.nightcats.com>

[Get-Articles.com](http://www.get-articles.com) : 1000's of reprintable business and internet marketing-related articles.

[Submit your article for reprint.](http://www.get-articles.com)