

Inside Spyware

Most computer users are aware of the dark side of the Internet. Our online world brings issues of credit card and identity theft, junk mail and seedy content right into our homes and offices. But how many computer users are unwitting accomplices to such activities?

Your computer, or those of the people in your organization, is possibly being used to send spam, harvest e-mail addresses for spam, make purchases using stolen credit cards or take part in a denial of service (DoS) attack, where an army of computers shuts down a Web site by flooding its servers with HTTP requests.

EarthLink's SpyAudit program, which scanned 1,062,756 PCs, found 29.5 million instances of spyware, an average of nearly 28 spyware items per computer.

How does this happen without your knowledge? Examples like those above are usually the work of a trojan, a small program that can be unknowingly installed on a computer and then accessed by another computer over the Internet. Together with programs called spyware, adware and viruses, trojans are a part of a group collectively known as "malware" or "pestware." While the majority of such programs are pests and nothing more, they have the potential to be quite nasty.

Trojans: RATS That Can Control Your Computer

Like the horse of old, a trojan carries with it an unexpected surprise. Trojans do not replicate like a virus, but they do leave behind a program that can be contacted by another computer. From there, they can do just about anything. While it's possible a trojan can be used to take control of a computer, the most common trojans are dialer programs. Dialers are used without your knowledge to make international or premium calls (900-type numbers) from your PC. That's more than an annoyance; it can get expensive.

Trojans are also known as RATS (remote access trojans) and they are most often hidden in games and other small software programs that unsuspecting users download then unknowingly execute on their PCs.

Two common trojans are known as Back Orifice and SubSeven. Back Orifice was originally developed as a remote administration tool. But it worked by exploiting holes in Microsoft software, which makes it a popular tool for nefarious applications. Both Back Orifice and SubSeven can be used to capture what is on a computer's screen and what is typed in using the keyboard; they can be used to remotely control devices, such as opening and closing the CD drive; or to set up FTP, HTTP or Telnet servers on an unsuspecting user's machine. Basically, anything that can be done with a computer can be done remotely using a trojan.

Spyware: Who's Watching Your Online Moves?

Spyware programs range from annoying to the dangerous, including keyboard loggers and screen capture applications that can steal passwords and other sensitive information. The programs are sometimes bundled in with shareware or freeware programs that can be downloaded from the Internet. Often times they claim to be helpful utilities that also carry a more sinister side.

Many of the programs are marketed as legitimate tools for keeping tabs on children and spouses online. One program called Activity Logger, for example, connects to the Internet on its own, records the URLs of sites visited and the keystrokes from e-mail and chat applications. It will also capture screenshots that can be made into a slide show.

Adware: Caught in a Marketing Nightmare

Adware is software that displays advertisements to computer users. Some of the strictest definitions of adware include applications that are sponsored for their free use. One of the most popular examples is WeatherBug, which offers a free version of weather software and comes wrapped in a skin that displays advertising. While older versions of WeatherBug had rather significant privacy issues, newer versions are pretty straightforward: you see the ad, but you get the weather. Is this adware? In the strictest sense, many people say it is. But to some computer users, the trade off seems fair. Hotmail, Yahoo Mail and AOL's Instant Messenger are among other software programs and services that display ads to their users in exchange for free usage. Many of these programs offer advertising-free versions for a price.

More infamous among adware watchers is Gator, which now goes by the name Claria Corp. Gator was controversial from the start. It began in 1998 offering e-wallet software. But it reports your Web surfing habits back to its parent company, which then sends you advertisements targeted according to your data. The vast majority of people consider it a pest, especially because the software is often bundled with other, more useful software. As annoying as it is, Gator is not very malicious.

As for adware that reports personally identifiable information, once again tolerance varies. Some people don't want any information, such as tracking the sites you visit, revealed. Others draw the line at logging IP addresses.

Viruses: Contagious Pests

For all the publicity viruses have gotten, they remain a serious threat. While viruses can potentially destroy a computer's data, most of the widespread viruses have leaned more toward annoyance. The most famous are e-mail viruses that replicate and spread using e-mail addresses stored on a computer. They still cost computer users and their employers hundreds of millions of dollars annually.

The MS Blaster worm that caused havoc in the summer of 2003 exploited a vulnerability in the Remote Procedure Call (RPC) function of the Windows operating system. Anyone who did not install a patch issued by Microsoft was vulnerable, marking a new era in virus prevention for many Internet users. No longer was using care with e-mail attachments enough to keep you safe.

Symptoms of Spyware and Other Pests

Depending on the type of pest that plagues your computer, it may be very easy to detect an infection. That's the good news. The bad news is some of the most dangerous infections, especially from RATS or spyware, can be very difficult to detect. That's why most of the checking and removing of pests is done with software designed to do just that. Nevertheless, there are some general symptoms you should know.

Your Computer Has a Mind of Its Own

Spyware, trojans and other pests contact other computers, and each pest is program of its own, therefore they use system resources such as CPU cycles, memory and an Internet connection.

Slow Computer

There are several reasons your computer may be running slow, but if you use it on a regular basis, then you're familiar with its noises, hang-ups and how it reacts. Older computers tend to run slower. Some applications cause computers to run slower. Computers are machines; they do not have moods. A sudden change in how your computer is running could be a sign of spyware or adware.

E-Mail Symptoms

If you're getting a lot of bounced back mail and see evidence of e-mails being sent without your knowledge, then it's possible that trojan spamware has found its way onto your computer. Spamware is a trojan that can turn your computer into a spam launching pad and create headaches for unknowing computer users, especially if it sends a virus. Even if your computer is not being used to send spam, trojans can steal a copy of your e-mail address book and send it back to a spammer.

Noises, Bells and Whistles

Victims of some trojans report CD drives opening and shutting, or programs opening and closing. Is your hard drive whirling away when you're not doing anything? Is there an unknown icon in your Windows system tray (lower-right corner of your screen)? If you have an external modem, there may be lights indicating data transfers blinking when you're not doing anything online. These are all signs a program may be up to no good in the background.

Offline Symptoms

Keyboard loggers can capture passwords and user names, so if the bank, brokerage or credit card accounts you access online appear to have been tampered with, your computer may be a place to start looking for clues. User names and passwords to e-mail and Web-based applications are also vulnerable.

If you have any reason to believe someone is interested in tracking what you do online, scan for spyware regularly.

Identifying Spyware: Malicious, Annoying or Misunderstood?

If you believe your computer has been infected with some sort of adware or spyware, there are a number of ways to identify the culprit. It's usually easier to identify adware because it is often less mischievous than spyware and can come from organizations that are widely considered legitimate.

Some adware sites consider Forbes.com Business Alerts to be adware because it run in stealth mode in the background. It also displays business news on your desktop. Some people have accused GoogleToolbar of being spyware because it includes a Page Rank feature that tells Google where people are surfing on the Web. Ironically, the Google Toolbar offers pop-up blocking, which can help keep unwanted ads and download windows from appearing as you navigate the Web. The Page Rank feature on the Google Toolbar can be disabled if you want to enjoy the benefits without any stealthy activity.

Most of the Web browser toolbars, like Google and the eBay Toolbar, (known as Browser Helper Objects, or BHOs) are technically spyware, but they are also useful to some people. Check this link for a fairly complete [list of BHOs and their file names](#).

Instant Messaging Pestware

An application called Buddylinks, which requires end-users to download, install, and agree to an end-user agreement, is known to spread marketing messages via AOL's Instant Messenger (AIM). It appears to be a recommendation from an AIM user that encourages contacts to visit a Web page to download a video game, such as the "Osama Found" game.

Buried in the software's accompanying End User License Agreement (EULA) is a statement that AIM users who download it explicitly give their permission to send marketing messages to their Buddy List contacts. In this way, the program can spread itself by sending links to the Web page — while seeming to come from a known contact.

For more information, [read this article](#):

Research Before You Download

Because spyware is often included with freeware and shareware, it doesn't hurt to do research on programs before you download them. A simple Google search, a visit to security-related forums, or checking sites devoted to spyware and anti-virus software can alert you to any problems people have reported with software.

Sites to Research Spyware

There are several databases online that track spyware and adware and give you information about the potential impact they can have on your computer.

- [Spywareguide.com](#)
- [Kephyr.com](#)
- [Computer Associate Spyware Encyclopedia](#)
- [Spybot Search & Destroy](#)
- [Counter Exploitation](#)

Locating Pests on Your PC

You'll find most annoying — yet legitimate — programs on a PC without much effort and with only a basic knowledge of where Windows keeps programs. The truly bad spyware programs make it much more difficult, because they have everything to gain from going undetected.

Your first stop should be the Add/Remove Programs section of your Windows Control Panel (Start Menu/Settings/Control Panel). You should also check the Windows Start-Up Folder (C:\Documents and Settings\All Users\Start Menu) to see if any programs have been added. If you are unsure of what a program is, check it against the spyware databases.

You'll also find evidence of spyware infestations in your computer's registry. Only experienced computer users should change the registry, and there are registry editors available that help makes changes when necessary. You can also use registry monitors to keep track of which applications are accessing your computer's registry.

Registry monitors include:

- [Active Registry Monitor](#)
- [Win-Expose-Registry](#)
- [Regmon](#)

Safe E-Mailing

You should know by now that opening spam or any e-mail from persons unknown or with an unexpected attachment is unwise. In addition to viruses, RATS (remote access [trojans](#)) and other programs can be present in e-mail attachments. Web sites advertised in unsolicited e-mail can try to plant dialers or other types of pests on your computer.

If you use Outlook or Outlook Express for your e-mail, there are settings you can adjust to make your e-mail safe from spyware and viruses. The Preview Pane, which lets you view e-mail while keeping your mailbox on the screen, has been a cause of concern among e-mail users, especially if scripting or ActiveX remains enabled. There have been reports of viruses, such as the [KAK-Worm](#), spreading by automatically opening e-mails. Malicious content like the

KAK-Worm exploits security holes in the software, so enabling or disabling the Preview Pane is not the ultimate issue. Keeping up with patches and security fixes is a better long-term solution.

To disable the Preview Pane in Outlook, click on the View menu. For more information on securing Outlook and Outlook Express, read this [article](#).

Safe Surfing

There's a lot to see on the World Wide Web, but you can't always be sure where it's coming from. If you visit Web sites that are not published by well-known publishers, it's even more important to regularly scan for pests. Pay close attention if you visit Web sites that advertise "too good to be true" deals or feature pornography.

Be careful what you download. Read all dialogue boxes carefully and close anything that looks suspicious. When closing dialogue boxes or pop-up advertisements, be sure to use the proper "X" to close the window. The Web is full of ads that feature mock "Xs" or "Close" or "OK" buttons within the ad. Clicking on them actually clicked on the ad itself. If you're not sure how to safely close a window that has opened in your browser, right click on the window in your Windows Taskbar (usually at the bottom of your display) and click on "Close."

Certain ads that appear online attempt to pass themselves off as security alerts or messages from tech support (these are called FUIs, or Fake User Interface ads). If you're using a computer within an organization, communicate with your tech support staff if you're unsure whether a message is legitimate, and familiarize yourself with how tech support communicates with the computer users in your organizations.

File-Sharing Applications and Spyware

If you use file-sharing applications to trade multimedia files, you are at a higher risk than most to be infected by spyware. There are a number of security risks posed by file-sharing software, including the installation of dialers and spyware bundled with file-sharing applications, as well as Internet connections that do not close and mislabel content.

We recommend that you read this [consumer alert](#) — issued by the Federal Trade Commission — about the use of file-sharing applications and the potential dangers.

File-sharing programs have created numerous headaches for colleges and universities, and several of them have set up Web pages alerting students to the legal and technical consequences of file-sharing software. Some of these pages give tips on minimizing the risk, while others attempt to dissuade the use of file-sharing completely. They serve as informative guides, especially if you need draw up your own policies. Examples include [St. Norbert College](#) and [Duke](#).

Browser Settings

The Windows operating system and Internet Explorer browser come with variable security settings. While the most convenient way to surf the Web might appear to be with the security settings on low, that's also the most dangerous.

Central to the issue of securing your Web browser is controlling ActiveX, which is the name for a set of controls that can be automatically downloaded and executed by your browser. While most of these controls are useful and help you experience content online, they can be used for malicious purposes.

Typically, you'll find that legitimate ActiveX controls are "signed" by their publishers. Ultimately, you want to OK the download of author-signed ActiveX controls and leave the rest alone. You can do this by adjusting your computer's security settings. Just follow these steps:

In Windows go to: Settings/Control Panel/Internet Options/Security. Highlight the Internet icon and click "Custom Level." Make sure the following settings are checked:

- Download signed ActiveX scripts = Prompt
- Download unsigned ActiveX scripts = Disable
- Initialize and script ActiveX not marked as safe = Disable
- Installation of Desktop items = Prompt
- Launching programs and files in a IFRAME = Prompt

You have now set your browser to alert you with a prompt when it attempts to download and install what could be legitimate content and ignore questionable content.

Now you want to check the list of "trusted publishers," which is a list of programmers (individuals or companies) whose ActiveX components can be downloaded without warning.

In Windows go to: Settings/Control Panel/Internet Options/Content. Click on the "Publishers" button. If you see any names on there you are not familiar with, delete them so their components cannot be installed without first prompting you.

Blocking Pop-Up Ads

One way to avoid the potential danger lurking behind pop-up ads is to install software that blocks and prevents them from appearing in the first place. Many ISPs offer tools to stop pop-ups from appearing. The Mozilla and Firefox Web browsers do not allow pop-ups. Even the Google Toolbar, which we discussed earlier, will block pop-up ads.

Microsoft added pop-up blocking to its Internet Explorer browser with [Windows XP Service Pack 2](#). The Service Pack also includes an updated Windows firewall and patches some holes exploited by hackers and worms.

Microsoft also has made [these instructions](#) available on how to set Internet Explorer in Windows XP Professional to block pop-ups. You can read them here:

You can find all kinds of [programs that block pop-up advertisements](#). Before installing them, research the developer and the company to make sure they are legitimate. Also be sure to note how they affect your system. Some pop-up blockers may discourage new windows — such as instant messages being sent to you — from opening.

Windows Messenger Pop-Ups

One form of pop-up with potentially dangerous effects is that's spam sent using the Windows Messaging feature in Windows XP. We don't mean the instant messaging software used by millions of people, but rather an administrative tool that systems administrators use to contact people on their networks.

While utilities that claim to stop such pop-ups exist, you can easily disable the Windows Messenger feature. Here's how:

In Windows XP go to Start/Control Panel/Administrative Tools. Double-click Services. Double-click Messenger. In the Startup-type list, choose Disabled. Click Stop, and then click OK.

ISPs and Spyware Prevention

The largest consumer Internet service providers (ISPs) have added spyware protection in the latest versions of their software to help keep consumers safe from online pests.

Once upon a time, it was anti-spam tools to help keep the e-mail inboxes of their subscribers clean. Now the attention had shifted to spyware. As with most ISP features, there is little to differentiate the spyware protection offerings among the major ISPs.

MSN

Microsoft's MSN ISP offers McAfee Security's anti-virus and personal firewall services as part of MSN Premium subscription service for broadband users in the United States.

MSN Premium subscribers receive McAfee VirusScan and McAfee Personal Firewall Plus desktop-protection services as part of their subscription to MSN Premium. MSN Plus and MSN Dial-Up Internet Access subscribers can access trial versions of the services and purchase them through the MSN site.

McAfee Personal Firewall Plus helps prevent potential hackers and other Internet threats from entering and infecting your PCs by acting as a protective barrier between the PC and the Internet.

EarthLink

EarthLink unveiled spyware protection in October 2003. Its Spyware Blocker works just like some of the [freeware removal programs](#), such as Spybot S&D. EarthLink subscribers choose when to run the program. It then detects and removes all common forms of spyware from their computer, including adware, system monitors, keyloggers, and Trojan horses.

America Online

AOL introduced AOL Spyware Protection as part of its 9.0 Optimized software. The product is actually software from

Aluria Software, which makes Spyware Eliminator, pop-up stoppers and optimizers. Unlike EarthLink, the AOL Spyware Protection automatically scans your computer once a week.

Members also can manually initiate a spyware/adware scan by clicking on the AOL Spyware Protection icon on their desktop, or they can set up automatic spyware scans at more regular intervals, such as daily/weekly or at a specific day and time. AOL regularly updates the Spyware Protection database to help members find and disable the latest spyware and adware applications.

Spyware Prevention Software

Much like anti-virus software that scans e-mail attachments as you go, some anti-spyware software packages aim to keep you safe as you surf. Many of these programs will detect cookies from advertisements or Web sites that may be helpful, so once again their effectiveness depends on your tolerance and how you use the software.

Spyware prevention software includes:

- [Spyware Inoculator](#)
- [SpySites](#)
- [SpyStopper](#)
- [SpyBlocker](#)
- [SpywareBlaster](#)
- [SpywareGuard](#)
- [Anti-keylogger](#)
- [Blue Coat ProxySG](#)

Secure Computing

By keeping up with the latest security patches and service packs, you will be plugging holes in your Windows operating system that could be used by malicious programs. Many people prefer to control their online privacy and don't like Microsoft's Automatic Updates feature. If that's true for you, a visit to [WindowsUpdate.com](#) will keep you up to date with the security patches your computer needs.

Firewalls

Many organizations already employ firewalls that are all but unseen to their computer-using employees. Personal firewalls are also a good way to stop malicious computers and programs from contacting your system. Microsoft Windows XP includes the Internet Connection Firewall. When enabled, it prevents would-be hackers from scanning your computer's ports and resources — including file and printer shares. It will also prevent RATs from contacting other computers if they are on your system. Enabling the firewall was essential to stopping the Blaster virus of 2003 and is also recommended for stopping Messenger Spam. To enable the Windows XP Internet Connection Firewall:

In Windows XP go to Start/Control Panel. Click Network and Internet Connections. Click Network Connections. Right-click your Internet connection, and then click Properties. Click the Advanced tab of your connection's Properties dialog box. Check the box next to "Protect my computer and network by limiting or preventing access to this computer from the Internet."

Firewall software includes:

- [Kerio Personal Firewall](#) [[Read the WinPlanet.com review](#)]
- [Zone Alarm](#) [[Read the WinPlanet.com review](#)]
- [Outpost Personal Firewall](#)
- [Sygate Personal Firewall](#)
- [eTrust EZ Armor](#)
- [BlackICE](#) [[Read the WinPlanet.com review](#)]

More Spyware, Adware and Trojan Resources

- [Safe Hex, Safe Computing Tips](#)
- [Pestware 101](#)
- [Anti-Mal 101](#)
- [eSecurityPlanet](#)
- [CEXX.org Spyware Discussion Boards](#)

- [Anti-Virus Protection 101](#)
- [Fending Off a Vicious Attack](#)
- [Deflecting Assaults on Privacy](#)
- [Dealing with Sneaky, Slimy Malware](#)
- [AntiOnline Spyware/Adware Forum](#)
- [Spyware and Adware Resources from About.com](#)
- [Malware: Is Your Workstation at Risk? Part 1](#)
- [Malware: Is Your Workstation at Risk? Part 2](#)
- [PCs Monitored, E-mail Bugged](#)
- [A Web of Electronic Denial](#)
- [Ad-Aware Review from WinPlanet.com](#)
- [AntiOnline Spotlight: Spyware Protection for Networks](#)
- [Spyware Solutions Not So Simple](#)
- [Spybot Search & Destroy Review](#)
- [An Arsenal to Combat Spyware](#)
- [Spyware Sneaking into the Enterprise](#)