

Computer Infections: Spyware and Virus

Spyware is a program that surreptitiously monitors your actions. While they are sometimes sinister, like a remote control program used by a hacker, software companies have been known to use Spyware to gather data about customers. The practice is generally frowned upon.

A virus is a malicious (usually) computer program that can travel surreptitiously from computer to computer.

The most marked difference between spyware and viruses are:

Virus writers have to remain anonymous on threat of prosecution, whilst spyware authors actively publicize and financially benefit from their malicious actions. The money spyware authors earn allows them to hire expert programmers to create more sophisticated spyware, perpetuating the cycle.

There are a number of companies that actually provide spyware development services, and will create custom spyware applications to your specifications. It's a very thin legal line, but companies continue to try and follow it.

If you believe the stories, the Internet is not a safe place. At every click, you run the risk of your computer being silently coerced into giving up passwords, credit card details, and private documents. You hardly dare visit a new Web site for fear of being targeted by this malicious software. Fortunately, the reality is somewhat different, and in this course, you'll learn the truth behind spyware.

The Problem with Spyware

At first glance, the spyware issues may seem quite obvious and easy to avoid. Unfortunately, the hallmark of really good spyware is that you don't know you're about to become a victim until it's too late.

As mentioned, although spyware is commonly associated with malicious Web sites, it quite regularly gets bundled with legitimate software by less than scrupulous developers. And just to really push the point home, many software developers include a clause in their **EULA** (End-User License Agreement) that prevents you removing the spyware if you want to continue to use the application. The eDonkey P2P client is just one example of this.

Although spyware tied to applications is relatively easy to avoid or disable, Web-based spyware is a whole different game, as discussed in the following sections.

First of all, it's important to understand that the term **spyware** is often used as a generic catchall category that lumps together a number of distinctly different software traits. A perfectly normal application can easily be classified as spyware because of a single function it performs, when in reality, the function in question is legitimate. For example, the **File** menu in Microsoft Word; when you click it, a list of the most recent documents the application used to access is visible at the bottom of the menu.

This type of functionality is called a **usage tracker** and is harmless; in fact, it enhances your experience and productivity. However, if a hidden application running on your computer without your knowledge silently tracks every document you open, and then stores this information for later use, it's considered malicious.

Go to ComputerRecover.com for a free download of the highest rated spyware remover on the market today.

Web site **cookies** are an interesting extension of usage tracking; not only do they allow Web sites to provide personalized interfaces such as user accounts, but they also allow in-depth tracking of Web browsing behavior. **Adware** works on a similar principle and is also generally harmless, although often irritating. You've probably seen some shareware or freeware applications that, instead of having limited functionality to encourage you to register, display context sensitive advertisements in a window. It's common for shareware applications to use adware techniques to earn their creators some money through advert syndication, especially **P2P** ([Peer to Peer](#)) clients such as [Kazaa](#) or eDonkey, shown in Figure 1-1.

Advertisement syndication is a simple method for application programmers and Web site designers to earn money from their products. They sign up for syndication programs with an online advertiser and create a link to an application running on the advertiser's server. The advertiser uses this application to automatically provide different advertisements (normally in a graphic image format such as GIF or JPEG) to the requesting application or Web site.

Every time a new advertisement is downloaded and displayed to a user, the programmer or Web site designer earns a tiny amount of money, sometimes as little as \$0.01. The more people that use the application or view the Web site, the more money the designer or programmer earns. Because millions of people use P2P clients, a successful programmer can quickly earn a significant amount of money!

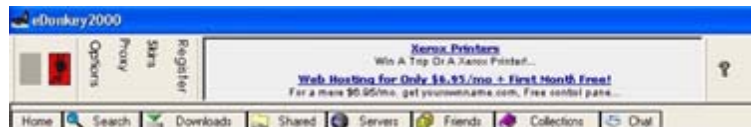


Figure 1-1: The eDonkey P2P client displays tracking advertisements in the toolbar.

Adware

There are a number of privacy concerns with adware, mainly because the advertisements displayed within the application are retrieved from a remote server on the Internet. As each advertisement is requested, the remote server logs your computer's IP (Internet Protocol) address and the time of the request, as well as other details. If you use the application over a period of time, the owners of the remote server can easily do the following:

- Build a picture of your usage of the application.
- Note the times you're most likely to be at the computer.
- Note the length of time you use the application.
- Note what you like doing when you use the application.

P2P Clients

P2P clients are also often the source of less innocent, true **spyware**. In this case, the term spyware is used to refer to a specific type of malicious application rather than as a generic term. A common technique with many of these clients is to silently include a spyware application within the installation process. The Kazaa P2P client is notorious for doing this and includes (among other things) an application called **Gator**.

Gator is also a **Trojan** application that masquerades as a legitimate and useful program when, in reality, it's anything but. It integrates itself into the operating system and monitors

Go to [ComputerRecover.com](#) for a free download of the highest rated spyware remover on the market today.

which Web sites are viewed and which applications are accessed. This information is used to display pop-up advertisements directly on your desktop, containing supposed special offers for products that might interest you. One of the most concerning "features" of Gator is its ability to store commonly used information for Web page forms. This is great if you want to save yourself from repeatedly entering your name and e-mail address, but not so good when Gator remembers your credit card number and gives it to Web sites without your consent.

Malware

Finally, and most seriously, there's an application category known as **malware**. This is software specifically designed to invade your computer, hijack normal operating system and application functions, and actively prevent you from removing it. The only difference between malware and a generic virus is that malware generally makes itself known through its visibly destructive actions. Some well-known examples of malware include the C2.Lop program, and the infamous CWS (CoolWebSearch). Some variants of CWS actually invade the Microsoft Windows networking subsystem, integrating themselves with the operating system, which makes them difficult to remove.

Browser Hijacking

Web-based spyware usually targets security vulnerabilities within Web browsers to install itself and modify the browser's functionality. This is commonly referred to as **browser hijacking**. The most basic form of hijacking is **home page hijacking**. As the name implies, a Web site author can use JavaScript functions to set a browser's home page to any Web site he selects. Although this may seem pointless and nothing more than a minor inconvenience, if the new home page is full of syndicated advertising banners, the author can quickly generate a lot of money from hijacking Web browsers. If you're unlucky, the new home page is a malware download site that infects your computer.

Spyware Categories

Economics drives the entire spyware industry, so it's no wonder that its creators want to make spyware as hard to remove and avoid as possible. The vast majority of Web-based spyware falls into one of three categories:

Toolbar hijacks: The most common types. They place a custom toolbar within your Web browser that displays advertisements and tracks your Web browsing.

Functionality hijacks: Prevents your Web browser and operating system from functioning normally. In some cases, they pop up application windows and advertisements on your desktop at random.

Dialer applications: Forces your computer to dial premium rate and international phone numbers at random times.

It's often a fine line between spyware and legitimate software, because many spyware applications include useful functions. A good example of this is [Alexa](#), which monitors the Web pages as you browse and displays links and advertisements related to the page content. Some users may find this a handy way to find related products and information, whereas others may consider it annoying and an invasion of privacy. Alexa is owned by Amazon.com, which does give it some legitimacy.

JavaScript is a scripting language used to create interactive Web sites. Netscape originally designed it.

Go to ComputerRecover.com for a free download of the highest rated spyware remover on the market today.

Web-based spyware refers to spyware that's maliciously installed from Web sites, as opposed to application-based spyware, which comes bundled with legitimate applications. Although Web-based spyware may originate from a malicious Web site, it doesn't necessarily need an Internet connection once infection has taken place. Dial-up Internet access is not a safeguard!

Porn dialers are almost solely responsible for bringing the topic of spyware into the popular media. Not only do these programs run up huge phone bills by making long distance calls, but there have also been numerous occasions where they've also downloaded illegal pornography to the victim's computer. In one case, legal authorities monitoring certain Web sites discovered these downloads, and the unfortunate victim's innocence was only proved after an independent security researcher discovered the dialer program.

Spyware Mechanisms

All Web-based spyware is dependent on being able to use features and security vulnerabilities within a Web browser to infect a computer. Part of the reason that spyware is difficult to defend against is that the features used to infect a computer are often the same as those used by legitimate software to enhance functionality. The first step in defense is to understand how spyware and malware work.

The life of spyware can be split into the following three stages:

Exploitation: Occurs when a malicious Web site exploits a feature or security vulnerability in your browser and gains enough access to your computer to start causing problems. It's an unfortunate fact those Web browsers, especially Microsoft Internet Explorer, have plenty of security flaws in them.

Infection: When the **payload** (the part of the spyware that actually does the damage) is downloaded to your computer via the security hole created in stage one.

Operation: Takes place as the spyware completes its tasks, such as displaying toolbars, sending Web browsing information to its creators, or dialing premium-rate phone numbers.

Misuse of Features

All Web-based spyware is dependant on being able to exploit features and security vulnerabilities within a Web browser to infect a computer; without the features and flaws, infection isn't possible. One of the most common methods of attack is through **ActiveX** controls. These are small programs downloaded to your computer to provide special functionality not available through basic HTML (Hypertext Markup Language) script, such as a Web-based interactive pie chart creator. However, because these are executable programs whose purpose is to extend the functionality of the Web browser, the developers of these controls have extensive access to the internals of both Windows and the Web browser.

Similarly, the **active scripting** functionality within Internet Explorer is a two-edged sword. Many security vulnerabilities have been found within both the ActiveX management system and the active scripting system, and the access these systems are granted by default makes it extremely easy for a malicious Web site to infect a computer. Internet Explorer Security Zones are supposed to prevent these types of security issues, but unfortunately, even this system has been proven unsecure.

Go to ComputerRecover.com for a free download of the highest rated spyware remover on the market today.

Browser Helpers

Once spyware has exploited a security vulnerability, the payload is installed on the victim's computer and usually hijacks Web browser functions. The most common hijack technique is to use a BHO (Browser Helper Object). A **BHO** is a DLL (Dynamic Link Library, a special type of executable file) that has complete control over Internet Explorer, allowing it to monitor and change anything it wants.

When Internet Explorer starts, it looks through the Registry for all installed BHOs, and loads each one in turn. Although this may seem perfect for little other than spyware, it's actually an extremely useful plug-in system. Download managers and other utilities, such as [FlashGet](#) or [GetRight](#); use BHOs to seamlessly integrate their functions with Internet Explorer to enhance its functionality. Although BHOs are commonly associated with toolbars and visible functionality changes, there's no requirement for this -- it's perfectly possible for a BHO to be installed and never announce its presence. Perfect for spyware.

Linking Web Browsing and Windows

Other types of hijacking exploit the tight links between Internet Explorer and Windows. It's common for spyware to use Windows policies to force the computer to act a certain way; for example, to change the Internet Explorer home page, and then set a policy to prevent you from changing back. This type of hijacking can be very difficult to reverse because it uses the Windows security system. In other words, to remove it, you actually fight Microsoft's security mechanisms!

Spyware can also use the multiple ways Windows knows to automatically start an application on boot, ensuring that the spyware is always running. Once running on a victim computer, many types of spyware actively seek out anti spyware tools and attempt to disable them. They also manipulate the Windows networking system to prevent the unfortunate user from even downloading anti spyware tools. Many of these programs are deliberately named to sound like legitimate operating system files, for example **svchost32.exe**; the legitimate Windows program is named **svchost.exe** and deleting the wrong one can cause serious damage.

Trojan Web Pages

One problem that's becoming more widespread is the use of Trojan Web page techniques to keep a computer infected. Newer versions of Windows, such as Microsoft Windows XP and Microsoft Windows Server 2003, use custom Web page interfaces to provide access to operating system functions. If spyware infects these pages, no matter how many times you delete the spyware-related executable files and Registry entries that appear, every time you access the infected management page, the spyware re-infects your computer. This is a technique used by the CWS malware.

Although this may seem like a desperate situation, things aren't as bad as they sound. Although spyware is annoying, a security risk, and in some cases very difficult to get rid of, all is not lost. It's your computer and you have overall control over it. You can remove most of the spyware and malware either manually or with an automated tool. Best of all, most spyware is very well known and removal techniques have been studied in depth by anti spyware researchers. If you do have spyware, it's not the end of the world.

Go to ComputerRecover.com for a free download of the highest rated spyware remover on the market today.

Defeating Spyware

Where is the Spyware Doctor?

After spyware has installed itself, there are three distinct investigative steps to resolve the problem:

Location: Sometimes computers misbehave at random for reasons other than spyware. Installing new drivers, running a new application, or even getting a virus can cause a computer to misbehave. All of these are problems that need resolving, but spyware diagnosis techniques won't help. Therefore, the first step in defeating spyware is to actually locate it and confirm that it is spyware.

Diagnosis: You've located a suspicious Registry entry or an unusual executable file, but how do you know what to do next? Just like viruses or normal applications, every piece of spyware is different. Before moving on to the next stage, it's essential to discover exactly which piece of spyware has infected your computer.

Removal: After you know the type of spyware affecting your computer, you can begin the removal process. Whether you use an automated removal application or decide to remove it manually, the process is made far easier by knowing exactly which type of spyware you're working with.

Locate the problem, diagnose it, and then remove or treat it -- almost the same process a doctor would use to treat a disease! You learn more about how to do this throughout this lesson.

Is Your Computer Infected?

That's a good question: How do you know if you're already a victim? In most cases, the results are obvious:

- Browser toolbars and other BHOs appear.
- Your browser home page is changed.
- You can't access your Web browser configuration settings.

In these cases, you immediately realize there's a problem, and move to the diagnosis stage.

Some spyware is not so obvious and easy to spot. On the whole, your operating system and Web browser may appear to work correctly, but random advertisements appear as you browse and Web sites you used to be able to get to are no longer accessible. Some spyware is downright sneaky.

Jumping to Conclusions

The moment your computer starts doing something funny, it's very easy to immediately conclude that spyware must be the cause. In reality, most people have fairly fixed Web browsing habits and visit the same small set of Web sites repeatedly, only visiting new Web sites when prompted to by links or e-mails. In this scenario, it's relatively rare to become a spyware victim, especially if the Web sites browsed are respectable ones.

Quite often, a slow computer can be because of failing hardware, a fragmented hard disk, or too many utility programs running in the background. If you think your computer has been infected by spyware, follow the investigative steps in this report, but don't rule out other causes straight away.

Go to ComputerRecover.com for a free download of the highest rated spyware remover on the market today.

Locating Spyware

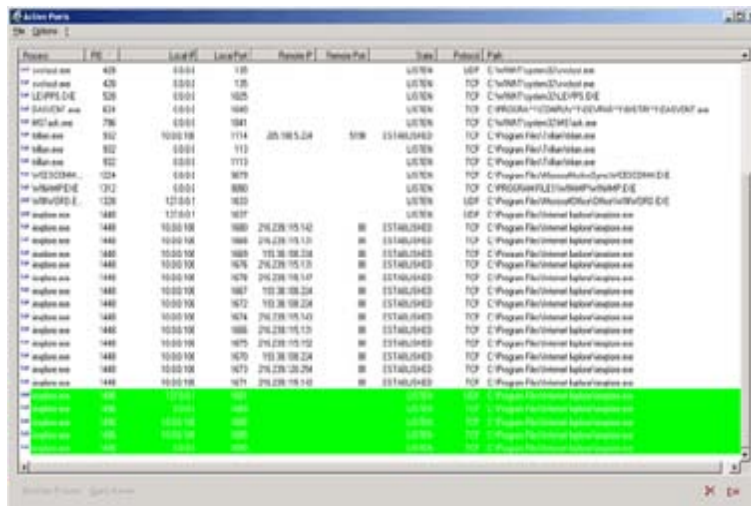
The easiest way to locate hidden spyware is to investigate the mechanisms spyware uses to hide and do its work. A lot of spyware communicates back to its creators via the Internet. An easy way to verify communication is occurring is to view all of the current, active network connections on your computer using [Active Ports](#).

Active Ports is an essential tool that lists all incoming and outgoing connections for all the active network connections, such as your Internet dial-up or broadband connection.

WARNING
 Before continuing, make sure you exit all open applications on your computer and wait for at least one minute. Doing this makes the data you're about to see easier to decipher.

The Active Ports window in the figure is split into a number of columns, the most important of which are:

- Process:** Lists the filenames of all programs that currently have active network connections.
- Path:** Lists the exact location of each process.
- Remote IP:** Lists the IP address of the server to which the process is connected.
- State:** Shows whether the process is making a connection to the server or waiting to answer an incoming connection request.



Using the output from Active Ports, it's easy to see whether any rogue processes are making network connections. Even more useful is the ability to watch for new connections being made. As an example, open Microsoft Internet Explorer and wait until your home page loads (if your home page is a blank page, browse to a Web site you normally use). Quickly switch back to Active Ports, and you'll see a new entry in the window highlighted in green similar to Figure 2-1. The process name is **iexplore.exe**, and the IP address of the Web server that hosts your home page also appears in the list. After the page has loaded, a few seconds pass and the Active Ports entries that were highlighted in green turn red. This signifies that the

Go to ComputerRecover.com for a free download of the highest rated spyware remover on the market today.

connection is now closing.

Task, program, process, executable; what's the difference? Microsoft use these specific terms to refer to the individual parts of an application. **Executable** is the technical term for a program --a file stored on disk that can be executed. After an executable has been launched, it becomes a **task**. A task is an executable loaded into memory and working away, and is used as a container for a process. A **process** is an individual piece of code that performs a specific action. The action can be quite complex such as providing a user interface or downloading a file. For example, when Microsoft Outlook is launched, under the Outlook task, there's an **outlook.exe** process that handles the user interface and a **mapisp32.exe** process that handles the sending and receiving of e-mail. You can view the tasks and processes running on your system by clicking **Start > Run** and then typing **taskmgr**. Alternatively, press **Ctrl+Alt+Del**, and then click the **Task Manager** button.

TIP

Active Ports highlights new connections in bright green, and terminating connections in bright red.

If spyware is present on your computer and is communicating to a remote server, you'd spot it in this list. The best method for investigating this is to close all applications, open one Internet Explorer window, and then watch the Active Ports output for a while. If spyware is communicating with a remote server, it usually gives itself away here.

WARNING

If you use Norton Antivirus, you may find that Active Ports (and other similar, legitimate tools) are detected as spyware. This is actually a false-positive, and can be safely ignored. These tools are not spyware and do not contain malicious code.

Alternatives to Active Ports

You may find the following tools helpful alternatives to Active Ports (some students taking this class have reported that Active Ports doesn't with Windows ME): [FPort](#) from Foundstone [TCPView](#) from Sysinternals

The Sysinternals site has some other very useful utilities on it, including [Handle](#). Handle will show you exactly which processes are opening what files on your system. (Note: The Handle link is for Win2k and XP only. There is a Windows 95/98 specific section on the left hand side of the Sysinternals page.)

WARNING

Microsoft Windows itself will quite often seem to make network connections at random. The only way to separate these legitimate connections from malicious, spyware connections is through experience. You'll learn some useful tips later in this lesson.

Leaving Tracks

Another favorite spyware trick is to fill up your hosts file with invalid entries for valid Web sites. When you type a **URL** (Uniform Resource Locator) into your Web browser, such as

Go to ComputerRecover.com for a free download of the highest rated spyware remover on the market today.

<http://www.cnet.com>, the Windows network stack uses various methods to resolve the FQDN (Fully Qualified Domain Name, for example **www.cnet.com**) into an IP address.

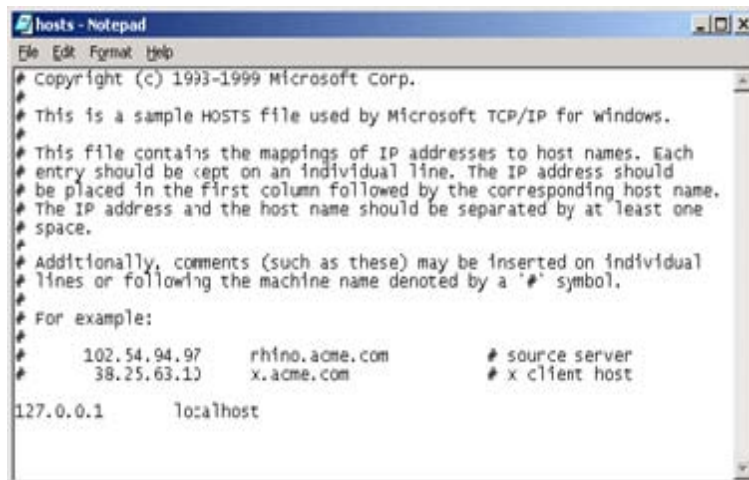
The first method Windows uses is to interrogate the hosts' file. This is a plain-text file, shown in Figure 2-2, stored deep within the Windows directory structure that contains a list of FQDNs and the IP addresses to which they resolve.

If you use Windows NT or 2000, the hosts file is named "hosts" and can be found in c:\winnt\system32\drivers\etc. If you use Windows XP, it can be found in c:\windows\system32\drivers\etc. For Windows 98 and ME, it's in the

System or Spyware?

It can be very difficult to decide whether an executable is a legitimate system or application file, or malicious spyware. Sometimes the directory it resides in is a good indication, but many spyware programmers deliberately write their files to the Windows system directory and name them as close to legitimate system filenames as possible. Before deleting any files you should always search the Web for the filename in question.

If spyware adds the FQDN of a Web site to your hosts file along with an incorrect IP address, you cannot access that Web site. This could be a real problem if the Web site in question is **www.download.com**, and you need to download a spyware removal tool. Under normal circumstances, a hosts' file has one 127.0.0.1 entry as in Figure 2-2; if yours has a lot of entries for Web sites, something suspicious may be going on.



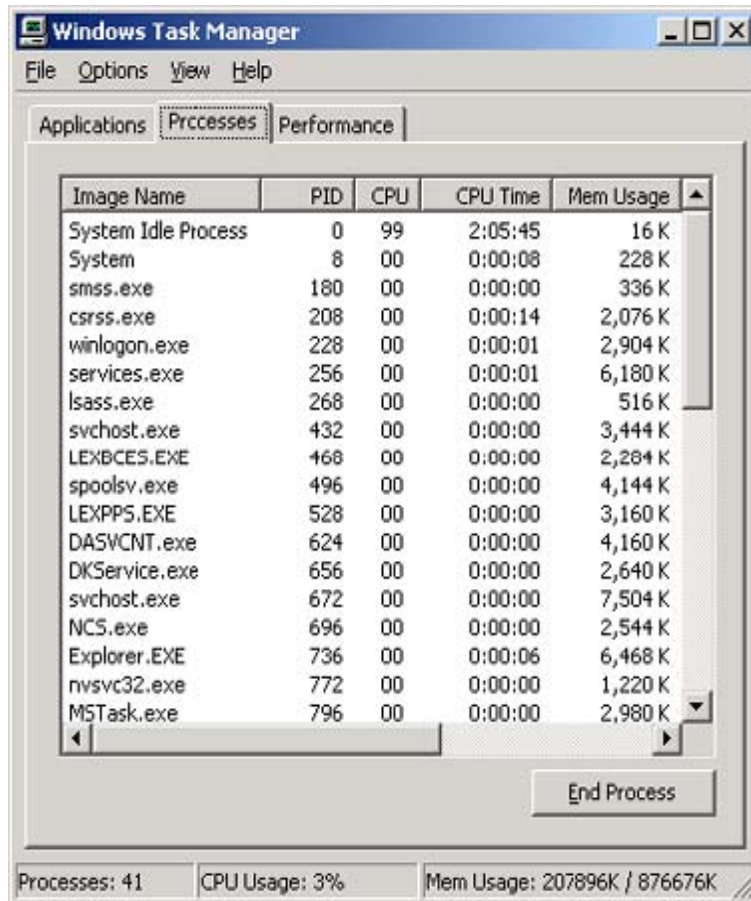
```
hosts - Notepad
File Edit Format Help
# Copyright (c) 1993-1999 Microsoft Corp.
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
# For example:
#       102.54.94.97       rhino.acme.com           # source server
#       38.25.63.10      x.acme.com               # x client host
127.0.0.1       localhost
```

Locating Bad Processes

If spyware is running, it will invariably show up as a process on your computer. Fortunately, the filenames and Registry keys used by all but the newest spyware are well known -- thanks to the efforts of anti spyware researchers. A quick way to determine whether any spyware processes are running is to view the current task list through Windows Task Manager, as in figure below.

Go to ComputerRecover.com for a free download of the highest rated spyware remover on the market today.

Diagnosis: Search your favorite search engine, such as Google or Search.com. Also visit the [WinTasks Process Library](#) to see which processes are specific to Windows.



As mentioned previously, the only sure-fire way to know if a rogue process is on your system is to gain experience in which processes are harmless and common. If you do spot a suspicious process, make a note of the process name and use the End Task button to kill it. Next, use the Windows Search function to locate the file on your hard drive. Don't delete it immediately though -- it may be an innocent system file!

Diagnosis with Spyware Doctor

The next step in the process is to make a final diagnosis. Although it's an interesting exercise to read up about specific types of spyware and try to manually diagnose the problem, this can get very time consuming. Fortunately, there are plenty of great anti spyware utilities available, most of them free. Antispyware tools are a growth industry and new, commercial applications are appearing all the time, just like antivirus software. Popular software includes Spyware Doctor, Webroot Spy Sweeper, and HijackThis.

Spyware Doctor is an all-purpose antispyware tool, and has been voted both CNET Best Anti-Spyware utility and one of the CNET [Top 10](#) programs on Download.com. It can fix both Web browser-based spyware and application-based spyware, as well as remove usage tracks from applications and immunize your computer against future infection.

Go to [ComputerRecover.com](#) for a free download of the highest rated spyware remover on the market today.



[Downloading Spyware Doctor](#) is simple. It features an easy-to-use set-up wizard. When you set it up, be sure to select the option that allows you to get the latest spyware definitions -- that option is critical to ensuring that Spyware Doctor uses the most up-to-date defenses to protect your system from the latest threats. Once you get Spyware Doctor installed, you'll be all set to run your first sweep. Just click the START button and Spyware Doctor will do the rest.



When the sweep is done, study the results of what Spyware Doctor found. You can click on the individual items found to learn more about them, or you can quarantine them with a click of the button. Putting found spies in quarantine effectively removes them from your operating system but gives you the option of restoring something later if you choose. Spyware Doctor also gives you the flexibility to automatically allow or remove certain spies so you can save time and focus on new potential threats. This is done under the Options section.

You can also set Spyware Doctor to run automatically on a pre-determined schedule. Just click the Options button on the left, then click the Schedule tab at the top, and set it to meet your specifications

Spyware Doctor highlights some items. The green items are usage trackers, so look at those

Go to ComputerRecover.com for a free download of the highest rated spyware remover on the market today.

first. Pick any green item in your list, and click the + symbol to its left to expand the item. A list of all the usage tracks relating to this item appears underneath, showing the exact Registry keys that do the tracking. You may be surprised at exactly what some applications store usage tracks of!

If you're sharing your computer and want to maintain your privacy, deleting these values is a good idea. The green items aren't serious spyware risks, so leave them unchecked.

Next, locate a red item and expand it. If your computer is truly spyware-free, all of your red items will be **tracking cookies**. Tracking cookies are interesting examples of the issues with adware systems. You've probably never visited the Web sites that show up as storing tracking cookies on your computer. However, you've probably visited other Web sites that use advertisement syndication from these listed Web sites; therefore, your browsing history is being tracked.

Tracking through Advertisements

What's very concerning is when different Web sites use the same advertisement syndication system, enabling the advertisement syndicate owner to track your browsing to completely unrelated and different Web sites. As a simple example, imagine that you browse to a pet shop Web site, followed by a dog owner information Web site, and finally to a dog food vendor's Web site. If all those Web sites use the same advertisement syndication system, someone can very quickly figure out that you own a dog! Apply the same process to visiting a credit card company, a loan company, and a debt management organization and the consequence of tracking through advertisements becomes more concerning.

If the worst has happened and you're infected with spyware or malware, Spyware Doctor shows these items too. Make a note of any items listed that aren't tracking cookies and keep it safe.

A **proxy server** is a server based somewhere on the Internet that will receive your requests for resources, such as Web pages or files on an FTP (File Transfer Protocol) site, download them on your behalf, and then send them to you. Just as you can register for a proxy to vote in an election on your behalf, you can use a proxy server to delete absolutely anything it believes is using a feature that spyware may use. Some items listed by Spyware Doctor very often are not spyware! Do not, under any circumstances, use it to fix or remove any items you're not absolutely sure about.

Incorrect Removal

Although Spyware Doctor may have given you a list of the spyware it found, you shouldn't just jump straight in and remove it. Some spyware masquerades as a different type of spyware, and incorrect detection doesn't result in correct removal. The mantra for this stage is search, search, search again, and search a little bit more to be sure.

An hour spent searching at this point can save hours of frustration and problems later. There are too many types of spyware and malware that will actively try to damage your system if removed incorrectly, so make sure you know what you're dealing with.

With automated tools such as Spyware Doctor, removal of spyware is generally as simple as selecting the Fix option. There's one piece of spyware that does merit a special mention due to its nastiness: **CWS**. Variants of this malware integrate deep inside Windows, making removal very difficult. If you're unfortunate enough to be infected by this menace, a great

Go to ComputerRecover.com for a free download of the highest rated spyware remover on the market today.

tool called [CoolWebShredder](#) can generally fix the problems.

Spyware Prevention

As the saying goes, prevention is better than a cure, and that's certainly the case where spyware is involved. There are some simple steps you can take to minimize the risk of spyware infection. Try [Spyware Doctor](#) for an install-and-forget-it software utility.

Web Browser Security

Although Internet Explorer zones aren't a reliable security mechanism, they do provide some protection. Place the Web sites you know and trust into the **Trusted Sites** zone, and increase the security on the **Internet** zone. Internet Explorer uses the Internet zone for any Web site that isn't listed in one of the other zones; therefore, its security settings apply to the majority of sites you visit.

As a minimum, make sure all the ActiveX and Active Scripting features are disabled. If practical, consider switching to another Web browser such as [Firefox](#) .

TIP

Although Internet Explorer is probably the worst culprit, all Web browsers have security flaws so it's essential you stay up to date with security patches.

Personal Firewalls

Apart from being essential, if you're directly connected to the Internet, a personal firewall can act as an early warning system against spyware that communicates home. Earlier in this lesson, you used Active Ports to monitor network connections; most personal firewalls do this in the background and alert you when a process tries to connect to a remote computer.

There's a huge [selection](#) of personal firewall software from which to select, including [ZoneAlarm](#) and [Kerio](#) Personal Firewall (formerly known as Tiny Personal Firewall).

Update Your Antivirus Software

Although antivirus software isn't designed to catch spyware, most desktop packages catch the methods spyware uses to infect your computer. This mainly happens through the Web browser cache -- when your browser downloads a Web page and stores it on disk, antivirus software intercepts the page as it's stored and analyzes it for viruses. Many JavaScript security exploits are categorized as viruses, so your antivirus software can also act as a warning system. GriSoft [AVG](#) is an excellent free antivirus suite.

Immunization

[Spyware Doctor](#) can immunize your system against spyware. By setting various Registry keys and creating dummy files, Spybot immunization can fool a significant amount of spyware into thinking it's already installed, preventing it from really infecting your computer. Spybot also includes a BHO that watches Web page requests within Internet Explorer. If it detects an attempt to load a known adware-based usage tracker, it will prompt you whether you want to allow it to continue.

Make Backups

Making regular backups of your system is a good idea anyway, but has the added advantage of letting you restore a previous, spyware free configuration in case your computer gets infected. Windows XP Restore Points are also perfect for rolling back to a clean version of your system. In Windows XP, select **Start > All Programs > Accessories > System Tools > System Restore**, and then follow the instructions.

Use a Proxy Server

Go to [ComputerRecover.com](#) for a free download of the highest rated spyware remover on the market today.

Although this won't prevent some types of spyware from infecting your system, most proxy servers can scan content before downloading it. This lets them trap malicious Web pages and usage trackers before they reach your computer. As an added bonus, all your Web browsing will appear to come from the IP address of the proxy server -- considering most proxy servers provide access to hundreds of users, usage tracking systems will be mostly avoided. There are plenty of anonymous proxy servers available for your browsing use.

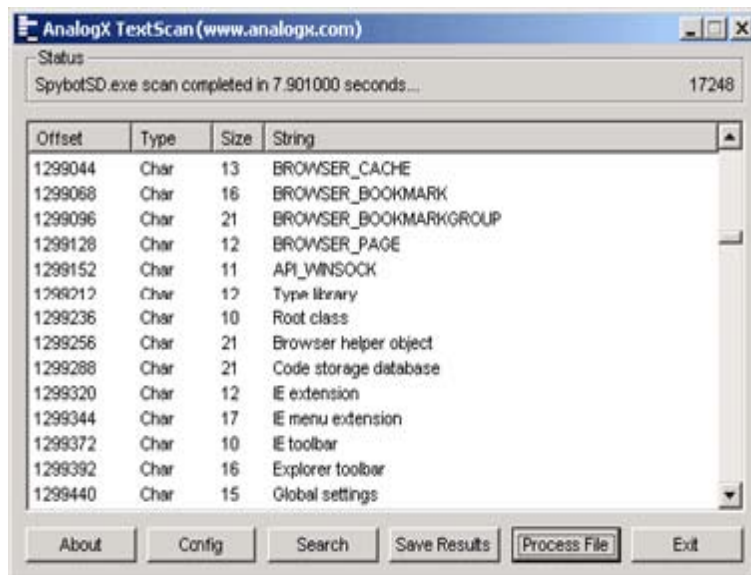
For You Computer Nerds

Spyware is a nasty trend that needs to be stopped immediately, but it does have an upside. One of the most interesting and challenging areas of research is trapping, analyzing, and defeating new spyware. We all rely on the dedication of the people who do this work for free, making it possible for everyone else to remove and avoid spyware.

Becoming an expert in reverse engineering is a long and difficult path, requiring the mastery of many different skills. The best reverse engineers can usually program in two or three different programming languages, including assembly, as well as know the hardware and operating system inside out. Although the individual skills can be difficult to master, the process is simple to follow.

Most researchers start with a dedicated computer that has a basic installation of Windows, as well as a few common antispymware tools. They then take a snapshot of the operating system using a setup wizard creation tool (for example, [Masai Editor](#)), and then deliberately infect the computer with the spyware target. The setup tool is run again, and produces a difference file that lists all the changes that occurred since the previous snapshot. This immediately allows the researchers to understand what changes the spyware has made.

The difference file probably contains a number of spyware executables that have been downloaded to the computer during infection. The researchers isolate these files and begin an analysis.



Every Windows executable must follow a very strict file structure, known as the **PE Format** (Portable Executable Format). This format tells Windows about the size of the file, which **resources** it contains (for example, icons, bitmaps, or cursors), and most importantly from a researcher's point of view, something called the **import table**. The import table is a list of all the operating system functions the executable uses; for example, to put a message box on screen, the import table includes the Windows function **MessageBoxA**. By analyzing the functions listed in the import table, a researcher can quickly determine whether the spyware target communicates over the Internet, writes files to the hard disk, or monitors Web pages as they load.

Go to [ComputerRecover.com](#) for a free download of the highest rated spyware remover on the market today.

Next, researchers extract **strings** from the executable to search for interesting text. If the spyware target writes URLs to the hosts file, the URLs will usually be clearly visible inside the executable file. An excellent string extraction tool is AnalogX [TextScan](#), shown in the figure below.

After all of the background information has been gathered, researchers begin work on reverse engineering and disassembling the spyware target. Using tools such as [Neuron PE Disassembler](#) or [Proview Disassembler](#), the executable target can be converted into assembly language source code. Using a live debugger such as [OllyDebug](#) and the assembly source code, known as the **dead listing**, a researcher can follow the logic of the spyware target and understand exactly how it works.

Antivirus companies such as Symantec and Network Associates use these same techniques to reverse engineer viruses and produce antivirus software. As you can probably imagine, these skills take years of study and dedication to master.

Glossary

Adware

while not necessarily malware, Adware is considered to go beyond the reasonable advertising that one might expect from freeware or shareware. Typically a separate program that is installed at the same time as a shareware or similar program, Adware will usually continue to generate advertising even when the user is not running the originally desired program. See also cookies, Spyware, and Web Bugs.

Backdoor

A backdoor in a computer system (or a cryptosystem, or even in an algorithm) is a method of bypassing normal authentication or obtaining remote access to a computer, while intended to remain hidden to casual inspection. The backdoor may take the form of an installed program (e.g., Back Orifice) or could be a modification to a legitimate program.

A backdoor in a login system could take the form of a hard-coded user and password combination which gives access to the system. A famous example of this was used as a plot device in the 1983 film WarGames, wherein the designer of a computer system had inserted an undocumented application (named after his son) which gave the user access to the system.

BHO - Browser Helper Object

A browser helper object, or BHO, is a plug-in for the Microsoft Internet Explorer web browser. The BHO application programming interface exposes hooks that allow the BHO to access the document object model of the current page and to control navigation. Each BHO is a COM object inside a DLL that is loaded by new instances of Internet Explorer. The Google toolbar is an example of a BHO.

Cookies

Persistent Client-State HTTP Cookies are files containing information about visitors to a web site (e.g. user name and preferences). This information is provided by the user during the first visit to a web server. The server records this information

in a text file and stores this file on the visitor's hard drive. When the visitor accesses the same web site again the server looks for the cookie and configures itself based on the information provided.

Malware

A generic term increasingly being used to describe any form of malicious software; eg, viruses, Trojan Horses, malicious active content, etc

Phishing

A form of Identity Theft - typically an e-mail is sent to you that looks like it comes from a legitimate company (E-Bay has been a typical target) telling you that you must update your records and verify your username and password. The site is really a place to collect that information from you and steal your identity, money, records and whatever they can. Congress is trying to work on laws to help, but based on the ineffective Can Spam act, it is doubtful to help. Knowledge is the most effective preventive mechanism today - Legitimate companies do not ask you for your login information by e-mail.

Spam

(From Hormel's Spiced Ham, via the Monty Python "Spam" song) To post irrelevant or inappropriate messages to one or more Usenet newsgroups, mailing lists, or other messaging system in deliberate or accidental violation of netiquette.

To indiscriminately send large amounts of unsolicited e-mail meant to promote a product or service. Spam in this sense is sort of like the electronic equivalent of junk mail sent to "Occupant".

Spyware

A general term for a program that surreptitiously monitors your actions. While they are sometimes sinister, like a remote control program used by a hacker, software companies have been known to use Spyware to gather data about customers. The practice is generally frowned upon.

Trojan Horse

An apparently useful and innocent program containing additional hidden code which allows the unauthorized collection,

exploitation, falsification, or destruction of data.

Virus

a virus is a (usually malicious) computer program that can travel surreptitiously from computer to computer.

Web Bugs

A web bug (also known as a tracking bug, pixel tag, Web beacon or clear gif) is a technique for determining who viewed an HTML-based email message or a web page, when they did so, how many times, how long they kept the message open, etc. Usually, a web bug is a transparent image or an image in the color of the background of what you are viewing. It is typically 1*1 pixels in size.

Worm

A computer worm is a self-replicating computer program, similar to a computer virus. A virus attaches itself to, and becomes part of, another executable program; a worm is self-contained and does not need to be part of another program to propagate itself. More notable Worms include Sobig and MyDoom

The name 'worm' was taken from The Shockwave Rider, a 1970s science fiction novel by John Brunner. Researchers writing an early paper on experiments in distributed computing noted the similarities between their software and the program described by Brunner and adopted the name.

Zombie PC

A personal computer being used by malware to perform a task without the knowledge of the user. Tasks include sending out Spam, serving pornography, performing a Denial of Service attack, etc