Beware Spyware

Updated: March 2004 **Platform:** Windows

Overview

Is your computer suddenly sluggish? Does your Web browser have mysterious new toolbars? Do advertisements pop up on your screen, even when you're not surfing the Web? You may be the victim of spyware or adware. These are the two latest variations of "malware" (**mal**icious soft**ware**) that includes viruses, worms and trojans.

Spyware and adware are generally defined as software that gets installed on your computer (usually without your knowledge), that you don't want and is for someone else's benefit. Spyware collects information and sends it to someone else or creates vulnerabilities to allow hackers to access your computer. Adware is more likely to bombard you with information that you don't want by putting extra toolbars in your Web browser, popping up advertising windows or installing software that redirects you to a specific Web site every time you open your Web browser.

As with other malware, spyware and adware predominantly target the Windows operating system. To date there is no known spyware that affects computers running the Macintosh operating system.

Where does it come from?

Probably the most important thing to know about spyware is how it gets onto your computer. While it's impossible to list every single source, there are two general categories: *Bundle Installers* are programs that piggyback on software that you do want while *Stealth Installers* sneak onto your computer without you knowing or even "doing" anything.

Bundle Installs

Many "free" programs that you can download from the Internet are only free to you because someone else has paid to bundle their spyware or adware with the program. The prevailing offenders are peer-to-peer sharing programs like the currently popular KaZaa.

The best defense against this type of spyware is to read the License Agreement before you install any new program. Some programs will offer you the agreement to read before you download the installer (you "agree" by downloading the installer), others will ask you to accept the agreement during the installation process.

KaZaa, for example, includes information about bundled programs on its Web site (which you can read before downloading the installer) and in a license agreement you are required to accept during the installation.

Programs besides KaZaa reputed to have piggybacked spyware include BearShare, Grokster, Morpheus and iMesh. There are certainly others and new ones are being developed so it's best to just get in the habit of reading license agreements when you install software.

Stealth Installs

The stealth installs are the nasty ones: they are either bundled with software and you're not told about them or they can be installed by code embedded in Web pages that runs when you view the page.

Since you don't know when they're being installed, it's harder to defend against this kind of attack. In general:

- You should be cautious with free software that is "too good to be true".
- If, while you're surfing the Web, a window pops up offering to install software for you, **DO NOT** click *Yes* unless you know and trust the publisher of the software. Read the "offer" very carefully before saying yes since the publisher of the software may not be the publisher of the Web site or they may be trying to trick you by saying that the software is necessary to "view the site properly".
- There are currently some security holes in Internet Explorer that allow programs to run on your computer when you load a Web page (web pages are, after all, computer codes that the browser interprets). That's not supposed to be possible, of course, and Microsoft does have a number of patches that you should

download to block the holes, but there will always be a lag between when new holes are discovered and when the patch becomes available. (Check your Internet Explorer security settings as described under Staying Clean to help guard against these.)

Search & Destroy

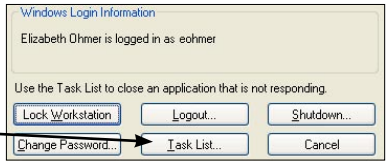
The program commonly referred to as Spybot is really called Spybot Search & Destroy – and that's what you need to do (whether you choose to use Spybot itself or not).

You can try to find malware yourself, but a program that can scan your computer could save you a lot of time.

Do It Yourself

> Note that whatever method you use to remove the spyware or adware the "host" program may not function after you remove the "parasites".

Even if you don't 'DIY', a quick check of your Task Manager can help you determine whether your system is running slow due to spyware.



1. Open the Task Manager by pressing Ctrl + Alt + Delete and clicking the Task List button.

2. If you see any of the following titles under the Applications or Processes tabs, you definitely have spyware.

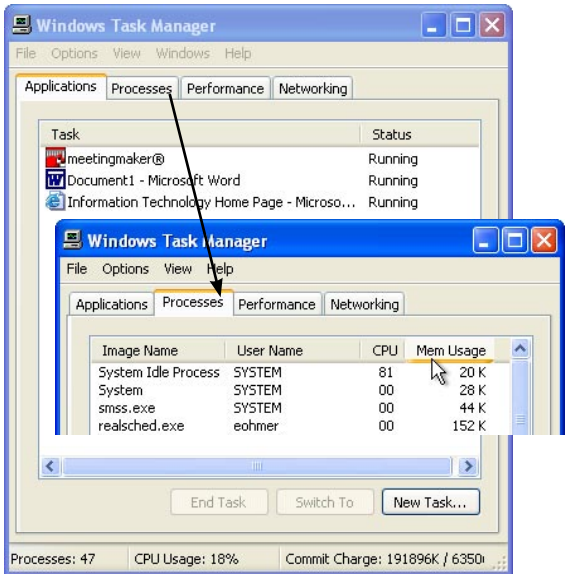
CommonName	**FavoriteMan**	**GAIN**
New.net	**Ncase**	**Alexa**

   (*These are just some currently common spyware programs, their absence doesn't mean you're clean!*)

3. If you see any Applications or Processes that you don't recognize, quit all programs and check the Task Manager again. If there are still Applications running, you may have spyware.

4. Do a search in your favorite Web search engine to gather information about unfamiliar Processes.

5. DIY – try to find those programs and executibles (.exe files) and delete them. Most of these programs aren't going be out in the open in C:\Programs - use the Search option from the Start menu to search your hard drive. Put the files in your Recycle Bin and empty it. Before you delete something, make sure it's not a legitimate part of your operating system by searching the Microsoft Web site (www.microsoft.com).



Sort the *Processes* list by *CPU* and *Mem Usage* and make sure you know what the top 'consumers' are.

Let a pro take over

Since spyware and adware are now "everywhere", detection and removal programs seem to popping up everywhere too, but, just like any other program you download of the Internet, make sure you get a program from a reputable source! While Information Technology doesn't endorse any particular anti-spyware programs, some programs that we've found to be effective and "safe" are:

- Spybot Search & Destroy (commonly known as Spybot S&D or simply Spybot) by PepiMK Software <security.kolla.de> (free but they accept donations)
- Ad-ware by Lavasoft <]\www.lavasoft.de> (there is a free version but the Plus and Pro versions offer more features)
- Spy Sweeper by Webroot <www.webroot.com> (there is a free trial but the version you pay for offers more features)

Other programs include Spyware Eliminator by Aluria, SpyRemover by ITCompany and PestPatrol. Check out the March 2, 2004 article Spy Stoppers from PC Magazine <www.pcmag.com> or search the Web for current program reviews.

The popular anti-virus software makers Symantec and McAfee are getting into the anti-spyware game, too. Their newest versions include spyware detection features, though currently they're not as robust as spyware specific programs.

> Spyware removal frequently involves editing the Windows Registry - if you accidently delete the wrong thing you could break Windows. Even if you picked a program to help you it's a good idea to back up your Registry before doing any spyware hunting.
>
> (Search www.microsoft.com for "backup windows registry" to get instructions for your version of Windows.)

Be aware that there ARE questionable companies that make anti-mailware programs. For example:

- Virtual Bouncer (from SpywareLabs) is distributed via the same bundling and drive-by download techniques as the malware it claims to remove and you have to pay for removal options. It also includes an "update" feature that can download and execute arbitrary code. This is definitely one to avoid!
- Stop-Sign (by eAcceleration) is also bundled and stealth-installed. If Stop-Sign detects reputable anti-spyware software, specifically Ad-aware and Spybot, it classifies them as "attackware".
- The free trial version of Spy Guardian Pro (SoftDD) apparently always reports that it found spyware but won't tell you where unless you pay for the full version (not necessarily evil, but ethically questionable – it might be better to scan with a program that tells you what it found).

Spybot, Adware and Spy Sweeper are fairly intuitive programs and have good instructions. Read the information on the Website before downloading and look at the help files that are built in – you should **never** let **any** program run on "auto-pilot" on your computer!

Regardless of which anti-spyware program(s) you choose, your best bet for catching the most spyware is to use more than one program.

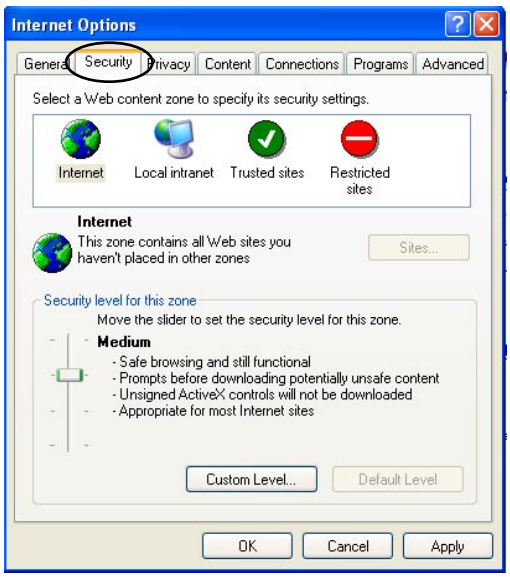
Last Resort

There are spyware programs that are so insidious that they're virtually impossible to remove. In these cases you'll need to re-install Windows. Consult your computer manufacturer and Microsoft for the best method of re-installing the operating system.

Staying Clean

Once you've gotten rid of all the spyware and adware, there are steps you can take to make sure your computer stays clean.

- **If you installed anti-spyware software, keep it up to date.** These programs compare lists of "known" problems to what they find on your computer to detect spyware and adware – if the list never gets updated the program will never detect the newest spyware programs. (Check your program's options for automatic update settings.)
- Check your anti-spyware program for "prevention" options: many of them offer real-time protection tools that watch for known spyware and alert you or prevent you from installing. (These are not 100% reliable, though, so you still need to pay attention!)
- Check your Internet Explorer Security settings to reduce the possibility of "stealth installs" when you're Web surfing.
  1. Open Internet Explorer.
  2. From the **Tools** menu select **Internet Options**.
  3. Click the **Security** tab.
  4. Make sure you have the **Internet** zone selected in the top pane of the window
  5. Set the slider under **Security Level** to Medium or higher (if there's no slider, clidk the Default Level button.)
  6. Click **OK** to save changes and close the window.



- Download and install Windows and Internet Explorer patches and updates (www.microsoft.com). Many viruses, worms, spyware and adware programs take advantage of network vulnerabilities to install themselves or to send information that helps hackers gain access to your computer.
- If you have Windows XP, use Restore Points (helpsheet available from www.lclark.edu/~infotech) to allow you to revert your system to a previous state.

Terminology

Adware
Malware that bombards you with advertising - this can be in the form of pop-up ads, restting your Web browser's home page or unwanted toolbars in your browser's window.

Blended Threat
Malware with combined characteristics. Is a self-replicating keyboard logger spyware or a worm?

Burrower
Malware that digs in deep and uses tactics that make it espcially hard to remove. It may hide behind ordinary file names or install multiple copies.

Drive-by Download
When you are misled into downloading (and installing) malware while Web surfing or software that installs itself when you visit a Web site.

Host
Software that you intentionally install that also installs software that you don't want (see Parasite).

Malware
A combination of the words **mal**icious soft**ware**. A catchall term for any kind of program that you don't want that does things to your computer that you don't want done.

Parasite
Software that comes bundled with "host" software - you don't want the parasite and it probably does things you don't want it to do. Often removing a parasite will disable the host.

Spyware
Malware that tracks your activities (Web sites you visit, keyboard strokes, etc.) or gathers information from your computer and sends reports without your authorization. Spyware can also open security holes that allow hackers access to your computer.

Trickler
A small piece of software installed in a hidden place that reinstalls malware after you've removed it. Tricklers often disguise themselves with common Windows file names.

Trojan
A program that does something unexpected: a screen saver that turns out to contain a virus, for example.

Virus
A program that damages your computer in some way usually by corrupting or destroying files. Viruses usually depend on "human assistance" to spread from computer to computer.

Worm
Self-replicating programs that may damage the infected computer (or the files) or may just clog the network as they propagate. These programs need a network connection to spread.

Zombie
A computer under the influence of malware. It may have a trojan that has taken it over or it may have spyware that has allowed hackers to control it.

Further Information

For information regarding any particular program, check the publisher's Website.

For general information on spyware, adware or malware in general visit your favorite Web search engine.

Check reputable sites like PC World Magazine (www.pcworld.com), PC Magazine (www.pcmag.com) CNET (www.cnet.com), InfoWorld (www.infoworld.com) and ZDNet (www.zdnet.com) for program reviews for information about programs before downloading and installing if you have any doubts.

SpywareGuide (www.spywareguide.com) and Pest patrol (www.pestpatrol.com), both commercial sites, include searchable encyclopedias of known spyware.