

Malware: The Enemy Within

What is Malware?

Malware is a general term used to describe any unknown, unwanted software that compromises the integrity of a computer or the information contained on one.

Malware falls in several categories:

Adware— Adware generates unwanted advertising pop-ups on your screen. They usually appear when your computer is connected to the internet.

Spyware— Spyware is software that tracks your internet browsing and computer usage habits and reports them back to a remote central database for use in marketing.

Betrayware— This is a program that pretends to detect and remove malware, but actually installs more. It may also simply pretend to detect malware as an inducement to purchase a “full” version. Distinguishing betrayware from legitimate malware removers has become a popular subject among computer professionals.

Virus— A program specifically designed to hurt a computer and spread to other computers.

Trojan— a program that appears desirable but actually contains something harmful.

Worm— Independent program that replicates from machine to machine across network connections often clogging networks and information systems as it spreads.

Cookie— A small piece of information your computer accepts when connecting to many internet sites. It is used throughout your session as a means of identifying you. Most cookies are quite harmless, some though are malevolent.

Logger— A program that records specific keystrokes or screen shots and sends them back to a specified location, such as an e-mail address.



About Betrayware

Betrayware is often considered the most egregious of malware. Very often the user of betrayware is often duped twice, first by installing something that is going to harm their computer, and second by actually paying for it. The story is common: while surfing on the internet, a user clicks on an ad for a product that claims to cure their computer of all spyware. The software that is downloaded seems to do a scan of the computer and then presents the bad news: the computer is heavily infected, and you will need to purchase a full copy of the software in order to clean it out. The only problem with this is, the software only pretended to detect spyware and is not capable of cleaning out anything. The whole scanning process is simply a show and an inducement to purchase. Indeed, some of these bogus programs actually add spyware, compiling insult with injury. The newest trick in the betrayware game is making a betrayware program look as much like a legitimate spyware killer as possible. Giving it a similar name seems to be a popular gimmick as well.

Malware: the usual suspects

These are some of the most egregious of malware distributors:

Kazaa and Gnutella— These P2P file sharing applications will purposely install malware if you are downloading a file or not.

“Free” software— Much software that is distributed for free (games, mp3 players, etc.) pays for itself by inserting spyware.

Unscrupulous individuals— Sometimes, people with access to your computer will manually install software to monitor activity.

Warez— Illegally distributed commercial software is very often rife with viruses.

E-mail attachments— e-mail attachments are the most common way to become infected with a virus. Most often, the sender will not know their e-mails are infected. Additionally, in the mid 1990's, a new type of virus was created that is capable of sending itself out through the e-mail account of an unsuspecting individual.

Rogue Websites— Websites with dubious themes (i.e. pornography, free mp3s) often distribute spyware under false guises.

The Effects (or Symptoms) of Malware

If your computer suffers from these symptoms, you are probably infected:

- Pop-Up Ads: while surfing the internet, you receive an unusual amount of pop-up ads. You receive pop-up ads at sites that usually do not have them (i.e. Google). You experience pop-up ads when the browser is closed.
- Browser Hijack: your home page changes without your knowledge or consent. URLs (internet addresses) typed into the browser take you to unwanted websites. Unfound websites bring you to a suspicious looking search engine.
- Unknown icons appear in the system tray (the area at the bottom of the screen that includes the clock).
- Even though no applications are running, the system is unusually slow. Normal applications have a hard time starting and running. The boot process seems to take forever.
- The screen image does unusual things, like turning upside-down or reversing.
- Rude messages appear in a Instant Messenger style window.
- Someone who has access to your computer hints that they know what you have been doing with it.
- People complain that you are sending them infected e-mail, even when you do not send them any.
- The physical aspects of the computer are effected: CD drawers open by themselves, drives run continuously, the computer will shut itself off.

Removing Malware*

The only real way to rid a computer of malware is through a legitimate removal program:

Ad-Aware SE published by Lavasoft

Ad-aware is an excellent **free** program that hunts and removes adware. It has an easy to use interface and is quite good for the casual computer user. A non-free professional version is available but not necessary to clean out a home computer.

Get Ad-Aware at: <http://www.lavasoftusa.com/support/download/>

This site contains both free and for-purchase versions.

Spybot Search & Destroy published by Patrick M. Kolla

The Spybot project is completely free and is financed through private donations. It is a bit more difficult to use then Ad-aware, but also a bit more thorough.

Get Spybot at: <http://www.spybot.info/en/index.html>

>>> Do not get these software packages from any other sites! Remember, sophisticated fakers and copycats are lurking! <<<

Norton Anti-Virus

Norton is considered the gold standard in virus detection, blocking and removal. This product constantly offers free updates. It is a commercial product available from any computer retailer, or from their website. On their website, you can download a free trial version.

Get Norton at: <http://www.norton.com>

McAfee Anti-Virus

This product is comparable to Norton. Purchase a copy at your local retailer or visit:

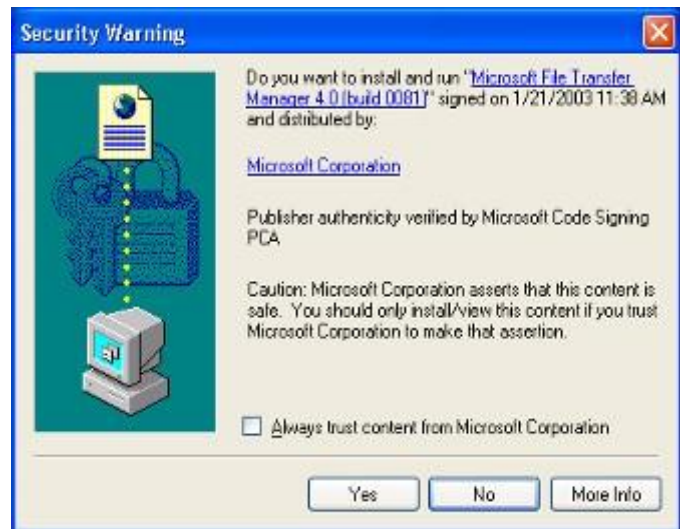
<http://www.mcafee.com/us/>

**It is always a good idea to create a restore point before making any major changes on your computer. See the Windows help system for information.*

Avoiding Malware

Be proactive in defending your computer!

- By law, any software that installs spyware or adware must say so in the End Users License Agreement (EULA). If you think a package is suspect, read it before installing.
- Download.com, the eponymous software database, will make a note of any installed spyware in its downloadable file descriptions.
- Avoid rogue websites, such as those offering pornography, gambling tips, free mp3s and other dubious subjects.
- Avoid using peer 2 peer file sharing services like Gnutella and Kazaa. Kazaa is the single largest disseminator of ad and spyware.
- If you use Windows XP, consider upgrading to Service Pack 2. It is free and very reliable. [Http://www.microsoft.com](http://www.microsoft.com).
- Make sure your internet browser setting is set to an appropriate security setting.
Microsoft IE: click on the *Tools* menu and then *Internet Options*. Click on the *Privacy* tab and make sure it is set to at least *Medium High*.
Netscape: Click on the *Edit* menu and then the *Preferences* item. Double click on *Privacy&Security* and then *Cookies*. Chose the option *Enable cookies from originating website only*.
- Avoid free utilities such as Gator or Weatherbug without first investigating them.
- Avoid *WareZ*, the name given to illegally distributed commercial software.
- Some unscrupulous websites attempt to download programs into your computer without your request. When this happens, a security warning box will appear. Always click the NO button.
- Only open e-mail attachments that you are expecting. A person's e-mail account can actually send out infected, attached messages without their knowledge.
- Keep your Operating System and Application software as up-to-date as possible.
- Always use common sense when going on-line.
- "Keep your ear to the ground" Very often, when there is a wide spread virus on the loose, it will be reported in the mainstream news.



Resources

Internet resources to better educate yourself about malware.

Firewall Guide

<http://www.firewallguide.com/>

This excellent website contains many independent articles about malware and computer protection.

Spyware Warrior

[Http://www.spywarewarrior.com/](http://www.spywarewarrior.com/)

A forum style website where people share the latest intelligence on malware.

Spyware Warrior Rogue Spyware Removers Section

[Http://www.spywarewarrior.com/rogue_anti-spyware.htm#products](http://www.spywarewarrior.com/rogue_anti-spyware.htm#products)

A dedicated portion of *Spyware Warrior* dedicated to exposing phony spyware removers.

A Note to Macintosh and Linux Users

The vast majority of malware is indeed written for the Windows operating system. It is an unfortunate case, though, that malevolent software has started to appear for these systems as well. Use the common sense tips for avoiding any possible damage to your system and keep aware of any developments from the manufacturers websites.

[Http://www.apple.com](http://www.apple.com)

[Http://www.linux.org](http://www.linux.org)