

**Spyware -- Malware – Virus – Trojans**

**1) Microsoft Update problem**

- a) Before we get into today's topic Pinnacle Computer Services would like to talk about a problem they are seeing with a Microsoft update last week.
- b) Microsoft update KB908531 from security bulletin MS06-015
- c) This security update introduces a new file, Verclsid.exe. Verclsid.exe is used to verify a COM object before it is instantiated by Windows Explorer
- d) The symptoms are:
  - i) Microsoft Office applications stop responding when you try to save or to open Office files in the "My Documents" folder.
  - ii) Office files that are located in the "My Documents" folder cannot be opened.
  - iii) If you open a file by clicking Open on the File menu, the application stops responding.
  - iv) When you type an address in the Address box in Microsoft Internet Explorer, nothing happens.
  - v) When you right-click a file and then click Send To, nothing happens.
  - vi) When you expand a folder in Windows Explorer, nothing happens.
  - vii) Some third-party applications stop responding when you open or save data in the "My Documents" folder
  - viii) Outlook stops responding
- e) Only certain computers are affected
  - i) Computers that have older HP software installed
    - (1) HP PhotoSmart software
    - (2) Any HP DeskJet printer that includes a card reader
    - (3) HP scanners

- (4) Some HP CD-RWs and HP DVD-RWs
- (5) HP cameras
- f) Work arounds
  - i) Find and rename c:\windows\system32\verclsid.exe to verclsid.old
  - ii) Uninstall update KB908531 and do a custom update and tag KB908531 as excluded
  - iii) Only for highly technical users goto <http://support.microsoft.com/kb/918165> and perform registry update

## *Adware and Spyware*

### Terms

**Spyware** - Any [software](#) that covertly gathers user information through the user's [Internet](#) connection without his or her knowledge, usually for [advertising](#) purposes. [Spyware applications](#) are typically [bundled](#) as a hidden component of [freeware](#) or [shareware](#) programs that can be [downloaded](#) from [the Internet](#); however, it should be noted that the majority of shareware and freeware applications do not come with spyware. Once installed, the spyware monitors user activity on the Internet and transmits that information in the background to someone else. Spyware can also gather information about [e-mail](#) addresses and even passwords and credit card numbers.

Spyware is similar to a [Trojan horse](#) in that users unwittingly install the product when they install something else. A common way to become a victim of spyware is to download certain [peer-to-peer](#) file swapping products that are available today.

Aside from the questions of ethics and privacy, spyware steals from the user by using the [computer's](#) memory resources and also by eating [bandwidth](#) as it sends information back to the spyware's home base via the user's Internet connection. Because spyware is using memory and [system](#) resources, the applications running in the background can lead to system [crashes](#) or general system instability.

Because spyware exists as independent [executable](#) programs, they have the ability to monitor [keystrokes](#), scan files on the [hard drive](#), snoop other applications, such as [chat](#) programs or word processors, install other spyware programs, read [cookies](#), change the [default home page](#) on the [Web browser](#), consistently relaying this information back to the spyware author who will either use it for advertising/marketing purposes or sell the information to another party.

Licensing agreements that accompany software downloads sometimes warn the user that a spyware program will be installed along with the requested software, but the licensing agreements may not always be read completely because the notice of a spyware installation is often couched in obtuse, hard-to-read legal disclaimers.

**Adware** - A form of [spyware](#) that collects information about the user in order to display advertisements in the [Web browser](#) based on the information it collects from the user's browsing patterns.

**Virus** - A [program](#) or piece of [code](#) that is loaded onto your [computer](#) without your knowledge and runs against your wishes. [Viruses](#) can also replicate themselves. All [computer](#) viruses are manmade. A simple [virus](#) that can make a [copy](#) of itself over and over again is relatively easy to produce. Even such a simple

virus is dangerous because it will quickly use all available [memory](#) and bring the [system](#) to a halt. An even more dangerous type of virus is one capable of transmitting itself across [networks](#) and bypassing [security](#) systems.

**Worm** - A [program](#) or [algorithm](#) that replicates itself over a [computer network](#) and usually performs malicious actions, such as using up the [computer's](#) resources and possibly shutting the [system](#) down, but cannot attach itself to other programs.

**Trojan Horse** - A destructive [program](#) that masquerades as a benign application. Unlike [viruses](#), [Trojan horses](#) do not replicate themselves but they can be just as destructive. One of the most insidious types of [Trojan](#) horse is a program that claims to rid your [computer](#) of [viruses](#) but instead introduces viruses onto your computer.

**Firewall** - A firewall is a system, which prevents unauthorized use and access to your computer. A firewall can be either hardware or software. Hardware firewalls provide a strong degree of protection from most forms of attack coming from the outside world and can be purchased as a stand-alone product or in broadband routers. Unfortunately, when battling viruses, worms and Trojans, a hardware firewall may be less effective than a software firewall, as it could possibly ignore embedded worms in outgoing e-mails and see this as regular network traffic. For individual home users, the most popular firewall choice is a software firewall. A good software firewall will protect your computer from outside attempts to control or gain access your computer, and usually provides additional protection against the most common Trojan programs or e-mail worms. The downside to software firewalls is that they will only protect the computer they are installed on, not a network.

\*\*\* It is important to remember that on its own a firewall is **not** going to rid you of your computer virus problems, but when used in conjunction with regular operating system updates and a good anti-virus scanning software, it will add some extra security and protection for your computer or network.\*\*\*\*\*

**Freeware** - Copyrighted [software](#) given away for free by the author. Although it is available for free, the author retains the copyright, which means that you cannot do anything with it that is not expressly allowed by the author. Usually, the author allows people to use the [software](#), but not sell it.

**Shareware** - Copyrighted [Software](#) distributed on the basis of an honor [system](#). Most [shareware](#) is delivered free of charge, but the author usually requests that you pay a small fee if you like the [program](#) and use it regularly. By sending the small fee, you become registered with the producer so that you can receive service assistance and updates. You can [copy](#) shareware and pass it along to friends and colleagues, but they too are expected to pay a fee if they use the product. Shareware is inexpensive because it is usually produced by a single [programmer](#) and is offered directly to [customers](#).

**Cookie** - A message given to a [Web browser](#) by a [Web server](#). The [browser](#) stores the message in a [text file](#). The message is then sent back to the [server](#) each time the browser requests a page from the server.

**Persistent Cookie** - Also called a *permanent cookie*, or a *stored cookie*, a [cookie](#) that is stored on a user's [hard drive](#) until it expires (persistent cookies are set with expiration dates) or until the user deletes the cookie. Persistent cookies are used to collect identifying information about the user, such as [Web](#) surfing behavior or user preferences for a specific [Web site](#).

**Session Cookie** - Also called a *transient cookie*, a [cookie](#) that is erased when the user closes the [Web browser](#). The session cookie is stored in temporary memory and is not retained after the [browser](#) is closed. Session cookies do not collect information from the user's [computer](#). They typically will [store information](#) in the form of a session identification that does not personally identify the user.

#### Things to Know

- 1) Make sure your OS is up to date.
- 2) Make sure your Antivirus Software is installed and download updates daily.
- 3) Make sure your internet browser is set to Medium.
- 4) Only download from sites you trust.
- 5) Read Privacy Statements and License Agreements
- 6) When an ad pops up ONLY close it using the Red X in the upper right hand corner. Do NOT try to close a window that does NOT have the red X. Do NOT click OK or Continue, it's a trick.

## Recommended Software

### Spyware

1. Spybot Free
2. Windows Defender Beta2 Free
3. Adaware
4. Spyware Doctor
5. Spy Sweeper
6. Pest Patrol

### Firewall

1. ProcessGuard
2. Kerio Personal Firewall
3. ZoneAlarm

## Links

[http://www.spywarewarrior.com/rogue\\_anti-spyware.htm#trustworthy](http://www.spywarewarrior.com/rogue_anti-spyware.htm#trustworthy)

<http://www.spywareguide.com>

<http://www.microsoft.com/athome/security/spyware/default.mspx>

<http://www.sunbelt-software.com/Kerio.cfm>