

Glossary of PC Security Terms

ActiveX — A Web technology that enables portable modules and makes it possible for a browser to interact with desktop applications, typically to provide additional user interface functions. Spyware is frequently downloaded through an ActiveX control.

Adware — Advertising components that are installed on a user's computer at some Web sites, "shareware" products (and sometimes, legitimately purchased commercial software.) Typically, Adware takes the form of pop-up ads that appear while the user is surfing. Not all Adware is deceptive or malicious.

Backdoor — Secret or hidden network entry points found by Malware.

Badware — A general term for Spyware, deceptive Adware, Malware, viruses and all other indisputably unwanted software.

BHO — Browser Helper Object. A .DLL module designed as a plugin for Internet Explorer to provide added functionality. For example, the Adobe Acrobat plugin that enables IE users to read PDF documents within their browsers is a BHO. Because BHOs have unrestricted access to the Internet Explorer event model, some forms of Malware are created as BHOs.

Bundling — The practice of including multiple software products in a package. A legitimate example is Microsoft Office Suite. Often, Adware and Spyware are bundled with shareware and freeware. In these cases, you are agreeing, unknowingly, to accept the Adware and Spyware when you accept the "free" software.

Cache Poisoning — Corrupting an Internet server's domain name system table by replacing an Internet address with that of another, rogue address. When a Web searches for a page with a particular address, the request is redirected by the rogue entry in the table to a different address. At that point, a worm, spyware, Web browser hijacking program, or other malware can be downloaded to the user's computer from the rogue location. Cache poisoning is also called domain name system (DNS) poisoning or DNS cache poisoning.

Cookie — A small file placed on a computer by a Web site that contains the user's profile and preferences regarding that site.

Cookie Poisoning — Modification of a cookie by an attacker to gain unauthorized information about the user, often for identity theft.

Crimeware — Broadly, all Malware with a common objective: getting money or confidential information. Also, any software designed expressly to facilitate illegal activity online. For example, tools and instructions that enable people with little technical proficiency to launch a phishing attack.

Dialer — Software programs that install themselves to a user's dial-up settings and dial numbers without the user's knowledge. Often, these numbers connect to potentially offensive sources. Once dialer software is downloaded, the user is disconnected from his/her Internet service provider, another phone number is dialed and the user is billed for the time used. Dialers are malicious in nature and can rack up expensive and unwanted bills.

DLL — Dynamic Library Link. An executable program that performs some function, but is not launched directly by the user. Some Spyware uses an ActiveX control to keep reinstalling itself. Usually it's a DLL file,

DNS Poisoning — Corrupting an Internet server's domain name system table by replacing an Internet address with that of another, rogue address. When a Web searches for a page with a particular address, the request is redirected by the rogue entry in the table to a different address. At that point, a worm, spyware, Web browser hijacking program, or other malware can be downloaded to the user's computer from the rogue location. DNS poisoning is also called Cache poisoning or DNS cache poisoning.

Download — (verb) The delivery of software to a system via an external medium, such as a Web site.

Downloader — (noun) A Spyware application whose sole purpose is to enable other Spyware to be installed continually on the user's computer.

Drive-By Download — A download that occurs without the user's knowledge or consent. It can occur as the result of visiting a specific Web site or by clicking a misleading button or function on a pop-up window (free tool, yes/no opinion poll, etc.).

Driver — A program that interacts with a peripheral device or special (often optional) software. The driver has the knowledge of the device or software interface that programs using the driver do not contain. A driver is often packaged as a DLL file.

Driver Hook — A method of enabling a third party to interact with an online transaction between two users. When the third party is undetected and unauthorized, the driver hook is Spyware.

E-mail Spoofing — The practice of forging an e-mail header so that the message appears to have been sent by reputable merchant, financial institution or other enterprise. Phishers and distributors of spam often use spoofing in an attempt to get recipients to open and respond to their solicitations.

Encryption — Scrambling data so that it becomes difficult to interpret.

EULA — End User License Agreement. (pronounced yoo'-la)The legal agreement between the manufacturer and the purchaser of software. It is usually displayed on screen at the time of installation. In order to install the software, the user must indicate acceptance of the terms of the agreement by selecting a check box so labeled.

Executable File — A file that contains a program. In a DOS or Windows operating system, an executable file usually has a file name extension of .bat, .com, or .exe. A file whose name ends in ".exe" is really a program that when "opened" – i.e., double-clicked, causes the operating system to run the program.

Extraction — The process by which Malware that has been quarantined is permanently removed from a user's computer.

Firewall — A barrier, typically hardware and software, that prevents computers from communicating directly with outside computer systems. Firewalls protect against worms and viruses, but not Spyware.

Hijacker — A Trojan that alters the settings of a browser to change the user's homepage. It can also alter a search page, Favorites menu, and system registry. Sometimes, hijackers act like Spyware.

History — A running list of Web sites visited by user, via a browser.

Homepage — For a Web user, the homepage is the first Web page that is displayed after starting a Web browser, such as Internet Explorer. The browser is usually preset so that the homepage is the first page of the browser manufacturer. However, the user can set it to open to any Web site. For example, "http://www.yahoo.com" or "http://earthlink.net" could be homepages.

ID Theft — The practice of unauthorized access and use of personal identifiers such as names, addresses, account numbers, passwords, Social Security numbers, etc. for the purpose of fraud.

Internet Explorer — The Microsoft-bundled browser used to surf the Internet.

Layered Socket Provider (LSP) — A system driver linked to the networking system for Windows-based computers. An LSP can access all data entering and leaving via the network interfaces.

Keystroke Logger — A hardware device or software program that records each keystroke typed on a particular keyboard, for report back to another party. Often used to record personal data for identity theft.

MD5 Checksum — A unique, 128-bit cryptographic message digest value derived from the contents of a file and generated by the MD5 program. This value is considered to be a highly reliable fingerprint that can be used to verify the integrity of the file's contents. If as little as a single bit value in the file is modified, the MD5 checksum for the file changes.

Malware — From malicious software, software designed specifically to interfere with, damage or otherwise disrupt a system.

Metamorphic Malware — Malware having the ability to change its signature (obfuscate) and change its function (mutate) each time it replicates, in order to escape detection by anti-Spyware programs that are designed to “recognize” Malware by its signature (name.)

P2P — (also Peer-to-Peer) A type of Internet network that enables a group of computer users with the same networking program to connect with each other for the purposes of accessing files directly from one another's hard drives. Spyware is often passed along in P2P transactions.

Package — All files, keys, executables and any other resources associated with a Spyware application.

Peer-to-Peer — (also P2P) A type of Internet network that enables a group of computer users with the same networking program to connect with each other for the purposes of accessing files directly from one another's hard drives. Spyware is often passed along in P2P transactions.

Pharming — A rogue practice in which malicious code is installed on a personal computer or server, misdirecting users to fraudulent Web sites without their knowledge or consent. Pharming has been called “phishing without a lure.”

In pharming, larger numbers of computer users can be victimized because it is not necessary to target individuals one by one and no conscious action is required on the part of the victim.

A particularly hostile pharming tactic is known as Domain Name System Poisoning (DNS poisoning)

Phishing — A kind of e-mail fraud wherein the perpetrator sends out legitimate-looking e-mails, typically with links to fraudulent Web sites that appear to come from well known and trustworthy sources. Phishers attempt to gather personal and financial information from the recipient for purposes of identity theft.

Polymorphic Malware — Malware having the ability to change its signature randomly each time it replicates. This is a technique makers of Malware use to prevent detection of the software by anti-Spyware programs that are designed to “recognize” Malware by its signature (name.) For example, a polymorphic file could look like this: Vx2T.exe

Pop-up — A small browser window that pops up in the foreground of a user’s main browser window. A variation on the pop-up ad, the pop-under, is a window that loads behind the Web page being viewed, only to appear when the user leaves the Web site.

Pop-up Blocker — Software that prevents pop-ups from being displayed on a user’s computer.

Privacy Policy — This policy covers how an organization treats personal information that it collects and receives, including information pertaining to how users apply their products and services. Personal information is generally defined as name, address, e-mail address, phone number, and information that is not otherwise publicly available. Typically, this means that an organization will explain why information is being collected, how it will be used, and how it plans to limit improper disclosure. Good privacy policies state that individuals can obtain their own data and make corrections, if necessary.

Quarantine — A process used by anti-Spyware solutions whereby Spyware is detected, blocked, rendered harmless and stored in a secure location on a user's computer, but not removed.

Ransomware — A scam that attempts to hold a user's data hostage until payment is received. Some ransomware is downloaded with rogue anti-Spyware programs.

In a typical ransomware attack, the user sees a pop-up indicating that his/her computer is infected with a particular virus or parasite and by purchasing the recommended product, the parasite can be removed. Usually, there is no such parasite, the ransomware merely holds the user's data "hostage."

RAT Tools — Remote Access Trojan: Malicious software packages that attempt to gain complete control over computer systems. These programs, (sometimes called Backdoor Software) are sometimes attached to Trojan Horses, viruses, worms, and Spyware. If a system is infected, there is virtually no limit to what these programs can do.

Remote Access Trojans — Remote Access Trojan: Malicious software packages that attempt to gain complete control over computer systems. These programs, (sometimes called Backdoor Software) are sometimes attached to Trojan Horses, viruses, worms, and Spyware. If a system is infected, there is virtually no limit to what these programs can do. Also called RAT Tools.

Remove Me — An option, typically on unsolicited commercial e-mail, that has the opposite effect of that intended. Often, a response from the recipient serves to validate that the e-mail address is valid. As a result, the recipient receives more e-mail, often because the original sender has sold the address to other spammers or malicious third parties.

Restore Point — System Restore is a Windows XP Professional feature that restores a computer to a previous state if a problem occurs, without losing the user's personal data files, e-mail or settings. System Restore monitors changes to the system and some application files, and it automatically creates easily identified restore points which enable the user to revert the system to a date of choice. They are created daily and at the time of significant system events, such as installations. Users can create restore points manually at any time.

Root Kits — Collections of software programs that a hacker can use to gain unauthorized remote access to a computer and launch additional attacks. These programs may use a number of different techniques, including monitoring keystrokes, changing system log files or existing system applications, creating a backdoor into the system, and starting attacks against other computers on the network. Rootkits are generally organized into a set of tools programmed to target a particular operating system.

Scan — A detailed examination of all software installed on a user's computer, usually done for the purpose of detecting malicious software.

Shareware — Software that is distributed in trial version free of charge. It is assumed that the user will pay for the full version of the product, if the user finds that it performs to his/her satisfaction.

ShellExecute API — The Shell API is essentially an extension of the Windows shell that provides most of the same functionality that launches applications in Windows Explorer through a programmatic interface including executable files such as .exe, .bat, .vbs etc.; any file on the local system or network with a registered extension (.doc, .pdf, .txt etc.) Web URLs, FTP URLs, e-mail clients using the mailto: directive, and any other 'monikers' associated with Windows.

Spam — Unsolicited commercial e-mail, usually sent out via open relays to millions of Internet users.

Spear-phishing — Targeted phishing attacks against known members or customers of a particular enterprise, typically those that are small to mid-sized. Spear-phishing yields far higher returns than phishing, and relies on the membership/customer database being compromised.

Spyware — Programming that is installed in a computer to gather information about the user secretly and relay it to advertisers or other interested parties; generally, any potentially unwanted software that could disrupt computer usage, installed without the user's knowledge. Spyware can get into a computer as a software virus or as the result of installing a new program.

SSL — (Secure Socket Layer): A security protocol that provides communication privacy. SSL enables client and server applications to communicate in a way that is designed to prevent eavesdropping, tampering, and message forgery.

Stego — (From steganography) A technique by which Spyware is hidden in a picture, such as a BMP or JPEG, or a music file. If such hidden files are polymorphic or metamorphic, they are extremely difficult to detect and remove.

System Monitor — A device that monitors computer activity. System monitors can record keystrokes, passwords, Web use, Instant Messages, e-mail and other transactions. This information can be saved and transmitted to a third party.

Toolbar — A row or column of on-screen buttons used to activate functions in an application.

Trojan (Horse) — A malicious program that is disguised as a harmless software program. Trojans do not replicate themselves like viruses, but are spread through e-mail attachments and Web downloads.

Typosquatting — (Also known as TypeJacking) Purchasing a domain name that is a variation on a popular domain name with the expectation that the site will get traffic from the original site due to misspelling of the name. For example, a typosquatter would register the domain names googkle.com or yahooo.com anticipating that users would navigate to that site by accident.

Update — As it pertains to Spyware, a version of an anti-Spyware solution that incorporates the latest target definitions - fixes to disarm newly detected threats. Updates are made frequently, and do not change the functionality of the product.

Upgrade — A version of a software product that incorporates major changes and new functionality.

URL — Uniform Resource Locator. The addressing system used universally to locate documents on the Internet. Briefly, a Web address.

Virus — A program or programming code that replicates by being copied or initiating its copying to another program, computer boot sector or document. Some viruses are benign or playful in intent and effect; some can be harmful, erasing data or causing the user's hard disk to require reformatting.

Wizard — A series of instructional steps and options to automate a task for users, such as the installation and configuration of a software application.

Worm — A self-replicating virus that does not alter files but resides in active memory and duplicates itself. Worms use parts of an operating system that are automatic and usually invisible to the user. It is common for worms to be noticed only when their uncontrolled replication consumes system resources, slowing or halting other tasks.