

Glossary

ASC includes the following Glossary in order to clarify some of the terms used in this document, particularly the more frequently used terms in anti-spyware products and research. This Glossary will be updated as we continue with our work.

ActiveX Control: See “Browser Plug-in.”

Advertising Display Software: Any program that causes advertising content to be displayed.

Adware: A type of *Advertising Display Software* that delivers advertising content potentially in a manner or context that may be unexpected and unwanted by users. The ASC’s Risk Model document details many of the behaviors that may be considered unexpected or unwanted. Many adware applications also perform tracking functions, and therefore may also be categorized as *Tracking Technologies*. Some consumers may want to remove Adware if they object to such tracking, do not wish to see the advertising caused by the program, or are frustrated by its effects on system performance. On the other hand, some users may wish to keep particular adware programs if their presence subsidizes the cost of a desired product or service or if they provide advertising that is useful or desired, such as ads that are competitive or complementary to what the user is looking at or searching for.

Alternate Data Stream: An extension to Microsoft's Windows NT File System (NTFS) that provides compatibility with files created using Apple's Hierarchical File System (HFS). Applications must write special code if they want to access and manipulate data stored in an alternate stream. Some spyware uses these streams to evade detection.

Automatic Download Software: Any program used to download and install software without user interaction. (See also: Downloader)

Backdoor: A program that provides attackers with remote access to infected computers. Bots are a sub-category of backdoor Trojans, which often use Internet Relay Chat (IRC) or peer-to-peer (P2P) protocols as their main method of communication (aka Backdoor Trojan).

Botnet: A type of *Remote Control Software*, specifically a collection of zombie machines running malware under a common command. A botnet's originator can control the group remotely. The botnet is usually a collection of zombie machines running programs under a common command and control infrastructure on public or private networks. Botnets have been used for sending spam remotely, installing more spyware without consent, and other illicit purposes.

Browser Helper Object (BHOs): see “Browser Plug-in.”

Browser Modifier: A program that changes browser settings, such as the home page, search page or destination URL, without adequate consent.

Browser Plug-in: A software component that interacts with a Web browser to provide capabilities or perform functions not otherwise included in the browser. Typical examples are plug-ins to display specific graphic formats, to play multimedia files or to add toolbars which include search or anti-phishing services. Plug-ins can also perform potentially unwanted behaviors such as redirecting search results or monitoring user browsing behavior, connections history, or installing other unwanted software like nuisance or harmful adware. Types of Browser plug-ins include:

- **ActiveX controls:** A type of Browser Plug-in that is downloaded and executed by the Microsoft Internet Explorer Web browser.
- **Browser Helper Object (BHOs):** A type of Browser Plug-in that is executed each time the Microsoft Internet Explorer web browser is launched unless it has been disabled,
- **Mozilla Firefox Extensions:** A browser Plug-in specific to Mozilla Firefox

Bundling: The practice of distributing multiple pieces of software together, so that when the software “bundle” is installed, multiple components may be installed. In many cases, bundling is a convenient way to distribute related pieces of software together. However, in some cases, unwanted software components, such as nuisance or harmful adware, can be bundled with programs users want, and can thereby be downloaded onto their computers without notice or consent.

Cookie: A piece of data that a Web site -- or a third party that was commissioned or approved by the website -- saves on users' computers' hard drives and retrieves when the users revisit that Web site. Some cookies may use a unique identifier that links to information such as login or registration data, online "shopping cart" selections, user preferences, Web sites a user has visited, etc. (See also Tracking Cookies.)

Dialer: Dialer is a colloquial term for *Dialing Software*.

Dialing Software: Any program that utilizes a computer's modem to make calls or access services. Users may want to remove dialers that dial without the user's active involvement, resulting in unexpected telephone charges and/or cause access to unintended and unwanted content.

Distributed Denial-of-Service (DDoS) Attack: A means of burdening or effectively shutting down a remote system by bombarding it with traffic from many other computers. DDoS attacks are often launched using the compromised systems of Internet users, often using botnets. An attacker will exploit a vulnerability in one computer system and make it the DDoS “master” using *Remote Control Software*. Later, the intruder will use the master system to identify and manage zombies that can perform the attack.

Downloader: A program designed to retrieve and install additional files. Downloaders can be useful tools for consumers to automate upgrades of essential software such as operating system upgrades, browsers, anti-virus applications, anti-spyware tools, games and other useful or enjoyable applications of all kinds. Automated upgrades are useful for closing off security vulnerabilities in a timely way. Unauthorized downloaders

are used by third parties to download potentially unwanted software without user notification or consent.

Drive-by-Download: The automatic download of software to a user's computer when they visit a Web site or views an html formatted email, without the user's consent and often without any notice at all. Drive-by-downloads are typically performed by exploiting security holes or lowered security settings on a user's computer.

Droneware: Programs used to take remote control of a computer and typically used to send spam remotely, run DDOS attacks or host offensive Web images. See also "Botnet."

End User License Agreement (EULA): An agreement between a producer and a user of computer software that specifies the terms of use putatively agreed to by the user. The software producer specifies the parameters and limitations on use, which comprise a legally binding contract. Some companies use the EULA as the sole means of disclosure of a program's behavior (including bundling, use of the user's data, etc.).

Exploit/Security Exploit: A piece of software that takes advantage of a hole or vulnerability in a user's system to gain unauthorized access to the system.

Hacker Tool: *Security Analysis Software* that can be used to investigate, analyze or compromise the security of systems. Some Hacker Tools are multi-purpose programs, while others have few legitimate uses.

Hijacker: *System Modification Software* deployed without adequate notice, consent, or control to the user. Hijackers often unexpectedly alter browser settings, redirect Web searches and/or network requests to unintended sites, or replace Web content. Hijackers may also frustrate users' attempts to undo these changes, by restoring hijacked settings upon each system start.

Host File: A file, stored on the user's computer, used to look up the Internet Protocol address of a device connected to a computer network. Some spyware has been known to change a host file in order to redirect users from a site that they want to visit to sites that the spyware company wants them to visit.

Joke Program: A nonmalicious but annoying program which is not intended to monetize the user.

Keylogger (or Keystroke Logger): *Tracking Software* or other technology that records keyboard and/or mouse activity. Keyloggers typically either store the recorded keystrokes for later retrieval or they transmit them to the remote process or person employing the keylogger. While there are some legitimate uses of keyloggers, they are often used maliciously by attackers to surreptitiously track behavior to perform unwanted or unauthorized actions included but not limited to identity theft.

Malware: The superset of malicious software, that often used as shorthand method for referencing multiple categories of software such as viruses, trojans, worms, spyware, etc.

Monitoring Software: "see Tracking Software".

Objective Criteria: The behavioral factors which anti-spyware companies use to decide whether to consider a process or program potentially unwanted.

Packer: A program that can compress and/or encrypt an executable file in a manner that prevents matching the memory image of that file and the actual file on disk. Sometimes used for copy protection, packers are often used to make spyware less easy to analyze/detect.

Passive Tracking Technologies: Technologies used to monitor user behavior or gather information about the user, sometimes including personally identifiable or other sensitive information.

Password Cracker: *Security Analysis Software* designed to allow someone to recover or decrypt lost, forgotten or unknown passwords. Password Cracker can guess a password by running a brute-force attack, e.g. testing each character combination to find the right password, or by running a dictionary attack, e.g. testing common words from large dictionaries, which could be used as password by users. While they can be a legitimate tool used by security administrators and law enforcement officers, Password Crackers pose a significant security and privacy threat when used illicitly.

Password Stealer (PWS): A password stealer (PWS) is malware that is specifically used to transmit personal information, such as user names and passwords. A PWS often works in conjunction with a keylogger or other tracking software.

Personally Identifiable Information (PII): "Personal information" is information concerning an identified or identifiable individual, the collection, use or disclosure which the individual would ordinarily want to control.

Different anti-spyware vendors will apply their own definitions of "personal information" within their own anti-spyware applications in response to the needs and preferences of their customers.

Such definitions may be informed by applicable legal protections afforded such information, such as the EU Data Directive, the Canadian Personal Information Protection and the Electronic Documents Act, the Japanese Personal Information Protection Act, the Australian Privacy Act, and the US sectoral privacy laws.

Port Scanner: *Security Analysis Software* used to discover what computer network services a remote system provides. Port scanning indicates where to probe for weaknesses.

Potentially Unwanted Software/Potentially Unwanted Program: A program with behaviors that may be unwanted by some users but desired by others. The behaviors in question often impact the user's privacy, security or computing experience.

Privacy Policy: A legally binding notice of how a company deals with a user's personal information. The privacy policy should contain information about collecting information and the secondary uses of data, including how information is shared with third parties and who those third parties are.

Privilege Elevation: A process that allows an individual or device to gain a higher level of privileges, usually administrator or system level access, on a computer or network. In some cases this can be done without appropriate consent or permission.

Registry: A database integrated into certain operating systems which store information, including user preferences, settings and license information, about hardware and software installed on a user's computer.

Registry Keys: The individual entries in the registry. The value of the keys is changed every time a new program is installed or configuration settings are modified. Spyware often changes registry key values in order to take control of parts of the system. These changes can impair the regular function of the computer.

Remote Access/Administration Tool (RAT): An executable application designed to allow remote access to or control of a system. RATs are a type of *Remote Control Software*. While there are many legitimate uses of RATs, they can be used maliciously by attackers to start or end programs, install and uninstall new software, or perform other unwanted or unauthorized actions.

Remote Control Software: An application designed to allow specific types of remote access to or control over a system.

Risk Modeling: The process used by anti-spyware vendors to determine the categorization of spyware, both in terms of level and type of risk.

Rogue Security Software: Software that appears to be beneficial from a security perspective but provides minimal or no security capabilities, generates erroneous alerts and often attempts to socially engineer a user into participating in fraudulent transaction.

Rootkit: A program that fraudulently gains or maintains administrator level access that may also execute in a manner that prevents detection. Once a program has gained access, it can be used to monitor traffic and keystrokes; create a backdoor into the system ; alter log files; attack other machines on the network; and alter existing system tools to circumvent detection. Rootkit commands replace original system command to run malicious commands chosen by the attacker and to hide the presence of the Rootkit on the system by modifying the results returned by suppressing all evidence of the presence of the Rootkit. Rootkits are an extreme form of *System Modification Software*.

Screen Scrapers/Screen Capturers: *Tracking Software* that records images of activity on the computer screen. Screen Scrapers typically either store the recorded images and/or video for later retrieval or they transmit them to the remote process or person employing the Screen Scraper. There are some legitimate uses of screen scrapers, but they are often used maliciously by attackers to surreptitiously track behavior to perform unwanted or unauthorized actions that can include identity theft.

Security Analysis Software: Any program used by a computer user to analyze or circumvent security protections.

Settings Modifier: A program that changes computer settings with or without the user's knowledge.

Snoopware: Sometimes used as a synonym for the narrower definition of Spyware—i.e. *Tracking Software*.

Software Bundler: A program that installs other potentially unwanted software in addition to itself. See: *Bundling*.

State Management Tools: Technologies used to store and make information available about the “state” of a system—i.e. information about current conditions and operations. Cookies are the most common form of a State Management Tool since they can be used to store data provided to a Web site and maintain a Web application session. State Management Tools can be used as a *Tracking Technology*.

System Modification Software: Any program used to modify a user's system and change their experience, such as by altering their home page, search page, default media player, or lower level system functions.

Spyware: The term Spyware has been used in two ways.

In its narrow sense, Spyware is a term for *Tracking Software* deployed without adequate notice, consent, or control for the user.

In its broader sense, Spyware is used as a synonym for what the ASC calls “Spyware (and Other Potentially Unwanted Technologies)”:

Technologies deployed without appropriate user consent and/or implemented in ways that impair user control over:

- Material changes that affect their user experience, privacy, or system security;
- Use of their system resources, including what programs are installed on their computers; and/or
- Collection, use, and distribution of their personal or other sensitive information.

In our documents, the ASC may use the term Spyware in its narrower sense, but will mark it as such [spyware(narrow)]. However, we understand that it is impossible to avoid the broader connotations of the term in colloquial or popular usage, and we do not attempt to do so. For example, we refer to the group as the ‘Anti-Spyware Coalition’ and vendors as makers of ‘anti-spyware software’, even recognizing that their scope of concern extends beyond tracking software. Therefore, the term spyware, when used generally in an ASC document will always refer to the broader colloquial usage.

Stream Files: See “Alternate Data Stream.”

System Monitor: *Tracking Software* that is used to monitor computer activity. System Monitors range in capabilities but may record some or all of the following: keystrokes, screen captures, e-mails, chat room conversations, instant messages, Web sites visited, programs run, time spent on Web sites or user programs, usernames, passwords or other types of data in transit. The information is typically either stored for later retrieval or transmitted to the remote process or person employing the Monitor. Keyloggers and Screen Scrapers are types of System Monitors.

Tracking Cookies: A Tracking Cookie is any cookie used for tracking users’ surfing habits. Tracking Cookies are a form of *Tracking Technology*. They are typically used by advertisers wishing to analyze and manage advertising data, but they may be used to profile and track user activity more closely. However, tracking cookies are simply a text file, and far more limited in capability than executable software installed on users’ computers. While installed software can potentially record any data or activity on a computer (see *System Monitor*), cookies are simply a record of visits or activity with a single Website or its affiliated sites.

Tracking software: Software that monitors user behavior, or gathers information about the user, sometimes including personally identifiable or other sensitive information, through an executable program.

Tricklers: *Automatic Download Software* designed to install or reinstall software by downloading slowly in the background so the download is less noticeable (and does not impair other functions). Tricklers are typically used to enable a spyware program to install silently or to reinstall after a user has removed components of the program from his or her computer.

Trojan: A program that appears to do one thing but actually does another (a.k.a. Trojan Horse).

Underlying Technology: One of the technologies listed in the table above that has been used to harm users; however with proper notice, consent, and control, these same technologies could provide user benefit.

United Virtualities Persistent Identification Element (PIE): United Virtualities PIE is a *Tracking Technology* designed to be an alternative to a cookie, utilizing Macromedia Flash. It is an example of a passive tracking technology.

User: The system owner or their designated administrator. In a household, this is commonly the person operating the computer.

Virus: Code that recursively replicates a possibly evolved copy of itself. Viruses infect a host file or system area, or they simply modify a reference to such objects to take control and then multiply again to form new generations.

Worm: Worms are network viruses, primarily replicating on networks. Usually, a worm will execute itself automatically on a remote machine without any extra help from a user. However, there are worms, such as mass-mailer worms, that will not always automatically execute themselves without the help of a user.

Zombie: A system that has been taken over using *Remote Control Software*. Zombies are often used to send spam or to attack remote servers with an overwhelming amount of traffic (a Distributed Denial of Service Attack). A collection of many zombies comprise a *Botnet*.