"Junkware": A New Name for "Spyware"

by Eric L. Howes

The name "spyware" was first used to describe unwanted commercial software during the spring and summer of 2000, when consumers became aware of "adware" -- advertising sponsored "freeware" -- which often monitors system use and reports potentially sensitive data to advertisers for the purpose of targeted advertising. The name "spyware" proved to be a catchy one, and consumers were soon using it to describe or name all manner of unwanted software that engaged in unwelcome behavior -- even software that did not technically "spy" on users. In other words, the term "spyware" became a loose, broad term used by consumers for a wide variety of unwanted, intrusive software that they understandably and rightfully deplore.

Although the name "spyware" has proved popular with internet users, it has caused more than its share of confusion because the term implies functionality (data gathering, backdoor connectivity, etc.) that some intrusive, unwanted software may not have. Not only have vendors of certain kinds of "advertising software" vociferously protested the application of the name "spyware" to their software, the name "spyware" has also caused users to confuse commercial advertising "spyware" with more traditional "spyware" such as keyloggers and other system monitors -- electronic snooping tools that differ markedly from commercial advertising "spyware" in that these snooping tools are deployed and used by individuals acting in their own interests, not by the companies who develop and distribute those tools.

Given that the name "spyware" has been overextended and is now only causing pointless confusion and useless haggling that distracts us from the crucial business of addressing the very real problems that consumers face with certain types of software on the internet, it is time that the name "spyware" be replaced with another one that more readily encompasses all the varieties of unwanted, intrusive commercial software that consumers are complaining about (and which they problematically lump together under the term "spyware").

While it will be difficult to find a replacement quite as catchy as the name "spyware," one possible replacement is "junkware."

Varieties of "Junkware"

By "junkware" we mean unwanted commercial software that is installed without the user's full knowledge, consent, and understanding, and that primarily serves the interests of commercial parties associated with the "junkware," not the end users on whose systems those unwanted applications are installed. The term "junkware" covers such applications as:

- **adware**: "advertising supported software" -- i.e., "free" software that is supported by the display of advertising -- often within the main window of the application -- or the use of the user's PC for other commercial purposes (e.g., distributed computing). This advertising is often accompanied by the collection and transmission of marketing and demographic data for the purpose of targeted advertising, which makes such applications spyware as well (see below for a definition of spyware). Although the software is billed as "free," the user in fact "pays" for the application by putting up with advertising as well as the collection of data (often about the user's behavior with the application or on the internet). Moreover, although the user typically clicks through EULA, thus consenting to this advertising and data collection, many (if not most) users are unaware of the true functionality of this software.

- **foistware**: commercial software that piggybacks on "free" software (a "host") and is installed along with the host application (such as KaZaA or Grokster). An alternative to straight "adware" that serves the same function, "foistware" often displays ads or collects marketing and demographic data for use by direct marketing companies, in which case such applications are spyware as well (see below for a definition of spyware). These piggybacking applications are referred to as "foistware" because they are unwanted by the user. Although users may have technically (legally) agreed to the installation of these "foistware" components during setup of the host application by clicking through a EULA, many (if not most) users are either unaware of these foistware applications or do not fully understand them.

- **spyware**: commercial software that monitors users' computer and Internet behavior, gathers other marketing and demographic data, and transmits those data to direct marketing and advertising firms, who often use those data for targeted advertising. Collected data may include personally identifiable or sensitive information, as well as information about users' internet behavior, computer usage, and usage of the application. Note that by the term "spyware" we do not mean such applications as keystroke loggers (keyloggers) or other similar system monitors that are used to snoop on users. Those applications do not have a marketing or advertising tie-in or use; commercial/marketing "spyware" does. (Note also that the term "spyware" here represents a subset of the larger category of unwanted software that I propose be called "junkware"; it is not used as a general term for all manner of unwanted, intrusive commercial software, such as the term is currently used among internet users and consumers.)

- **hijackware**: applications or web sites that set the user's default browser home page to an unwanted URL, change the default search engines defined within the browser to unwanted search engines and sites, or add unwanted toolbars and other custom plugins/add-ons to the user's browser and system. These applications and web sites may also configure Windows to prevent users from changing those settings back to the users' preferences or uninstalling the unwanted toolbars and plug-ins/add-ons. These applications and web sites may also edit the HOSTS file to tie known web sites to certain IP addresses, thus ensuring that users are unwittingly directed to unexpected, unwanted web pages.

- **drive-by-downloaders**: unwanted applications that install automatically when the user visits a web site. These are usually ActiveX controls and plug-ins, and users may or may not (depending on their Internet Explorer Security zone settings) see a pop-up requesting agreement to a EULA that authorizes installation of the application. In all cases, though, the download is initiated by the web site being visited, not the user.

- **porn dialers**: applications that employ users' modems to dial 1-900 numbers (often overseas) and connect with online services that distribute porn. The 1-900 phone charges that result from these phone calls are usually astronomical and outrageous. Moreover, these porn dialers are often installed via "drive-by-downloads," and users are frequently unaware that their modems are even being used to connect to 1-900 numbers (they find out later when the phone bill arrives).

There are many other terms that people have coined for these types of "junkware," however, "junkware" is a comprehensive term for all of these types of unwanted, intrusive commercial software.

Keep in mind that any one application may fulfill several of the above definitions. Thus, there can be "adware" that is also "spyware." There may be "drive-by-downloaders" that are both "spyware" and "hijackware." And so forth.

"Junkware" is often distinguished from other (more traditional) forms of malicious software such as viruses, trojans, and worms by the fact that, in most cases, the user clicks through a EULA (end user license agreement) at some point -- by contrast, no virus will ever ask you to agree to a EULA. Thus, the companies who push "junkware" on users can claim that users "elected" to install their applications. Nonetheless, this "junkware" is unwanted by and unknown to users even though they may have technically (legally) agreed to the installation of that software.

What "Junkware" Does

"Junkware" is a broad term that covers a wide variety of unwanted software applications that are pushed on users. "Junkware" often does one or more of the following things:

Stealth/Rogue Installation

- automatically installs with little notice or warning when users visit "junkware"-infested web sites with active content options enabled, as many sites require them to be;

- tricks users into installation by the use of deceptive buttons and hyperlinks, false error boxes and system notices, uncloseable popups, or other confusing GUI elements;

- falsely poses as Microsoft Windows Update software, "anti-spyware" software, or other software that may be desired by users;

- uses known "malware" such as the W32.Dlder.Trojan and/or exploits known security holes in Internet Explorer and Windows to install on users' systems and reconfigure users' systems;

- piggybacks on other host applications and web sites which install the accompanying "junkware" modules -- even when users uncheck the appropriate boxes and decline the installations -- and often provides no visible means to opt-out of the "junkware" installation alone;

- uses frequently changed/morphed installers and installation methods to avoid detection by "anti-junkware" applications such as SpyBot Search & Destroy and Ad-aware;

High Pressure Installation

- foists itself on users by piggybacking on other host applications which require installation of that "foistware";

- uses scare tactics (e.g., displays of users' drive contents, IP addresses, or browser headers; opening the CD-ROM drive) to exploit users' fears and pressure them into installation;

- is required by ISP's in order to provide "member content" and "connection maintenance" to users;

- installs along with drivers for hardware and is required for proper functioning of that hardware, or installs as part of a BIOS/CMOS software package;

Stealth Execution

- configures itself to automatically launch and run silently in the background every time Windows or Internet Explorer start without notifying users or seeking their knowing consent;

- obscures or hides its execution and behavior from users and "anti-junkware" utilities;

Rogue System Reconfiguration

- reconfigures users' systems to allow itself unfettered access to the Internet and allow "junkware" servers uninhibited access to users' computers;

- hijacks users' web browsers to drive users to unwanted web sites and search services by making undesired system customizations and locking users out of the settings that would allow them to restore their browsers to a preferred state;

- adds unwanted or unsolicited toolbars, searchbars, and other custom plug-ins or add-ons to the users' browsers or systems;

- replaces critical Windows system files, thus interfering with the normal and proper operation of the users' systems and even imposing a system "death penalty" on the PCs of users who do attempt to uninstall it;

Data Gathering

- monitors users' use of their computers and the internet, collects usage data and other personally identifiable or sensitive data about users, and provides those data via a network connection to direct marketing and advertising companies;

Backdoor Connectivity

- establishes unannounced, unwanted network connections for the purposes of making unrequested updates to the software and users' systems or supplying data to interested parties;
- makes unauthorized dial-up connections to 1-900 numbers without users' full understanding and consent;

Obfuscation

- buries key notices, terms, and conditions in complex EULAs and Privacy Policies that few consumers can make any sense of;
- provides insufficient notice of installation, data gathering, backdoor connectivity, system reconfiguration, or other undesirable behavior;

No Choice (Opt-Out/In)

- won't take "no" for an answer because it provides no readily available means to opt-out of (let alone opt-in to) privacy invasive data gathering, system reconfiguration, and/or system updating for good;
- demands that consumers to agree to outrageous terms & conditions such as the acceptance of unannounced / unsolicited updates, renunciation of third-party uninstallation methods (i.e., the use anti-"junkware" utilities such as SpyBot Search & Destroy and Ad-aware), or the uninstallation of "conflicting" programs (i.e., anti-"junkware" utilities such as SpyBot Search & Destroy and Ad-aware).

Uninstallation Countermeasures

- provides no visible means for uninstallation and removal;
- refuses to be uninstalled when the host application is uninstalled;
- provides broken uninstallers or uninstallers that actually install more "junkware";
- takes active measures to avoid being uninstalled by "junkware" removal utilities like Ad-aware and SpyBot Search & Destroy, blocks the download and installation of those utilities, and even silently uninstalls such utilities without the user's permission;

Other Definitions of "Spyware" or "Junkware"

Others in the "anti-spyware" scene or industry may classify software applications differently than I do. See in particular the following web pages...

SpyBot Search & Destroy - Target Policy (Patrick Kolla)
http://security.kolla.de/index.php?lang=en&page=knowledgebase/targetpolicy

SpywareGuide.com
http://www.spywareguide.com/category_list_full.php

Lavasoft Threat Assessment Chart
http://www.lavasoftusa.com/support/resources/

PC Pitstop - What is Spyware?
http://www.pcpitstop.com/spycheck/whatis.asp

and.doxdesk.com - Parasites
http://www.doxdesk.com/parasite/

Kephyr - Spyware
http://www.kephyr.com/spywarescanner/library/glossary/spyware.phtml

COAST - Glossary
http://www.coast-info.org/glossary.htm

Webopedia.com - Spyware
http://www.webopedia.com/TERM/s/spyware.html

...for other attempts to classify and define all the varieties of "junkware" (a.k.a, "spyware"). Note that some of the software described on those pages may be more traditional "malware" (i.e., viruses, trojans, worms).

Conclusion

Some may object to the name "junkware" because of the unpleasant connotations that it carries. If another more satisfactory name can be found, then it should be adopted. The important thing, however, is that we not let a dispute over a misused word like "spyware" distract us from the very important business of addressing the problems that consumers are complaining about when they encounter a broad class of unwanted commercial software on the internet, whether we call that class of software "spyware," "junkware," "greyware," "ad-ware," "bad-ware," "advertising software," "unwanted-ware," "mysteryware," or even "x-ware."

Definitions and terms ought to help us understand the world and grapple with the problems that it presents, not stand in the way of our efforts to solve those problems. When we are dealing with consumer complaints about intrusive, unwanted software on the internet, the particular name for that broad class of software is less important than the varieties of software that it allows us pull together under the umbrella of one term and discuss productively. Put another way, the particular name for that linguistic umbrella is less important than its ability to facilitate our attempts to address consumers' problems and concerns with the abusive software that falls under its cover.

29 March 2004