

Information Security Threats from Unsolicited Commercial Software

Dennis Monroe
dj.monroe@bitwaretech.com
BitWare Technologies

Unsolicited commercial software is a huge threat to information security in today's world. Otherwise known as spy-ware or ad-ware, this parasitic software is wreaking havoc on computer systems and user privacy. Recent research showed that one in three computers have spy-ware hidden on their hard drive and that the average is the same for business computers largely because of a lack of centrally managed spy-ware removal tools (Piercy, 2004).

Spy-ware comes in five basic forms ad-ware, spy-ware, scum-ware, homepage hijackers, and dialers (Clover, 2004). Many of these are benign tracking cookies used to remember a user's particular browsing habits and preferences. Others carry a far more maniacal purpose invading users' privacy, corrupting data, reducing system performance, and stealing valuable information, often for criminal intent.

Ad-ware is the most common type of spy-ware. Taking advantage of lax browser security settings and common social engineering methods, ad-ware is typically found in the form of a tracking cookie or software unwittingly installed by the user. Many freeware programs are supported by ad-ware software, which is installed along with the program. Once installed users will commonly receive unwanted pop-up adds while browsing (Clover, 2004).

Spy-ware is written to steal personal information, credit card numbers or passwords (Piercy, 2004). Often times this information is used by criminals to steal money or a person's identity. Spy-ware is propagated through browser security holes or by users who unwittingly install the spy-ware on their computer through installations of other software and Trojan Horses. One recent attack that targeted banking customers in the U. K. used a combination of a Trojan horse and Phishing (using bogus web sites to capture users' personal information) to steal personal information, credit card numbers and money (Ilet, 2004).

Scum-ware uses software on a user's computer to add links and banner adds to web sites that the user is visiting. The web site's author is unaware of the ads that are being associated with their site and is not compensated. Furthermore, scum-ware delivers targeted advertising to the user based on key words contained in the Web content the user is viewing. Like other forms of spy-ware scum-ware is commonly installed on a computer when the user downloads and installs several desirable free-ware programs (Scumware.com, 2004).

Homepage Hijackers are a malicious form of spy-ware that change a user's homepage to the makers' sites (generally loaded with advertising), and often times prevent them from changing it back (Clover, 2004). A similar type of parasite changes the users default browser to one that is supported by advertisers and offers links to their web sites. Hijackers commonly exploit Internet Explorer vulnerabilities that allow them to be installed secretly as .hta files on a user's computer. Others are installed as .exe files by unwitting users (Cexx.org).

Dialers are a particularly malicious attack because they steal money directly from the user via premium rate phone numbers dialed from a computer (Clover, 2004). same social engineering techniques that hackers use. Additionally, spy-ware makers use browser vulnerabilities.

A dialer is a very small program, often installed using the ActiveX technology. Dialers often promise access to free porn, free games or free cracks for commercial software. Once installed, a dialer offers to use your dial-up device to call in to the service, usually calling a quite expensive toll number. Some dialers explain the costs of the connection they will be making, like it is required by local law in some countries, but many dialers just display a button offering to connect, without informing the user of what is happening behind it. In the worst case, the dialer sets up the expensive number as the default Internet connection, meaning the user will have to pay high rates for being online, without even knowing it until receiving the next bill (Safer-Networking.org, 2004).

Spy-ware makers have many methods for distributing their acrimonious wares. Many of their methods use the same social engineering techniques that hackers use. Additionally, spy-ware makers use browser vulnerabilities, e-mail, cookies, and bundling to spread parasitic software across the web. Some spy-ware changes registry settings and in many cases prevents the user from changing them back.

One common method for distributing spy-ware is through bundling. Bundling is the process of hiding spy-ware tools within the installations of otherwise desirable software. "The P2P file-sharing programs are notorious for this; in particular, iMesh and Grokster come with countless unwanted add-ons. (Clover, 2004)" This method of social engineering offers the user something for free in an attempt to install unwanted software on the user's computer. People should always use extreme caution when downloading and installing any type of free software. Most of these companies make their money through advertising and won't hesitate to take advantage of an unwitting user to make money (Clover, 2004).

Many spy-ware tools are installed through Internet Explorers ActiveX installation option. With this method the user will be prompted to install the software (assuming that their browser security settings are set to the correct level). Often the prompt will attempt to trick the user by stating that the software is a necessary security update, or that the user has spy-ware on their machine (Clover, 2004). "For this reason, you should never click 'Yes' to a "Do you wish to download and install..." prompt unless you are 100% sure you trust the publisher of the software, which might not be the publisher of the web site you are viewing— read the dialogue box very carefully. (Clover, 2004)" .

Some of the more malicious spy-ware such as homepage hijackers and dialers use even darker methods of distribution. Most of these applications are installed through Internet Explorer vulnerabilities. Therefore it is important to always ensure that a computer's Web browser and operating system are up to date with the latest patches. Additionally, some security holes can be eliminated by setting the security level for the internet zone within Internet Explorer to it's highest level and excluding the Web pages that are frequently visited and have been deemed safe (Clover, 2004). One recent threat uses the iFrame vulnerability in systems that are not running Windows XP service pack 2 to redirect a user's browser to several Web pages that each attempt a different method to install spy-ware. Once the spy-ware is installed the computer is crippled by the amount of new software and pop-up ads (Shor, 2004).

Once unsolicited commercial software makes its way on to a computer system the threats to sensitive data and system performance are numerous and real. Recently, I was asked to look at an associate's machine that was having performance issues. Any time that she attempted to access the Internet her computer ran so slowly that browsing was no longer possible. Upon running a spy-ware removal tool I found over 1200 pieces of spy-ware located on her computer. Once the spy-ware was removed her system performance was returned to normal.

Spy-ware can also leave security holes, which are often used by hackers as a backdoor into a computer system, or as way to steal valuable information from a user while they are browsing the Internet. Data collected from spy-ware can be sent to hackers who may use it to steal money, credit card numbers, personal information, or even a person's identity. One recent attack in the U.K. used a Trojan horse to capture keystrokes and take snapshots of users' machines while they accessed banking sites. The information was then sent to hackers who used it to steal money and access accounts (Ilet, 2004).

Aside from creating security holes, tracking browsing habits and degrading system performance, spy-ware is a serious threat to data integrity. Poorly written, hidden, or otherwise malicious code can corrupt data, destroy files, and may be difficult to remove. In extreme cases an infestation of spy-ware can result in the need for complete operating system reinstallation (Shor, 2004).

However, there is hope and many free and commercial software programs exist to scan for and remove unsolicited commercial software. Two that I use and recommend are Spy-Bot Search and Destroy (download: www.safer-networking.org) and Ad-Aware (download: www.lavasoftusa.com). Spy-Bot Search and Destroy is completely donation supported and a full feature version can be downloaded for free.

Ad-Aware is primarily a commercial product; however, Lavasoft does offer an excellent free-ware version that can be used to scan a system. I recommend using both products, as they often maintain slightly different lists of spy-ware threats. Some proclaimed spy-ware removal tools are distributed by the spy-ware makers themselves and should be avoided at all cost. A list of questionable spy-ware removal tools can be found at <http://www.doxdesk.com/parasite/>.

Additionally, computer users can reduce the affects of spy-ware by running a personal firewall on their machine. Firewalls control access to a network resource and can be used to monitor open ports on a computer system. Unsolicited software that attempts to access the Internet will be stopped by a personal firewall and the user will be notified. A free personal firewall can be downloaded from http://www.zonelabs.com/store/content/catalog/products/sku_list_zs.jsp.

User awareness and increased browser security settings are the last lines of defense against malicious software attacks and unsolicited commercial software. All computer users should take personal responsibility and research any free-ware before installing it on their machines. Additionally, taking the time to increase browser security settings and defining Internet zones can prevent many types of spy-ware from making its way on to a computer system.

The threat from spy-ware and other forms of malicious software is one of the most dangerous modern threats to Internet security. Affected most are individuals and home users who do not have comprehensive security awareness. Their personal information, credit card numbers, money, and web browsing habits are all susceptible to threats from spy-ware. However, with a bit of education, security awareness, and readily available removal tools, threats from spy-ware can be reduced, and users can once again browse the Internet without fear.