Running head: THE INS AND OUTS OF SPYWARE

The Ins and Outs of Spyware

Lesley Herring

East Carolina University

Abstract

This paper addresses a hot topic in the security field right now, because it is getting out of hand and it is the fourth greatest threat to network security. Spyware is a bigger threat than viruses and in most cases it is harder to eradicate. I will discuss what spyware is, categories of spyware, types of spyware, symptoms of spyware, research sites to find out more information, prevention techniques, and removal tools.

The Ins and Outs of Spyware

Today, there is a bigger threat to safe and secure computing. This threat has quickly become a bigger headache than viruses, and in some instances it causes more damage than viruses. Time is spent battling this threat more than any other threat in my environment. While working at an insurance company for the past two years many different types of this threat have been seen. A call typically comes in through the help desk initially and then is passed on to me to investigate any unusual or malicious activity. Things that have been investigated consists of end-users calling about pop-ups, complaining that the computer is running slow, the home page of internet explorer is redirecting them to a webpage that is not bookmarked, and from time to time complaining that the computer will not completely boot all the way up. The threat is known as spyware. This paper will discuss what spyware is, what the symptoms of infection are, prevention techniques, sites to do additional research, and removal tools.

In my environment, spyware is the number one thing that affects the end-users. "The term spyware, as it relates to computers, first appeared October 16, 1995 in a Usenet post poking fun at Microsoft's business model" (Schmidt & Arnett, 2005, p. 68). Spyware is "any software intended to aid an authorized person or entity causing a computer, without the knowledge of the computer's user or owner to divulge information" (Thompson, 2005, p.42). In November of 1999, the first freeware program to include built-in spyware was a popular game called "Elf Bowling"; many users learned with surprise that the program actually transmitted user information back to the game's creator, Nsoft (Spyware – Information About Spyware, n.d.). Schmidt and Arnett state that with reports from multiple sources indicating that spyware has reached 90% home users PC (Schmidt & Arnett, 2005). The puzzle is how did it get there?

Categories

Spyware is installed two different ways, conspicuous and inconspicuous. Conspicuous behaviors are clearly evident to the user and inconspicuous behaviors include installation of spyware without consent (Awad & Fitzgerald, 2005).

Spyware can also be broken down into four categories. The first category is the overt provider. The overt provider inhibits conspicuous behavior. The overt provider is where users consent to its existence and receive positive consequences. Not in all but in some of the spyware programs globally unique identifiers (GUID) are used to collect customer information and in turn is shared within a network or interlinked websites to better server the user. For example, WhenU.com is an adaware company that provides customers with information on bargains and online savings. Another example would be Microsoft's error reporting service it collects data about machine configuration and network connections and sends it to its online crash analysis server to help diagnose software problems so that service patches can be developed and made available to the user community (Warkentin, Luo, & Templeton, 2005, p. 81).

The second category known as the double agent is conspicuous and is damaging to the end user. For example, "Xupiter launches pop-up ads, changes default home pages, redirects mistyped or incomplete URLS to affiliate sites and redirects search requests to off-brand search sites" (Warkentin, Luo, & Templeton, 2005, p. 81).

The third category known as the covert support is inconspicuous software but provides the end-user positive consequences. An example would be of helpdesk personnel have commonly provided support to users by viewing client screens remotely via network monitoring software (Warkentin, Luo, & Templeton, 2005). For example, "ComScore Network's Marketscore, which is a free downloadable application that increases internet surfing speed and

protects email from viruses, but also tracks user habits and compiles statistical data for industry research" (Warkentin, Luo, & Templeton, 2005, p. 81).

The fourth category known as the parasite is inconspicuous and has negative consequences, most occurs by drive-by downloading. The spyware that fits in this category are the most difficult to remove and typically consists of keystroke loggers (Warkentin, Luo, & Templeton, 2005).

Methods of Infection

Most users do not know they have spyware on their machine, much less how it got there. "Studies show that as many as 90 percent of Internet-enabled US home computers are infected with an average of 26 spyware programs" (Braff, 2005, para. 1). There are several methods that an end-user can be infected by spyware. "The main sources of spyware infections are pop-ups, free downloads, and shareware" (Zhang, 2005, p.46).

Drive-by downloading is a method typically used to infect computers with spyware. It typically occurs when a user visits a website or clicks on a web ad. Bundleware is another method that is used. Most users get more than they bargained for in some instances when they install one piece of software that is bundled with several others. Most file sharing programs such as Kazaa, Morpheus, Bearshare, Limewire, and Grokster use this type of methodology. Peer-to-peer networks are bad; spyware can hide in group directories and spread itself through infestation of the directories on a user's PC (Sipior, Ward, & Roselli, 2005, p.41). From time to time, the end-user wants to download a utility and after installing it, they have any extra added toolbar or icons on the desktop this is sometimes known as piggy-back applications. Another method of infection is by visiting a website that uses java or activex, once it is activated, the applet or activex code can download and invoke the spyware (Ames, 2004). The one that gets me is that

there are some intelligent spyware programs that will direct the end-user to a “removal site” where they download a program that supposedly removes their adaware, which in fact is more spyware (Pournelle, 2005). “Spyware can masquerade as a legitimate plug-in needed to launch a certain program or pose as a browser help object such as a toolbar. Spyware can also covertly install other spyware programs as part of an “auto-update” component” (Sipior, Ward, & Roselli, 2005, p.41)

Just remember, nothing is free, not even freeware or shareware. “You “pay for free” by sacrificing some personal information or some loss of personal privacy in exchange for great “free” features in software functionality that you can download without paying for as a “piggybacked” part of some other free applications you might wish to use” (Stafford, 2005, p.34).

Types

There are several types of spyware. Cookies, browser hijackers, system monitors also known as keyloggers, malware, dialers, spybots, adware, Trojan horses, browser plug-ins and tracks.

- Cookies are small devices stored on an individual user’s Web browser on behalf of a Web server, usually passive (Stern, 2005).

  “Simple cookies identification enables the site to recognize the user when he returns to the site, and it allows the site to associate the user with the known stored data he has provided” (Ames, 2004, p. 25).

  “Associated cookies track activity and store data gathered from the user’s interaction with each member site, once there, the spyware looks for recognizable cookies on the users systems” (Ames, 2004, p. 26).

- “Browser hijackers replaces the user’s home page, alters other browser settings and redirects searches and some URLS to the spyware vendors home page” (McFedries, 2005, p.72).
- System monitors “also referred to as key-stroke loggers, surreptitiously collects data from user-computer interaction, both locally and online. User keystrokes and mouse-clicks can be recorded while shopping or banking on the Web and locally while using software such as spreadsheets or videogames. This data can be transmitted back to the spyware installer, shared with other businesses such as marketers or sold to data consolidators” (Sipior, Ward, & Roselli, 2005, p.40).
- Malware is software such as worms and Trojan horses. Some such programs capture PCs and use them to disseminate bulk e-mail (spam). Zombie is the term for such a captured PC (Stern, 2005).
- “Dialers change dial-up settings on a computer to connect to another location, which may result in expensive long-distance charges. A stealth dialer makes its calls without any prompting from the user. A hijacking dialer changes the default Internet dial-up connection, so that all future Internet connections are routed through numbers that incur expensive charges” (Shukla & Nah, 2005, p. 86).
- Spybots monitor user behavior, collects logs of activity, and transmits them to third parties (Stern, 2005).
- “Adware is used for direct marketing on the Web, with or without user consent. By monitoring users Web browsing or by using detailed target market profiles, adware, delvers specific advertisements and offerings, customized for individual users as they browse the Web. These advertisements can take the form of pop-up or pop-under ads. Web banners, redirected Web pages, and spam e-mail” (Sipior, Ward, & Roselli, 2005, p.40).

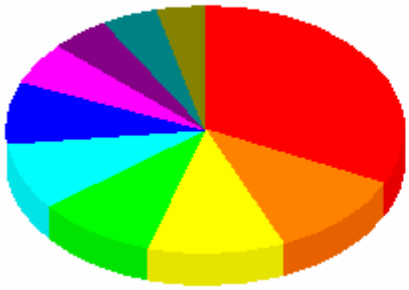
- "Trojan horses are a malicious form of spyware named for the Trojan horse from Greek history, a Remote Administration Trojan (RAT) or Trojan can take control of a user's computer by installing itself with a download and taking directions from other computers it contacts via the Internet. Trojans can turn a PC into a spam proxy without user knowledge or use Microsoft Outlook e-mail as if it were a browser to allow for a torrent of pop-up ads. Trojans can also be designed to steal data or damage computer files" (Sipior, Ward, & Roselli, 2005, p.40).
- "Browser plug-ins typically appear in the form of search toolbars in browsers. Not all browser plug-ins are harmful; however, many have been known to transmit user data to their creators and are installed using covert means" (Shukla & Nah, 2005, p. 86).
- Tracks records information about actions the user has performed, listing, opened files, and programs. This information could then be provided to third-parties (Stern, 2005)

Symptoms

In a survey of over 600 North American businesses by IDC, spyware was ranked as the fourth greatest threat to network security (Hinde, 2004). Spyware can cause a lot of devastating effects to the end users computer. "Microsoft claims that half of all computer crashes reported by its customers were caused by spyware and its equivalents. Spyware is also responsible for about 12% of all technical support calls and accounts for the biggest category of customer complaints according to Dell" (Shukla & Nah, 2005, p. 85). During the research of this paper, spyware infected my computer. My desktop had been taken over by this black screen with this yellow box that appeared on my desktop it stated "Warning, Spyware detected on your computer, install an antivirus or spyware remover to clean your computer". Below the box there was a link to a list of top spyware removers that were most likely just more spyware infections. During infection, it

also dropped a Trojan on my computer. The anti-virus suite that we use at work is called Trend Micro OfficeScan; it protects networked clients and servers from viruses, Trojans, worms, and hackers, plus spyware, grayware, and blended threats. As the table below illustrates, the top threats on my network today are indeed spyware programs. These spyware programs wreak havoc on the end-user's machines causing several different symptoms.

Top 10 Viruses Detected



Virus Name	Virus Count
1. ADW_SAVENOW.A	288
2. ADW_WEBSEARCH.AH	107
3. SPYW_SOFTOMATE.A	104
4. SPYW_EXCTSEAR.A	93
5. JAVA_BYTEVER.A-1	81
6. JAVA_FEMAD.B	80
7. DOS_AGOBOT.GEN	54
8. ADW_SIDESEARCH.A	46
9. JAVA_BYTEVER.A	44
10. SPYW_SPYANYWER.A	38

Some of the symptoms that the computers inhibit are that usernames and passwords are stolen to launch attacks and gain access. A Trojan may be installed in order to remotely control the computer as well as capture every keystroke. Be careful, spouses may run a keystroke recorder to monitor spouses whom they suspect of cheating. The computer may become hijacked and become a zombie so it is used in denial of service attacks against other computers. Emails can be sent without the user's knowledge causing a spam launching pad. Dial-up users can be a victim of a dialer program. The program hijacks the modem and makes calls to 900 numbers running up the telephone bill.

The biggest complaint in the end-user community is typically browser related. Some computers may have the browser redirected to spyware-affiliated addresses, and display pop-up advertisements. Some of the users may not be able to launch internet explorer. In some cases,

even after removing the spyware, internet explorer still may not open. The spyware application may send to the server surfing habits so that the server can in turn spam the computer or push pop-ups to the screen.

Phone home applications are becoming more popular for legitimate and illegitimate websites. There is some spyware software that has the ability to phone home information, also known as an ET application. Keep in mind, not all phone home applications are detrimental, "legitimate licenses remote monitoring applications can also operate just like spyware, stealing machine cycles and telecommunications resources to "report home," such as the case with Kodak digital camera software and its update agent provided by "BackWeb"" (Stafford, 2005, p.36). Since some of the spyware programs do phone home, usually there is so much chatter it reduces the available bandwidth.

Many symptoms of spyware may impair the performance of the computer. Machine performance may be downgraded by increasing the number of CPU cycles. A number of programs running simultaneously may increase therefore cause the system to freeze and crash. In the lab at Computer Associates they infected a computer with one adware pest; it slowed the computer's boot time by 3.5 minutes (Thompson, 2005).

There are a number of other symptoms that a computer may have. Extra icons may appear, system settings may change, and spyware programs may shut down the computer or open and close the cd-rom drive and open or close programs. In some cases, spyware may cause random error messages, cause software conflicts, create new and unexpected toolbars, and some common keys, such as tab may no longer function. Another thing that may happen is that hard drives can be scanned to obtain information from a user's files and application programs such as email, word processors, and games.

Prevention Techniques

For the work organization, education and protection are vital. Most organizations deal on a daily basis with customer's personal information. There should be policies in place that forbid visitation of websites known for placing spyware, gambling, and pornography. The policies should also prohibit peer-to-peer file sharing and downloading of freeware and shareware. We actually use a web content filtering product called Websense, where I work at. The organization should also look at installing security software. Develop corporate policies and values on privacy. Business must also develop best practices to collect and use consumers' person information by notifying and getting consent from consumers instead of surreptitiously collecting and disseminating information. Educating business with the improper information collection and distribution is also necessary. Developing corporate policies and values privacy is vital because corporate IT and marketing actions visibly influence the way the organizations deal with customers, prospects, employees, shareholders, and the media. (Ames, 2004)

For the home user, pay attention to what is being installed. Many spyware programs will try to get the end-user to download software to get rid of the spyware that is on their computer, when in fact it is more spyware. Before installing any software, read the end user license agreement (EULA) carefully. If there is a suspected infection, immediately disconnect from the internet to prevent further harm. Do not open spam or any e-mail from persons unknown or with an unexpected attachment. If XP is the current operating system, disable the messenger service. Install a spam filter for scanning the local email client. Install or if there is one present, activate the pop-up blocker. Install a firewall, it can block spyware from sending information over the internet and block the self-update features of spyware. Do not participate in peer-to-peer programs, malware, viruses, and worms hide in these programs. Run a virus check on unfamiliar

files. Keep operating system patched at all times. Consider using Mozilla Firefox rather than Internet Explorer. However, if Mozilla cannot be used, enforce the usage of high security settings in Internet explorer. Last, but least please install an anti-spyware solution. The end-user might want to consider installing multiple ones because one will not remove all of them.

More Information

To find out more information about spyware, please visit the sites below.

http://cexx.org/adware.htm

http://www3.ca.com/securityadvisor/pest/search.aspx

http://www.kephyr.com/spywarescanner/library/index.phtml?source=bassindex

http://www.spywareguide.com/

http://www.stopbadware.org/

http://www.spywarewarrior.com/

http://www.trustgauge.com/

Removal Tools

Steve Gibson is credited with creating the first anti-spyware program, Optout in 2000 (Schmidt & Arnett, 68). There are several anti-spyware applications on the market today. Please visit the sites below for more details.

Norton Internet Security [Read the WinPlanet.com Review]

Windows Defender (Beta 2)

SpyBot S&D (freeware) [Read the WinPlanet.com Review]

Ad-aware (free version available) [Read the WinPlanet.com Review]

Geek Superhero [Read the WinPlanet.com Review]

X-Cleaner (freeware)

Spy Sweeper [Read the WinPlanet Review]

PestPatrol [Corporate Edition Review]

HiJack This

StartUpList (detects programs running at Start-Up)

Trend Micro Anti-Spyware

SpyRemover

Keylogger Killer

Who's Watching Me

Personal AntiSpy

Keylogger Hunter (freeware)

KL Detector (freeware)

Spy Detect

BHODemon (scans for Browser Helper Objects that run when your browser is started)

a^2 Software

Yahoo Anti-Spy Toolbar

There are probably several other anti-spyware products on the market, but this was just a list of a few of them. Spybot, Ad-aware, and Windows Defender, which happens to be all free happens to be successful for myself. Cnet has recently just come out with their list of the top 10 antispyware apps. It is good to note that out of ten applications, three are free. Cnet's lists consists of Lavasoft Ad-aware, ZoneAlarm Anti-Spyware, Tenebril SpyCatcher, Webroot Spy Sweeper, PC Tools Spyware Doctor, McAfee AntiSpyware, Spybot Search and Destroy, Microsoft Windows Defender beta 2, Trend Micro Anti-Spyware, CA eTrust PestPatrol. Just remember to run them all, but not simultaneously because just one will not clean it all.

In conclusion, Spyware is the PC user's latest and biggest problem; a larger source of worry, concern, and frustration than anything PC users have faced before, and potentially more damaging that the worst computer viruses (Gibson, 2005). After reading this paper, I hope the end-user community has more information in regards to what spyware is and how to prevent it.

References

*Ames, Wes (2004, September/October). Understanding Spyware: Risk and Response [Electronic version]. *IT Professional*, 6(5), 25-29.

*Awad, Neveen Farag, Fitzgerald, Kristina (2005, August). The Deceptive Behaviors that Offend Us Most About Spyware [Electronic version]. *Communications of the ACM, 48*(8), 55-60.

*Braff, Andrew T. (2005, August). Defining Spyware: Necessary or Dangerous. *Shidler Journal for Law, Commerce+Technology*. Retrieved March 13, 2006 from http://www.lctjournal.washington.edu/Vol2/a001Braff.html

*Gibson, Steve (2005, August). Spyware was Inevitable [Electronic version]. *Communications of the ACM, 48*(8), 37-39.

*Hinde, Stephen (2004, December). Spyware: the spy in the computer [Electronic version]. *Computer Fraud & Security, 2004*(12**),** *15-16.*

*McFedries, Paul (2005, August). Technically Speaking: The Spyware Nightmare. *IEEE Spectrum, 42*(8), 72.

*Pournelle, Jerry (2005, June). Drive-By Spyware & Other Horrors [Electronic version]. *Dr. Dobb's Journal, 30*(6), 96-98.

*Schmidt, Mark B., Arnett, Kirk P. (2005, August). Spyware: A Little Knowledge is a Wonderful Thing [Electronic version]. *Communications of the ACM, 48*(8), 67-70.

*Shukla, Sudhindra, Nah, Fiona Fui-Hoon (2005, August). Web Browsing and Spyware Intrusion [Electronic version]. *Communications of the ACM, 48*(8), 85-90.

*Sipior, Janice C., Ward, Burke T., Roselli, Georgina R. (2005, Spring). The Ethical and Legal Concerns of Spyware [Electronic version]. *Information Systems Management, 22*(2), 39-49.

Spyware – Information About Spyware. (n.d.). Retrieved March 14, 2006 from http://www.spyware.gadget-info.com

*Stafford, Thomas F. (2005, August). Spyware was Inevitable [Electronic version]. *Communications of the ACM*, *48*(8), 34-36.

*Stern, Richard H. (2005, January/February). FTC cracks down on spyware and PC hijacking, but not true lies [Electronic version]. *IEEE Micro*, *25* (1), 6-7, 100-101.

*Thompson, Roger (2005, August). Why Spwyare Poses Multiple Threats to Security [Electronic version]. *Communications of the ACM*, *48*(8), 41-43.

*Warkentin, Merrill, Luo, Xin, Templeton, Gary F. (2005, August). A Framework for Spyware Assessment [Electronic version]. *Communications of the ACM*, *48*(8), 79-84.

*Zhang, Xiaoni (2005, August). What Do Consumers Really Know [Electronic version]. *Communications of the ACM*, *48*(8), 44-48.