

Spyware Study

Prof. Robila

CMPT 495

Computer and Data Security

**Group:
Francis Rivera
Douglas Schemly
Igor Yussim**

Due:

December 12, 2005

Table of Contents

Topic	Page
Spyware and the History of	3
Spyware Prevention	6
Anti-Spyware	11
Works Cited	16

Francis Rivera
CMPT 495
Prof. Robila

Spyware and the History of

Spyware is intrusive software that infects over ninety percent of the PC's that are on the net. As a matter of fact, the computer that I'm using to write this paper is infected with Spyware. I have tried my best to get rid of it on my own, but I just do not want to spend the money for a good anti-spyware tool. So I live with it, just like many other people out there who do the same thing.

But what is spyware and why is it so bad? Spyware, According to Microsoft is a general term used to describe software that “performs certain behaviors such as advertising, collecting personal information, or changing the configuration of your computer”. These actions are a personal intrusion into ones privacy and provide a danger financially and politically to people. Most of the time, you consent to having spyware on your machine in exchange for free software. However, the terms and agreements are often not portrayed in a manner that is understandable. That is way almost all of us always click I accept when installing downloaded software, without reading the terms of the agreement.

How does spyware work? There are two main whys in which spyware works. The first way that I will discuss is Tracking Cookies. Tracking Cookies are cookies that are used to track web pages that are visited by the computer. That information is then sent to a server that will then send specific marketing pop-up ads according to the web pages that where visited. The signs that your computer has Tracking Cookies are that you receive many pop-up ads, even if you are not on the web, slower runtime and

frequent computer crashes. The second Type of spyware that I will discuss is A Browser Hijacker. A Browser Hijacker is malicious software that changes your browser settings and usually adds unwanted toolbars. The way the Browser Hijacker then redirects you from the sites you want to other sites to artificially increase hits on that site, which increases revenue. You can tell if your computer has been browser hijacked by the changing of your homepage, being misdirected from the pages that you are trying to visit, and slower runtime and frequent crashes.

In the second part of this paper I will discuss the history of spyware. The word spyware first appeared in 1996 on the Usenet. It was used to sarcastically point out Microsoft's business strategies, according to PCsecurity.com. As a matter of fact the word spyware did not come to mean what we know it as today until the year 1999, when the first anti-spyware software came on the market called OptOut. Most people had there first experience with spyware when the popular free internet game called Elf Bowling came out in 1999. The software supposedly contained tracking software which was used to send data back to the games creator Nsoft. Weather this was true or not, it being said made the mass public aware that spyware existed and that it was a threat to their privacy.

Though the general public did not become aware of spyware until 1999 what we now consider spyware today did exist before that. In 1998 the company NetZero was started. The idea was to provide people with free internet access in exchange for them displaying what NetZero called the ZeroPort. The ZeroPort which was developed by Dash is a small navigational toolbar that can never be closed. It displays advertisements to the person who is surfing the web. Also the material that is being searched on the web is being sent back to a central server where the information is analyzed so that the

advertisements, which must remain on while the person is on the web, can be tailored to what that particular person is viewing. The idea was that the person who had NetZero would be shown the products that were advertised by the ZeroPort and a percentage of the proceeds would be sent to NetZero so that they could provide free internet and make a profit.

In conclusion, what started out as a way to provide people with free internet access at the price of viewing the ZeroPort, turned into the most intrusive invasion of privacy known to man. Spyware is the new virus of computing. Though it does not replicate like a virus, it is as dangerous if not more. Spyware has the potential to cost a person very dearly, whether financially or politically.

Douglas Schemly

CMPT 495

Prof Robila

Spyware Prevention

Learning what spyware is one important step to fighting it. The next step is to learn ways to prevent spyware from being placed on your computer. There are five things that a person can do to help prevent spyware being installed on their computer. The five actions are safe surfing, adjusting your browser's security settings, keeping your computer's software updated, using firewalls, and using spyware prevention software. To understand these prevention steps involves a further look into what they mean.

The first one safe surfing can be a crucial step in preventing spyware. What exactly does it mean to safely surf the net. First it means only go to the web sites you know and trust. Stay away from the strange sites, like porn sites, ones that are offering the free software or just the strange ones that people say have funny things on them. Many of these sites will ask you to download certain programs onto your computer and will attempt to do that. This leads to the next step people can take in safe surfing, which is to ignore and properly close pop ups. These pop up ads usually appear as some great software, a technical support message, or a security alert. These are called FUI's (Fake user interfaces). Some other examples of these ads can be ones offering quicker downloads, a better search engine, or to the offer to remove spyware off your computer. The best bet is to ignore them and close these windows. A problem is though is that

some of these pop ups have a face X or close tab that directs you to the site. That is why it is important to make sure you click on the right X or close tab. Another option is to use the ALT and F4 keys together to close the window. A last option is to right click on the window in the Window's task bar and then choosing close. The last thing that is involved with safe surfing is to watch what you download. The freeware programs or P2P (peer to peer) programs that people download contain spyware with them. Using the file-sharing applications place users at a higher risk to be infected with spyware than other people who don't. The risk involved with using these applications include the spyware that is bundled with the program, the internet connections that do not close, or mislabeled files being shared. People will find out what a popular song or movie is and then have spyware program and just name it with the file so people download and use it placing the spyware on their computer. Before downloading any software there are a couple of steps to take before you do. First read all the security warnings, license agreements, and privacy statements associated with the software you download. The second step is to do some software research. This can be accomplished by typing in the name of the software with the word spyware in a search engine and see what results come up. Here it can be seen if anybody reported any link of spyware with the program. Another research step is to search the databases of sites that list programs that contain spyware. Some examples of sites are PestPatrols Spyware database, Kephyr, and Spyware-Guide.com.

In addition to the safe surfing is keeping your software updated. It is important to keep the software on the computer updated plugs the holes in the software that attackers use to attack the computer. Windows is notorious with its software update and they are a

pain to keep up with but it is crucial to download and install them. Two options are to run the automatic updates for the Windows operating system. To accomplish this right click on My computer go to properties into automatic updates and then check the box that says make sure my computer is updated. The second option is to visit windowsupdate.microsoft.com and in the site let it scan the computer and download anything that is listed as crucial. The same applies with all other software where it is necessary to check the websites of the software to see if there are any updates, usually should be checking once a month.

A little more complicated defense against the installation of spyware is adjusting the browser's security settings. One recommendation is in internet explorer to open up tools and then click internet options. In the internet options window click on the privacy tab and change the security zone setting to at least medium or higher. A major issue in the security of the browser is the ActiveX controls. ActiveX is a set of technologies that allows software components to interact with one another in a networked environment, regardless of the language in which the components were created. This definition of ActiveX is from the Windows glossary. Why ActiveX is dangerous to the computer: One reason is that when the browser runs an ActiveX control it is running an .exe file which is an executable program. This concept is an idea attackers can use for malicious purposes. The steps to take control are as follows: Open up the control panel and select the internet options. Click on the security tab and choose custom level, here there are a bunch of internet properties with options to choose from. In these make sure the following are set:

Download signed ActiveX scripts = Prompt

Download unsigned ActiveX scripts = Disable

Initialize and script ActiveX not marked as safe = Disable

Installation of Desktop items = Prompt

Launching programs and files in a IFRAME = Prompt

Active Scripting = Disable

Scripting of Java applets = Disable

The problem with these setting is that many prompts will appear while surfing, so there is an additional step where it is needed to add the sites trusted into the trusted sites area. To access this it is under the security tab and click on the trusted sites icon. In this window make sure “Require server verification (https:) for site in this zone” is unchecked.

A fourth thing to do to increase the protection against spyware is to use firewalls. Even though most of the spyware that is placed on computers comes bundled with software that is downloaded some is actually placed on the computer by hackers. Firewall aid in stopping computers and programs from connecting to the system. They also prevent hackers form scanning the computer’s ports and resources including file and printer shares. Windows XP provides a firewall to its users. To activate the firewall go to the control panel, click on network and internet connections, then click on network connections, right click on the internet connection being used. From here select the properties and click on the advanced tab, in here click on the box next to “Protect my computer and network by limiting or preventing access to this computer from the internet.” After this is accomplished the firewall will be turned on. In addition to free firewalls there are many firewalls available for purchase that will provide more protection for the computer.

The best available method for the prevention of spyware is to use spyware prevention software. Here is a list of some of the spyware prevention software available: Spyware Inoculator, Spysites, SpyStopper, SpyBlocker, SpywareBlaster, SpywareGuard, Anti-Keylogger, and Blue Coat ProxySG. To understand what this software entails it is needed to take a look at them. Spyware Inoculator is one that is priced at \$24.95 which has the following features: blocks spyware installation, blocks tracking cookies, scans your PC for and removes spyware tracking cookies, disables flash animation, prevent other users from changing your home page, online updating of the database from within the program, and the current protection count is 3,857. Another spyware prevention software is SpyBlocker priced at \$19.95 with the following features: blocks spyware before it reaches your computer, starts up when your computer starts up, speeds up internet surfing up to 300%, cuts down Email SPAM, works with your entire system and all browsers, completely automatic with no complicated settings, works with Windows 98 up to XP and has fast customer supports service and support forums. To find more information on these spyware prevention software's search for them by typing in the name and open up the webpage that has them.

Taking all these steps will help prevent installation of spyware on the computer but it will not stop it completely. It is inevitable that eventually a computer will acquire some spyware on it, so it is necessary to take the steps in removing it off your computer. That is where Anti-spyware and spyware removal programs come into play.

Igor Yussim
CMPT 495
Prof. Robila

Anti-Spyware

If you don't want spyware on your computer, you can try to remove it manually.

However, spyware removal is a difficult and complicated process for even the most experienced computer user. Without the use of a spyware detection utility this can become nearly impossible. Even if you think you've successfully removed a piece of spyware manually, it can leave a tickler that completely reinstalls the spyware program the next time you start up your PC. As a survival tactic, these same malicious programs often leave similar traces elsewhere on your system so the game of cat and mouse never ends, unless you have a spyware detection and protection utility in place. Your best bet is to use an adware or spyware removal utility to rid yourself of problem causing programs.

Spyware is getting smarter. The newest threats are better than their predecessors from just a few months ago at hijacking your browser, watching your Web surfing, and stealing your data. Your current anti-spyware program may not be up to the challenge. The good news is that spyware fighters are evolving, too. An array of updates and new products were tested. The test group included five paid stand-alone tools--McAfee AntiSpyware 2006, PC Tools' Spyware Doctor 3.2, Sunbelt Software's CounterSpy 1.029, Trend Micro's Anti-Spyware 3.0, and Webroot Software's Spy Sweeper 4.0; three all-in-one security suites--Panda Platinum Internet Security 2005, Symantec Norton Internet Security 2005 AntiSpyware Edition, and Zone Labs' ZoneAlarm Internet Security Suite

6.0; and three free products--Lavasoftware's Ad-Aware SE Personal Edition 1.06, Microsoft's publicly available beta of Windows AntiSpyware (Beta 1.0.615), and Safer Networking's Spybot Search & Destroy 1.4. Though the suites cost more than stand-alone spyware apps, they come with antivirus, firewall, antispam, and privacy components.

While adware can be a major annoyance, spyware can be very dangerous, so the focus was the latter type of threat. Spyware not only installs itself surreptitiously in a system but can also download other unwanted applications without your consent. Dozens of spyware programs were collected, including the latest versions of threats used in our last anti-spyware roundup as well as new malware. As a result, we can't precisely compare scores between the two reviews, though we can draw some conclusions.

In all, these spyware programs added 73 unwanted files to the test computer. With them, the anti-spyware tools' abilities were challenged to detect and clean up the components. Here is how the products fared.

Webroot's \$30 Spy Sweeper 4.0 removed 90 percent of the spyware components--the highest score--which helped make it the Best among the stand-alone applications. This product is recommended if you already have antivirus, antispam, and firewall software. Of the three all-in-one suites, Panda Software's \$50 Platinum Internet Security 2005 was the best. Panda scored the highest of the three in total spyware removal and second-highest among all products, removing 86 percent of the spyware components. Panda also removed spyware without forcing the user to make case-by-case decisions.

Among the free products, no clear winner emerged. If you don't want to pay for a spyware fighter, it is recommended running more than one free program to increase your protection.

The biggest improvement came from McAfee AntiSpyware 2006 (\$30), which nabbed 79 percent of total spyware components in our tests. Last year's McAfee AntiSpyware 2005 removed only 22 percent of spyware tested. Both spyware and anti-spyware have changed since the previous tests, but this improvement is still noteworthy.

Symantec's suite also removed 79 percent of total tested spyware components; however, it made some poor recommendations. For example, it advised to give Internet access to the FXAgent Trojan horse, a keylogger activated from an embedded e-mail link claiming to lead to a Symantec removal tool. When installed, the resulting dlhost.exe file, which subsequently tries to access the Internet, was added to the Windows system directory. Symantec says that it has since made available a software update for the suite that would recognize this Trojan horse and eliminate it upon first contact.

The biggest disappointment was Sunbelt Software's CounterSpy (\$20. CounterSpy removed only 66 percent of total spyware components, down from 85 percent in last review. Microsoft's free Windows AntiSpyware beta also removed only 66 percent of total spyware components. The similarity is not surprising, since the two products share

technology from Giant Company Software, an anti-spyware firm that Microsoft acquired in December 2004.

One key measure of anti-spyware software is its ability to remove spyware processes running actively in memory; such processes represent a portion of the total spyware components mentioned above. Panda was the only program that removed 100 percent of the running processes. McAfee followed closely, erasing 96 percent. Spy Sweeper came in third, at 88 percent.

Some spyware components in our test group altered Internet Explorer's home page, search page, browser helper objects (BHOs) and toolbars, and Trusted Sites Zone. We tracked the anti-spyware products' ability to detect and reverse these unwanted changes. Spy Sweeper did the best job of detection and cleanup, removing 100 percent of the BHOs and toolbars embedded in our test PC's browser, as well as reversing all of the browser start- and search-page changes. Panda and McAfee removed 100 percent of the BHOs and toolbars, but they failed to reverse any changes to browser start and search pages. Trend Micro and the ZoneAlarm suite also did not reverse start- and search-page changes, but they did remove 50 percent and 86 percent, respectively, of the BHOs and toolbars. Symantec reversed all page changes but removed just 79 percent of the BHOs and toolbars.

Besides removing all BHOs and toolbars, Webroot's Spy Sweeper was the only anti-spyware application to detect and remove a particularly nasty variant of Look2Me. This

tenacious program hooks into the Windows Logon and tracks the Web sites you visit while also downloading additional spyware and adware.

Works Cited

www.microsoft.com

www.pcsecuritynews.com

www.gainpublishing.com

<http://www.microsoft.com/athome/security/spyware/default.msp>

<http://www.spywareguide.com/>

<http://home.planet.nl/~kleyn080/Spywareinfoen.html#voorkomen>

<http://www.intranetjournal.com/spyware/preventsoftpr.html>

<http://www.intranetjournal.com/spyware/filesshare.html>

<http://www.pcworld.com/howto/article/0,aid,117879,00.asp>

<http://www.pcworld.com/howto/article/0,aid,117425,00.asp>

<http://www.pcworld.com/howto/article/0,aid,118058,00.asp>

<http://www.pcworld.com/howto/article/0,aid,118060,00.asp>

<http://www.webroot.com/resources/spywareinfo/protection.html>