What is Spyware?

Daniel Jonasson
danjo620@student.liu.se

Johan Sigholm
johsi264@student.liu.se

Abstract

During the last few years the term spyware *has become increasingly spread. The definition, though, is still quite indistinct. In this paper we strive to explain what spyware really is, what types and forms it comes in, and examine how it relates to other forms of malicious software. We take a closer look at one instance of especially malicious spyware and also at a number of anti-spyware programs that are out on the market. Finally we compile a list of recommendations on how to protect oneself from the spyware threat and how to become spyware-aware.*

Our findings show that it is close to impossible to be completely safe from spyware attacks and that none of the anti-spyware programs manage to handle all forms of attacks. However one can reduce the risk by running several of them and increase one's consciousness about the dangers. From our examination of the situation today we draw the conclusion that spyware is becoming an increasing problem for both companies and end-users but that, however improving, anti-spyware software still is incapable of addressing all the threats.

1 Introduction

Security and privacy issues are in the focus like never before. New viruses, security compromising software bugs and various forms of malicious software threatens the integrity of our data as well as our own on a daily basis.

Most of these threats have been around for quite some time but the last few years a new type of threat has become more and more frequent: the threat of spyware.

In this paper we will examine what spyware really is and how it relates to other forms of malicious software such as viruses and trojans.

The rest of this paper is organized as follows. A theory section tries to explain what spyware is, who uses it and why they do, followed by a section with a case study of a real spyware application and its use. Finally we try to give the reader a recommendation of how to protect oneself from spyware and draw some conclusions.

2 Theory

2.1 Definition of Spyware?

There does not seem to be a consensus about a definition for spyware but in loose terms it is a piece of software that gathers information about a computer's use and relays the information back to a third party, for example with the intention of customized advertisements [14]. Another example of spyware is a so called *keylogger* that could introduce backdoors to a system by sending a user's keystrokes to the initiator of the attack.

Some formal definitions that more or less agree on what spyware is:

> Software that gathers information about use of a computer, usually without the knowledge of the owner of the computer, and relays the information across the Internet to a third party location [13].

> Applications that lurk in the background and capture enverything from keystrokes to the URLs of Web sites I visit [7].

> Spyware is software, installed by a third party without the user's fully informed consent, with undisclosed subroutines that track a host's Internet activity and send the information to a spymaster [6].

Spyware is often introduced to a user's system embedded within another software package such as a file sharing application, an instant messenger or another network dependent program [14]. When the user installs the package the spyware is installed as well and starts gathering and sending personal information in one form or another. It is therefore often hard, even for experienced users, to distinguish between what is normal, intended, communication and what is spyware related.

The explosive growth of the Internet together with many operating system's ambition to hide complexity from their users (i.e. allowing background threads to communicate with remote servers) has created an environment where it

is hard to prevent spyware. 'As is often the case, there is a tension between usability and security, and to date market pressures appear to favor usability' [14].

In the sections below we describe different classes of what can be considered as spyware. Together they give an overview of spyware rather than a formal definition.

2.1.1 Adware

Adware can do a number of things from monitoring your Web surfing and spending habits to popping up ad windows as you surf.

Often adware comes *bundled* with other software that is financed through the advertisement revenues. Depending on whether the EULA (End User Licence Agreement) gives the user knowledge of this it is debated if adware should be categorized as spyware or not.

Many times adware can be rather harmless, just modifying the ads after the user profile without any kind of automatic information gathering or transfer. However, due to the publicity of spyware lately, adware has gotten a very bad reputation in the eyes of the general public and many companies are reluctant to utilize adware from fear of smearing their company image.

On the other hand there are many adware applications that deploy various strategies to stay hidden and hard to remove while gathering as much information as possible. Often these applications are actually another form of spyware (for example key loggers) that just use the adware-front as means of infiltration.

2.1.2 Cookies and E-mail tracking

Cookies and e-mail tracking are (or at least can be) a passive form of spyware. They do not contain any code of their own but rather rely on existing Web browser or e-mail client functions. For this reason they are often considered to be a mild form of spyware.

Cookies are used to store a *state* in the user's Web browser on behalf of a Web server. Only the initiating server may later retrieve the cookies but since many sites use the same provider of advertisement, cookies open up for the possibility to track the user's behaviour across these sites [14].

In a similar way, e-mails containing HTML-code - with for example a URL to an image on a remote server - can be used to keep track of a user. Within the URL there is a unique identifier related to the e-mail address that is picked up by the server to verify the validity and use of the e-mail account.

2.1.3 Browser Hijackers

A simple form of browser hijackers, that 'enter your computer' when you visit a web site and for example click an OK-button, attempt to overtake certain functionality of the default browser on a user's system. One common approach is to change the start page of the browser to one where advertisement is shown [15]. It is also common that the hijacker generates pop-up windows with additional advertisements, sometimes so many that the user is not able to close them all and the browser (or even the computer itself) slows down and crashes.

A more serious form of hijacker, that could be distributed together with a normal program, install a BHO (browser helper object) or similar that alters the behaviour of the browser. With a BHO it is possible to monitor all the user's activities within the browser software, such as all typed or clicked URLs and produce arbitrary responses to these events. One consequence of this is that a user's search strings could be recorded and passed on to a third party.

Moreover, since in Windows, the Internet Explorer browser and the Explorer application (that among other things handle local file browsing) are closely linked together a BHO could create many problems also outside the Internet browser. For instance imagine all links between file types and their default executing application replaced with the BHO or simply removed [8, 3].

2.1.4 Spybots

Spybots are maybe what most people think of when spyware is mentioned. They closely monitor different aspects of user behavior and transmits the data to a third party. Spybots are different from a normal key logger in the sense that it contains some sort of reasoning about what to collect. This could be the characters typed into secret fields of a Web form, address book entries, a list of visited URLs or any other data found on the host computer.

A spybot could be installed as some form of helper object to existing applications (such as a BHO or a modification of an existing DLL) or as an application of its own that is launched as the OS boots [14].

2.2 Who Uses Spyware?

Why does spyware exist? Who sees any purpose in using it? The obvious answer to this might be thieves who want to steal sensitive information for financial reasons; such as credit card information, safe passwords etc. However, many of the spyware users are common people spying on someone close to them. Spyware can be divided into several categories [1] but the major ones are:

2.2.1 Personal Espionage

The primary use for a common key logger is, surprisingly enough, to spy on a spouse. Other common areas of use are parental supervision of children to protect them from online crime and actually children spying on their parents to find out credit card information or to avoid the parental control above [1].

2.2.2 Corporate Espionage

In many work environments with strict demand for security communication monitoring is used to protect company secrets. It is however much debated whether it is ethical (or even legal) to monitor your employees or not. Some claim that the personal integrity risk outweighs the possible benefits while others think that the one who pays the salary should be able to confirm that it is well spent.

One spyware application on a key machine in a company can reveal a wealth of sensitive information, trade secrets and contacts. In spite of this, surprisingly many corporations do not take corporate data theft seriously.

2.2.3 Mass Espionage

A very common form of spyware is the non target specific one. Instead as many people as possible are targeted, often with the purpose of showing advertisements but also to gather demographical and behavioral data. One such example is described in detail in the case study below.

Although it can be argued that the directed forms of spyware are the most serious ones, maybe compromising very sensitive data, it is probably the 'mass espionage' that constitutes the overall largest nuisance. We have not found any numbers on the costs imposed by this form of spyware but it is safe to assume that maintenance, halted production, data loss or exposure etc. together make up a substantial cost.

2.3 Propagation of Spyware

In order to understand why spyware has increased so much over the last few years it is interesting to examine how it spreads to new clients. A report from the University of Washington [14] seeks to define a characteristic behavioral pattern for users who more often get their computers infected with spyware. This can be used to get an image of what methods are used for distribution of spyware.

The analysis shows that there are a few activities which especially increases the risk of getting a spyware infection. Some of the main correlations that were found between spyware infected clients were that they also frequently visit many web sites, download executable files and download peer-to-peer file-sharing software.

Visiting a lot of web sites seems to have a clear link to the degree of infection. The reason for this is assumed to be that being exposed to a lot of different web sites also makes the risk greater of encountering ones infested by malicious spyware code (like the one mentioned in the case study in chapter 3).

Downloading executable files exposes a client to a greater risk of being infected with spyware. Although many clients these days are equipped with anti-virus software and personal firewalls much of the spyware software slips through anyway because they cannot, in the same ways as with viruses and worms, distinguish spyware from legitimate software

Another factor which increases the risk of spyware infection is downloading and installing peer-to-peer file sharing software. The report [14] shows that the most popular program, Kazaa Media Desktop, has been downloaded 265 million times from the site download.com by clients all over the world. This program comes bundled with many types of spyware, all in all 12 different types have been bundled with the Kazaa software.

These behavioral patterns of users who are likely to get infected with spyware also shows us the main three ways in which spyware is spread; by malicious web sites exploiting security vulnerabilities or tricking users to download software by ways of social engineering, spyware being masked as legitimate software or distributed by way of a Trojan horse, or spyware being (legally) bundled with peer-to-peer software or other freeware software.

3 Case Study

As we saw earlier there are different types of spyware, ranging from fairly innocent cookies to application-based malware. We will now take a look at a real case where a malicious type of spyware is used to infect clients, and ultimately generate large profits for the creating company by use of dubious methods.

3.1 Background

Seismic Entertainment, an Internet marketing company controlled by former 'spam king' Sanford Wallace, was sued by the US Federal Trade Commission (FTC) in October 2004 in order to stop them from infecting consumer PCs with spyware [2]. The investigation performed prior to the suit shows in detail how the spyware is distributed, installed and executed on client machines and what actions are performed. An intricate scheme is unveiled, involving security vulnerabilities, mobs of shady affiliate companies and sheer terror. This is ultimately topped off by Seismic offering the users to buy an anti-spyware software, in order to

have all spyware removed, which they themselves installed in the first place.

3.2 Distribution Method

The Seismic spyware is distributed by use of a security flaw in Microsoft Internet Explorer where the normal security policies are circumvented. The users are lured in by advertisements on several legitimate web sites. After clicking on one of these ads, the users browsers are redirected to a site controlled by Seismic.

According to the standard policy, users are always prompted when a web site wants the client to download new software. However, exploiting a certain vulnerability in the browser code, a website could upload arbitrary executable code to the visiting users computer without prior notice [4].

The vulnerability which is exploited existed in versions 5.01, 5.5, and 6.0 of Internet Explorer, but has been addressed by Microsoft by a patch first released in November 2003 [11] and also included in several subsequent cumulative patches, including Service Pack 2 for Windows XP. The vulnerability involves cross-domain security model of Internet Explorer which among other things controls the security policy for software downloads. This vulnerability allows remote attackers to bypass zone restrictions and execute Javascript by setting the window's 'href' to the malicious Javascript, then calling execCommand("Refresh") to refresh the page [12]. In the default 'medium' security setting the user is asked whether a web site is considered to be trusted for software downloads. The user can then either authorize the download and installation of the new software or stop the process. The Seismic spyware code, however, circumvents this security policy by exploiting unpatched clients with the above described vulnerability.

3.3 Spyware Action

After the spyware software is installed and executed the default home page is altered to direct the user to another Seismic-controlled page, where a deluge of pop-up messages are presented every time a new browser was opened. These messages displayed ads from Seismics clients, some of which were of pornographic nature, generating income for Seismic.

Furthermore, the MSN search function integrated in Internet Explorer is replaced by one controlled by Seismic, through which they receive payment for each click generated by a user. Other spyware programs were installed, generating even more pop-ups, adding new tool bars and monitor and transmit user information to remote Internet sites. Trying to remove these programs has no effect since they would be re-installed the next time the computer was rebooted.

By this time the computer is so infested with spyware that normal work slows to a crawl and the machine is almost impossible to use. There are also obvious risks of crashes or lost data. To remedy this, the Seismic spyware software presents pop-ups with information about a program called *Spy Wiper*, made by a Seismic affiliate. The effect was enhanced by showing large stop sign messages saying 'If your CD-ROM drive(s) open, you desperately need to rid your system of spyware popups immediately', whereby the CD-ROM trays were ejected. For each copy of Spy Wiper sold as a result of this 'terror' Seismic received about 50% of the profits [13].

3.4 Results of the FTC suit

It is still unsure if the FTC suit will lead to the companies in this case being held responsible for their actions. While Seismic Entertainment has filed for bankruptcy, some of the other companies, such as Spy Wiper, are still active. The FTC has therefore added some of these other companies to the suit [5]. It remains to be seen if the money can be tracked from Spy Wiper and the other affiliates, and if it can be proven that they were aware of the Seismic 'marketing techniques'. Since these kinds of proceedings take a long time, and the risk of getting caught is not very high, other similar companies are free to use similar or even more refined tactics to spread spyware to computers worldwide.

4 The degree of spread

It is very hard to say exactly how many computers worldwide are infected with spyware since not many large scale studies have been performed. The earlier mentioned report from the University of Washington [14] shows that 5.1% of all hosts on the university network were infected by one or more of the four most spread spyware programs (Gator, Cydoor, SaveNow and eZula). These are all adware applications, commonly bundled with freeware software such as peer-to-peer programs, used to collect demographic information and generate a user customized profile for targeted advertisements [14].

The measurement was performed during august 2003 and by examining timestamps of messages being sent from Gator-infected computers the actual infection date could be established. This showed that the number of infected computers has grown with over 100% from one year to the next. Although this infection rate is far from the dramatic spread seen in worm distribution it shows that the problem is defiantly increasing.

5 Recommendations

The threat of having spy software installed on one's computer leading to credit card thefts or other stolen personal information causes many people to refrain from doing shopping on the Internet or freely using on-line resources. Although you can never be 100% certain that you computer is malware-free there are some easy steps one can take to minimize the risk of having one's computer infected.

IT analyst Terry Bollinger defines the real problem that spyware causes as one of trust: 'How do you construct a reasonable level of trust when your sources are not fully certified?' [7]. Bollinger reasons that in order to achieve an acceptable level of trust you must rely on several separate sources instead of just one which is often the cause. 'If you are trusting in antivirus software and firewalls alone, you're going to be sadly let down.' The most common solution is to make use of anti-spyware programs that are available for download on the net. Many of them are free of charge and can, if updated regularly, locate most of the existing spyware. The key is, though, to use several anti-spyware programs in order to make the vendors 'compete for your trust'.

We will now take a look at the three most common anti-spyware programs available today. They are all free of charge (or offer a free trial) and can be downloaded from their respecitve web sites.

5.1 Spybot Search & Destroy [10]

This is the leading free anti-spyware program at the moment and is a highly recommended tool for finding spyware. It is both fast and comprehensive finding both spyware and other types of malware. By using the updating function the program is always up to date with the latest patterns. Spybot Search & Destroy also includes an early warning function if a program is trying to modify registry entries or system files without your knowledge.

5.2 Lavasoft Ad-Aware SE Personal Edition [9]

This program is also free of charge for personal use. It is pretty slow and uses more system resources than Spybot Search & Destroy, but is also quite thorough. One downside is that some more advanced functions such as browser hijacking prevention is only available in the non-free version.

5.3 Webroot Spy Sweeper [17]

This program has the ability to work as a shield against unauthorized changes made to your startup files. The program lists different spyware components in a tree diagram and lets the user choose whether to keep, delete or quarantine the located spyware. This program is available as a free trial, but costs $30 for a one year subscription.

5.4 Becoming Spyware-aware

It is important to realize that you are not completely protected from spyware just by using the above mentioned programs, although it is a good start. We have tried to find a 'best program' winner by reading different side-by-side comparisons made by different web sites, but since results vary too much it is impossible to say which program is the best, or even the most effective. Therefore it might be wise to use one or more of these programs in combination to receive a sufficient level of protection.

The Anti-Spyware information webpage SpywareGuide.com has put together a 10-step list of how to monitor one's system and check for the signs of spy software [18]:

1. *Work environment.* Assume you are being monitored. Most workplaces have the right to do this so by default get used to the fact that someone is monitoring you. There are several ways employers can monitor employees. Some use activity logging software to see what programs are being accessed and for how long. Naturally many will use spy software programs also known as *snoop ware* or a key logger to take snapshots and log all keystrokes. An employer may actually monitor internet traffic as it moves across an intranet.

2. *Anti-Spy programs.* A popular way to find out if someone is spying on you. Anti-Spy programs look for signatures or traces that are specific to certain spy software. Some simply do text string scanning to find them, and others actually extract and attempt to remove the spyware.

3. *System resources.* Poorly written spy software will almost always put a drag on system resources. Watch out for poor system resources, running out of memory, lots of hard disk activity or a screen that flickers.

4. *Machine access.* Watch for people trying to gain access to your machine. Many software programs that are designed for spying require physical access to the target machine.

5. *Installation monitors.* Currently on the market are software programs that will log every installation that occurs on your machine. It is best to leave these hidden on the system. It is possible to catch the installation of many spies in this way.

6. *Anti-virus*. Many anti-virus programs can catch prolific spy software because they are often classified as *Trojan Horses*. Keep anti-virus software up to date and make sure it is running in the background.

7. *Personal firewall.* In today's treacherous Internet it is very helpful to also run a personal firewall. Firewalls will alert you to both inbound and outbound activity. You can control what is allowed in and out of your system. Watch for suspicious programs you do not recognize trying to send data out of your system.

8. *Smart downloading.* Simply use common sense when downloading and avoid sources you cannot trust. If you are someone who frequents *warez* or *crack* sites you will more than likely encounter a Trojan or virus.

9. *Common sense.* Be careful about what you install on your system. Do not run e-mail attachments and read the EULA (end user license agreement).

10. *Spy software.* Ironically you can monitor for spy software by installing spy software on your system first! Since spy software can record all keystrokes it can monitor and record the installation of another spy software.

As mentioned in this list the anti-spyware programs is just a part of protecting oneself of spyware infection. It is also important to be observant of unusual behavior when performing common tasks with one's computer. To understand that what you do on the internet might be monitored is an important step to becoming spyware-aware.

6 Conclusions

In this paper we have tried to shed some light on the topic of spyware, what it is, its consequences and what can be done to protect oneself from being infected. As we have seen, the definition of *spyware* allows for many different types of 'severity classes', ranging from web cookies on one end of the scale to key loggers and browser hijackers on the other. Spyware also has various areas of use, both as legal monitoring applications and illegal tools for information theft. Our answer to the question 'what is spyware?' must therefore be quite broad; it is any piece of software that, with or without expressed user consent, monitors computer activities and lets this information be known to a third party.

We have also seen that the method of distribution can vary greatly. In our case study we saw that spyware was distributed by exploiting security vulnerabilities in installed software. A much more common way of distribution is the software bundle in which spyware is included together with peer-to-peer software or other freeware. A conclusion one can draw from this is that you, as a computer user, have to be careful not only keeping your software up to date with patches, but also being restrictive with what software bundles you download and to keep anti-spyware installed and updated.

Another conclusion that we draw from this study is that spyware is rapidly becoming a factor to take into account when considering safety on the internet in general. Since so many Internet-connected computers are infected with various types of spyware today, and studies indicate that the number of infected computers is growing, this is a becoming a serious problem. On the other hand information about spyware and its effects is not something the average user knows about.

If we try to make a guess of how the spyware situation will look in five years from now, we predict that spyware will both be a larger problem than it is today, but also that users will be more knowledgeable about the situation and that there will be more tools on the market to fight spyware. Microsoft has recently taken an interest in the spyware problem and is now, by acquisition of the anti-spyware firm Giant Company Software, developing an anti-spyware software of their own [16]. If anti-spyware software is included in the next generation Windows operating system, like the Windows personal firewall was in Windows XP Service Pack 2, this will probably lead to a great increase in the use of anti-spyware software by people who are not aware of the problem today.

References

[1] Porter A. A day in the life of spies - spyware everywhere. *http://www.spywareguide.com/*, 2005.

[2] Buckley C. Us government targets spyware. *Electric News Network, http://www.electricnews.net/news.html?code=9558620*, October 2004.

[3] Dino Esposito. Browser helper objects: The browser the way you want it. *http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnwebgen/html/bho.asp*, January 1999.

[4] FTC. Ftc memorandum in support of a temporary restraining order against seismic entertainment. *http://www.ftc.gov/os/caselist/0423142/041012memo0423142.pdf*.

[5] FTC. Ftc memorandum in support of motion to name additional defendants. *http://www.cdt.org/privacy/spyware/20050401ftc.pdf*, April 2005.

[6] Lawton G. Invasive software, who's inside your computer. *Computer*, 35(7):15–18, July 2002.

[7] Bollinger T. Harrison W. User conficence - and the software developer. *Software, IEEE*, 21(6):5–8, November 2004.

[8] http://www.spywareinfo.com/. Bho's - browser helper objects. *http://www.spywareinfo.com/articles/bho/*, April 2005.

[9] Lavasoft. *http://www.lavasoft.de/*, May 2005.

[10] Patrick M. Safer networking. *http://www.safer-networking.org/*, May 2005.

[11] Microsoft. Microsoft security bulletin ms03-048. *http://www.microsoft.com/technet/security/bulletin/ms03-048.mspx*, November 2003.

[12] mitre.org. Cve - common vulnerabilities and exposures. *http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0814*, August 2003.

[13] Stern R.H. Ftc cracks down on spyware and pc hijacking, but not true lies. *IEEE Micro*, 25(1):6–7, 100–101, January 2005.

[14] Levy H.M. Saroiu S., Gribble S.D. Measurement and analysis of spyware in a university environment. *Proceedings of the First Symposium on Networked Systems Design and Implementation (NSDI '04), San Francisco, CA*, March 2004.

[15] techtarget.com. What is malware, and what are the most common types? *http://searchsmb.techtarget.com/sDefinition/0,,sid44_gci991471,00.html*, April 2005.

[16] theregister.co.uk. Microsoft buys anti-spyware firm giant. *http://www.theregister.co.uk/2004/12/16/ms_fights_spyware/*, December 2004.

[17] Inc. Webroot Software. *http://www.webroot.com/products/spysweeper/*, May 2005.

[18] LLC Xblock Systems. How to detect spies. *http://www.spywareguide.com/txt_detect.html*, May 2005.