

~ COLORADO TECHNICAL UNIVERSITY ~

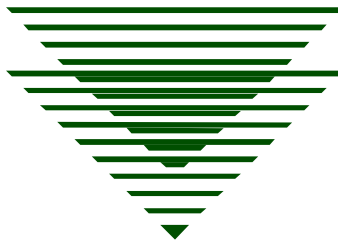
Certification and Accreditation

The Corporate Spyware Problem

**Professor Karl Seifert
Submitted in Partial Fulfillment of the Requirements for
CS-662
Information Systems Security**

By

**William P. Flinn
Fort Collins, Colorado
December, 2005**



Hypothesis

Spyware presents a problem for more than just individuals and individual computers. The spyware problem can have far reaching effects on corporate computer and network performance. Spyware also presents a challenge to employee productivity and the ability of a company to maintain its compliance with the various regulations governing the industry segment to which that company belongs. Spyware enters from a variety of sources. It takes a variety of tools and methodologies to combat spyware, including technical solutions and employees exhibiting personal awareness.

The Corporate Spyware Problem

Of the many types of threats that are present in the world of information technology, one that is getting a great deal of mention and attention lately is the problem of “spyware.” Actually, spyware is just part of what is coming to be known as a larger problem in general with malicious software, or “malware.” Regardless of definition of what actually constitutes spyware, it has presented itself as a real and significant problem for individuals, and especially for enterprise systems. While individuals may only have to worry about how spyware affects their own computer, enterprise system administrators have to worry about the various performance degradations, data theft, threats to regulatory compliance, risk definition, and other issues associated with dealing with and fighting this type of threat.

The purpose of this paper is to discuss the definitions of spyware, whether it is commonly encountered in adware that a user willingly installs, or enters a computer system without a user or system administrator’s knowledge. The effects of spyware, once on the system, will be discussed with regard to spyware’s effects on degradations of system performance, effects on a system’s ability to meet regulatory compliance, resources spent to combat the problem, and staff hours spent on spyware eradication and control. Some ways that spyware is being dealt with will be discussed as well.

Significant Background

Even before computers were routinely connected to the Internet, various threats, such as viruses and theft of data existed. It’s just that these threats were typically much slower in spreading and typically relied on someone physically touching the computer for the attack to take place. Viruses, for instance, were usually installed onto a computer by an unsuspecting user inserting a floppy disk that had previously been used in an infected machine. In order to steal

electronic data from a computer, someone had to physically be there to copy the files onto a floppy disk.

Since the increase in the ability of businesses and individuals to connect to the Internet, things such as email and online information gathering have become ubiquitous and routine. Likewise, the use of the Internet to spread virus attacks had become common as well. Virus attacks lead to attacks which compromise computers for the purpose of destroying data, causing an interruption to normal business use, or taking over the machine for use by others. All of these things are happening against the user's knowledge or permission. As these threats continued to evolve, other types of invasions became common. Many businesses found that they could advertise over the Internet for little or no cost, and could do so to large numbers of people very quickly. In fact, many of the costs were typically born by the end user who became victims of business with less than legitimate practices, resorting to aggressive online advertising tactics, including the use of software tools that proliferated advertising measures. The end users are the ones that suffer from performance problems and time spent deleting many useless emails and clicking out of numerous pop-up windows.

Enter the terms "spyware," "adware," and "malware," all and any of which refer to the types of programs that exist on an end-user's system and do not enhance that user's ability to perform the normal business functions that their job requires. There are types of adware or even spyware that appear as browser tool bars which could enhance a user's web experience, but often hidden underneath is a spyware type program meant to gather data against the user's will and without permission. This type of threat is clearly still evolving, and much will likely be discussed about spyware in the foreseeable future.

What is Spyware?

Depending on who is asked about what they think spyware really is, various definitions or perceptions will arise. To some, the meaning of spyware is any type of software installed on a computer that will steal personal information and send it to an unknown web site or email address without the user's knowledge, leading to a common type of identity theft. Still others term spyware as those types of software that use stealth methods to capture information such as login accounts and passwords for the purpose of later compromising or attacking systems. And still others term spyware under a more generic definition to include adware, which refers to applications that deliver advertisements and annoying pop-ups to the user's desktop. The perception under this definition is that adware is necessarily spyware because in addition to delivering advertisements, it may also be performing the harvesting and delivery of other personal or system information to places outside the user's computer and network to an unknown location, and without the user's permission.

The common ground in these various definitions is that spyware (and adware) often cause problems in computer systems. What most often separates spyware from adware is the definition that spyware is on the computer without the user's knowledge. In fact, an article by Ann Saita includes the following definition of spyware in this way: *"Strictly speaking, spyware is an application or process on the PC that tracks Internet usage and then uploads that information to a server somewhere, usually without the information or consent of that user."* (Saita, 2005, pg. 2). In an article by Aaron Hackworth, there is the notion that on a multi-user computer, one user willingly installs a piece of adware, being willing to put up with the advertising, for some desired function. Another user who shares that same multi-user computer then comes along, and is subject to whatever side effects that the adware causes, including the harvesting of Internet usage

data. All this is happening without the second (and subsequent users') knowledge or permission (Hackworth, 2005, pg 2).

In some instances the problems are as innocuous as popup ads and large amounts of advertisements. In yet other cases, the problems are more sinister, including harvesting and outright theft of information including passwords, credit card information, or other personal information. Also, depending on who is giving definitions or opinions on what is and isn't spyware, some will say that the defining line is in the fact that many types of spyware are put on the computer completely without anyone's knowledge, while adware is purposely placed on the computer and even comes with an end user licensing agreement (EULA), an example that will be discussed in the next section. As will be discussed further in this paper, having extremely long and verbose EULAs is one method that spyware (adware?) authors use to "hide in plain site" as it were, and get their products onto computers by relying on the fact that the typical user doesn't care to read this enormously long document.

How Does Spyware Get In?

There are various common methods that spyware and adware use to infect a computer system. One such common, yet preventable method is the ability of spyware types of programs to enter a computer system through holes in an un-patched operating system or other un-patched software (Webroot, 2005, pg. 4). As has been known for quite some time, it is imperative that computer users routinely patch their systems, applying critical and security updates to their operating systems and installed software. As many recent threats rely on a user to visit a certain web site or open an email attachment in order to become infected, patching the system will provide a high level of mitigation and protection against this type of threat.

Another very common method for spyware infection comes from the social engineering aspect of computer use. Users are lured into visiting a particular web site or opening an email attachment (Shavlik, 2005, pg. 3). The ability to lure users to open an email or visit a web site is not a very difficult undertaking, as emails can easily be disguised as a message from a trusted friend or relative, and malicious Internet links can easily be disguised on legitimate business or banking links. Some users willingly trust these links and are taken to a web site containing the spyware and are easily infected. As mentioned above, a great deal of infections are mitigated simply by keeping patches up to date, but since spyware and malware tactics are evolving rapidly, some are able to get in because a patch does not yet exist to prevent it.

According to FaceTime Communications, Inc., a type of software type referred to as “greynet” is installed because a user trusts the application to perform a legitimate function. This type of software is particularly challenging because users often install this software without the IT department’s knowledge or permission (FaceTime, 2005, pg. 4). Besides being a spyware type of application, this type of software often leads to some of the network performance problems discussed later in this paper. An example of greynet applications are such things as the popular Skype voice over IP/instant messaging/P2P application. This software is manufactured by the same originators of the KaZaa music sharing program, the peer-to-peer application that gained notoriety for a variety of reasons, including allegations that the software was tampering with system files, such as placing entries into the HOSTS file on a computer to redirect traffic to certain locations on the Internet (Healan, 2003, ¶1-2). Greynets are discussed here because FaceTime Communications, Inc., in their whitepaper, describes this type of application as using various techniques to avoid detection by network security tools.

As previously mentioned, adware programs can indeed be included in the same category as spyware. There are two essential issues with adware that are being commonly discussed. First is the fact that adware, in many cases, is willingly installed as legitimate software. A user downloads and installs the adware because they are willing to put up with a certain amount of advertising in order to enjoy the features that the program offers. As part of the software installation process, users are typically required to read and accept an end user's licensing agreement (EULA). Here then is one of the less than ethical techniques used by adware companies to ensure that their software is installed. By making an EULA that is so long and cumbersome to read, the typical end user will get bored or frustrated, not want to read the entire EULA, and simply install the software. In one instance, an EULA of one of these programs was said to have taken 131 online screen page-down commands to get through the entire document (FaceTime, 2005, pg. 8). To add to the seemingly unethical nature of these EULAs, besides being extremely lengthy, is the contents of the EULA, including such things as prohibiting a user from using packet sniffers or other devices to intercept the adware (spyware?) traffic once installed (FaceTime, 2005, pg. 8). Another issue being discussed along the lines of adware that is willingly installed, is that of the issue of its installation on a multi-user computer. One user obtains the software, agrees to the EULA, and uses the software. Another user of that same computer comes along, not knowing that the software was even installed, therefore not necessarily agreeing to the EULA (Hackworth, 2005, pg. 2). This brings up the question of whether or not this represents an installation of spyware, according to the definitions given earlier in this paper. It is commonly held that adware often contains hidden "features" that harvest and deliver data, albeit that it may be something as innocuous as data about web browsing habits.

Effects of Spyware on The Corporate Network

There are a number of effects that spyware has on the corporate network and computing environment. One of the most notable is the effect it has on performance. In one survey, 71% of companies reported that the biggest effect to their network and computer systems that was caused by spyware was poor (“sluggish”) system performance and computer crashes (Saita, 2005, pg. 2). The same article mentioned that employees complained of system crashes and having to deal with an extremely high number of pop-ups. This is alarming in that this indicates that spyware alone has a major effect on computer performance. This directly relates to a high level of lost production. In general, a huge problem caused by spyware is that it consumes system resources, user time, and network bandwidth (Hackworth, 2005,pg. 6).

Regulation compliance was mentioned as being greatly threatened by spyware on corporate systems. Types of spyware such as key loggers and backdoors compromise financial security and lead to increased risk (Shavlik, 2005, pg. 2). Specifically, a credit card company’s database that is compromised puts the company in violation of Gramm-Leach-Bliley compliance. If hospital insurance records are compromised, then HIPAA compliance is in jeopardy. Clearly, spyware has the ability to steal and send sensitive data without the user’s (or company’s) knowledge. If the information or data is any of the types mentioned above, then major compliance issues come into play, not only with GLB and HIPAA, but with other compliance such as Sarbanes-Oxley, and if a federal government system, then federal regulations are involved. One article put it quite succinctly: *“If the integrity of a user’s PC can’t be trusted, compliance with any form of privacy or data protection legislation is out the window”* (FaceTime, 2005, pg. 6).

Resources and money spent to deal with the problem are another notable issue. For instance, it was reported by Dell Computers that twelve percent of its customer's support requests were caused by spyware (Webroot, 2005, Pg. 3). Staff hours needed to eradicate spyware amounts to a large dedication of resources. One major HMO – an organization clearly worried about HIPAA compliance – has a staff of ten people who's sole purpose is to eradicate spyware (Webroot, 2005, pg. 3). These are just a few examples of how companies are finding that they have to dedicate staff and monetary resources to fight this problem. Add to that the cost of purchasing multiple tools and software packages to find and eradicate spyware on computer systems, and the total cost of this problem is very high.

How to Combat the Threat

Combating spyware is a two-edge sword, so to speak. On one hand, the spyware itself causes a rather large problem from a security and performance point of view. On the other hand, tools to combat spyware represent yet another set of applications that have to be installed onto a computer. This software then has to run in the background to monitor the computer and fight any problems caused by recognized spyware that come up. These additional applications represent yet another set of code that consumes the computer's resources (memory and processor) or requires additional resources on a central server if a centrally managed enterprise tool is used.

Technical solutions to combat spyware seem to be encountering an endless cycle where a particular tool is implemented to block or remove the spyware, the spyware is improved to counteract the solution, then the solution is improved to counteract the spyware improvements. This is because there is evidently enough financial or other motivation to make the continuing development of spyware worthwhile (Hackworth, 2005, pg. 1). Another difficulty with technical

solutions is that although spyware is often grouped into the same category as viruses, using traditional antivirus solutions to combat spyware offers an incomplete fix (FaceTime, 2005, pg. 12). The use of patching as a type of technical solution against spyware seems to be an effective preventive measure against spyware that attacks flaws in program code, while individual anti-spyware programs seem to be effective when used together, but limited in what they are able to detect and fix individually. That is to say that one product will find and fix certain spyware applications, while it takes another to find other pieces of spyware, and then possibly a third and subsequent anti-spyware products to catch what is left over.

Beyond technical countermeasures, the most effective means of preventing spyware attacks may very well rest on the shoulders of the end-user. Humans, after all, are the ones that visit questionable websites, open email attachments, and install software on their computers without questioning the software's legitimacy or reading the EULAs. There may be a variety of reasons why people are so complacent about computer security, ranging from complete apathy to simply being part of a "security unaware" culture. Regardless of the reasons for user induced spyware attacks, computer security awareness training and an ongoing security "aware" environment will help mitigate many of these spyware problems. Beyond that, an aggressive system of patching, antivirus measures, anti-spyware tools, and other external security measures (firewalls, etc) will help reduce the instances of spyware problems.

Conclusion

Spyware in the corporate environment is causing a number of very serious problems. To begin with, spyware is having an extremely negative effect on computer and network performance. Spyware activities take up computer resources and network bandwidth. The constant barrage of pop-ups and browser redirections cause computers to crash and behave

sluggishly. This in turn leads to a serious reduction in employee performance and productivity. Spyware infections also have the potential to lead to serious legal and regulation compliance problems. Health care companies and hospitals risk falling out of HIPAA compliance, while financial companies risk their GLB and Sarbanes-Oxley compliance.

The solution to this problem is not simply one of implementing technical mitigations. Antivirus, anti-spyware tools and patching can only do so much. End users must take on some of the responsibility of preventing their own activities from contributing to the spyware problems on their computers. Spyware infections on their machines directly affect the overall health and security of the corporate network that they are attached to as well. While network administrators can take care of making sure that proper patching and antivirus updates are taking place regularly, it is up to the user to be careful about things such as opening email attachments, visiting suspicious web sites, and installing software without reading EULAs. In fact users should question whether or not installing any software obtained from the Internet in general is an acceptable or authorized corporate practice. Companies can provide some measure of awareness of this issue by having an up to date acceptable use policy in place. Spyware is presenting a real and present danger to corporate computing and network systems. Appropriate measures must be taken on all fronts to combat its effects.

References

FaceTime, 2005, Whitepaper: *Spyware Prevention: Effective Network Protection Through Defense in Depth*, FaceTime Communications, Inc.

Hackworth, Aaron, (2005), *Spyware*, CERT Coordination Center, Carnegie Mellon University.

Healan, Mike, 2003, "KaZaa Tampers With System Files," Downloaded from <http://www.spywareinfo.com/articles/kazaa/> on December 14, 2005.

Saita, Ann, (2005), *Spyware Survey: Coming to terms with the problem*, SearchSecurity.com, Downloaded from http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci1131072,00.html on December 1, 2005.

Shavlik, Inc, 2005, Whitepaper, *Spyware and Patch Management: An Integrated Approach to Network Security*, August, 2005, Downloaded from <http://www.shavlik.com> on December 1, 2005.

Webroot, Inc., 2005, *Spyware: IT Strategy Guide*, Infoworld, Infoworld Media Group.