Global Information Assurance Certification Paper

Spyware: Installation, Removal, and Prevention

GIAC Security Essentials
Certification (GSEC)
Practical Assignment
Version 1.4c

Option 1 - Research on Topics
in Information Security

SANS East, Washington, D.C., December, 2004

Submitted by: Britt Fleming
January 26, 2005

A corporate Help Desk specialist receives a call from an unhappy user: The user's machine slowed down to a crawl, before finally "freezing up". The cause? Spyware. Now, multiply this scenario by the thousands every day. "Houston, we have a problem." This paper examines what spyware is, how it becomes part of the Windows PC environment, and why it is so destructive. A study of the process of removing spyware follows, with emphasis on providing a methodology that will enable specialists (or any determined user) to return infected machines to service as quickly as possible. Finally, options for prevention are explored, ranging from technical solutions to legal action.

Table of Contents

List of Figures

Abstract/Summary

A corporate Help Desk specialist receives a call from an unhappy user: The user's machine slowed down to a crawl, before finally "freezing up". The cause? Spyware. Now, multiply this scenario by the thousands every day. "Houston, we have a problem." This paper examines what spyware is, how it becomes part of the Windows PC environment, and why it is so destructive. A study of the process of removing spyware follows, with emphasis on providing a methodology that will enable specialists (or any determined user) to return infected machines to service as quickly as possible. Finally, options for prevention are explored, ranging from technical solutions to legal action.

Introduction

Spyware is a major threat to information security. Once installed on desktop and laptop computers, it robs machines of valuable bandwidth and processing power by gathering user information, generating pop-up advertisements and maintaining connections to external web servers. In order to minimize this threat, it must be removed from infected systems and measures must be taken to prevent re-infection. The large number of hours expended by IT departments to remove spyware is in itself a significant resource drain. Spyware is also known as adware, with the difference being that it actually collects user data and sends it back to a server for analysis. It should also be noted that Spyware thrives in the realm of Microsoft desktop operating systems, namely Windows 98/2000/Me/XP, by virtue of being the dominant operating system in the world today.

Spyware is clearly a form of malware that has been modified to support seemingly legitimate (but questionable) business objectives. Whether downloaded by user selection or injected into the unknowing user's files by an ActiveX control, the undesirable code has considerable value as an advertising or marketing agent to those who developed it. With this in mind, let us begin our analysis of the spyware installation process with the computer user.

Spyware Installation

How is spyware installed on the computer in the first place? Understanding this is critical to performing spyware removal and prevention. Software cannot be installed without being downloaded from the internet or a disk and without running an installation program. This may be done with or without your permission or knowledge. Spyware developers have taken advantage of a so-

called gray area in which the user consents to downloading and installing software by acknowledging, via mouse click, that the EULA (End-User License

Agreement) has been read and agreed upon, even though the user may not in fact have read the text in full. This installation tactic is pure social engineering. The question here is whether or not the user was duly aware of what he or she was downloading and installing and is subject to debate. Even if the user has read the EULA in its entirety and consents to the provisions contained within, has it been made clear that the installed program will, in turn, download and install additional iterations of commercial software? Is the user aware that multiple advertising banners may be displayed in a manner that interferes with casual web browsing, regardless of which site is visited? Perhaps, once spyware has been installed, the user has noticed a significant slowdown in the performance of the computer or that the banners become so prevalent at times so as to require a reboot in order to resume operation. In this case, is the user at fault for being unknowledgeable, or is the spyware source guilty of misrepresentation and trickery? Regardless of the user's skill-level or intentions, it is a fact that no one wants their computer to be unusable; and this is the condition we're trying to avoid.

Spyware is often installed along with freeware, which requires the user's consent via a EULA. It can also be downloaded by clicking on an enticing offer on a web site, which may or may not require a EULA. In some cases, it is hard to determine how the spyware was downloaded in the first place. A particularly sophisticated example of spyware is midADdle. Assuming it is downloaded in a freeware package, such as an Instant Messaging program, midADdle installs itself as a resident program within the Windows OS, complete with registry entries. One can assume that the user is asked to read and acknowledge a EULA before allowing installation to begin. The principal component of the midADdle program is a Trojan downloader, which carries as its main payload a Browser Helper Object (BHO).[1] A BHO is an ActiveX Control that serves to control Internet Explorer browser actions (The Google toolbar is a good example of a legitimate BHO).[2] Once the Trojan is downloaded and installed, files are written into the registry; and the BHO is embedded in the browser. MidADdle begins at once to track keywords in web sites selected by the user. Keywords are sent to a database, matched against promotional keywords (supplied by paying advertisers), and the browser is directed to a midADdle web site. At this point, "interstitial" web pages (meaning they are displayed in-between web sites viewed by the user) containing advertisements containing subject matter that coincides with the keywords collected from the user are displayed. After 10 seconds, or if a Continue button is selected, the original web site is displayed; and the user temporarily regains control.

As midADdle collects more data on the user, the database grows and more ads are displayed for marketing customers. The spyware developer is paid by the advertisers according to CPM, or Counts Per Mille, which means counts per thousand. Every time an interstitial is displayed to a user, a fractional amount is logged and billed to the customer. This means if each "hit," or interstitial display, is worth .05, then a thousand hits will earn the developer $50. It follows that

web sites sponsoring midADdle, as well as the midADdle developers themselves, would benefit greatly by spawning the program on every machine possible and by displaying as many interstitial ads as possible.

The midADdle developer maintains that this is equivalent to the experience of viewing commercials in between television shows.[3] In fact, the interstitials appear between web sites that have not paid for them; and the user neither wants nor expects them. Television advertisements are always presented by sponsors of the program being viewed in conjunction with the ad. The comparison also falls flat in other ways. Television ads have never compromised the functionality of a television, nor have they pre-empted or prevented television programming. Furthermore, because television bandwidth is considered property, any attempt to broadcast without permission is illegal. The television and radio economy is highly regulated by the FCC, has been for many years, and bears little resemblance to what is occurring on the internet.

The intentions of the midADdle vendor and sponsors are quite clear. One need only look at the vendor's web site.[4] This site also promotes the spyware with a step-by-step demonstration of how it works. Further investigation shows a number of web sites that support the spyware development community. Here you find reviews and trade tips on the latest software and techniques in web marketing and on spyware and adware in particular.[5]

Of course, there are many, many more species of spyware roaming at large in the web jungle. They may even be categorized by function. The reason I selected midADdle as an example, however, is because it is a fairly recent variation of programs that incorporate a Trojan with a BHO payload. It is also a particularly disruptive and stubborn parasite and manages to reappear even after being uninstalled using the Add/Remove option in the Windows control panel. With these factors in mind, we will begin to examine ways to identify and permanently delete spyware from an infected system.

Spyware Removal

The most obvious symptoms of spyware infection are a profusion of browser pop-up ads, sluggish internet connections, and degraded processor performance. The processor performance is impacted due to the collection of data on the user's machine. When the data is sent to a spyware server, it uses up valuable bandwidth, causing the speed of the internet connection to seem sluggish. Once it is analyzed by the spyware server for marketing value, in accordance with the marketing rules requested by the sponsor, pop-up ads are generated on the user's machine, causing even more bandwidth and processing power to be consumed.

There are a few other possible causes of these types of symptoms besides spyware. Try to make a reasonable determination of the cause before assuming the problem is spyware, based on connectivity data, the condition and age of the machine, user behavior, and related issues. For instance, is the sluggishness of Internet Explorer actually being caused by a network slowdown? Is the user's hard drive full, or on the verge of crashing? Is the machine running multiple sessions of spreadsheets and databases with huge file sizes and simply needs a RAM upgrade? This is not to say that a computer might not have these problems along with that of spyware, but is always good practice to make sure other possibilities have not been overlooked.

There is, however, an easier way to identify a possible spyware problem on a desktop or laptop if they are connected to a managed network domain. Several vendors offer web content management applications that perform a variety of functions. One of these, Websense, in addition to blocking objectionable and unproductive web surfing, will also produce a report identifying the number of internet connections made to external servers by each machine. A large number of hits may indicate an infestation on the machine, as the spyware agents make numerous connections to the spyware servers. By starting with the machines with the most hits, you can eliminate your biggest spyware problems in the domain. In cases where content filters are not a practical choice or they fail to locate spyware-infected computers across multiple types of network connections, it may be necessary to examine machines on a case-by-case basis.

Whether removing spyware from a Windows machine at home or on a domain, one of the first requirements is to ensure critical updates have been downloaded and installed. Some spyware is based on well-known exploits; if these security vulnerabilities are closed, then those variants are kept at bay. Some of these exploits focus in particular on Internet Explorer and ActiveX Controls, which is the environment in which most spyware operates. For Windows XP, installation of Service Pack 2 takes care of much of the required patching, as well as providing a client firewall and added security features for Internet Explorer. Timely and thorough system patching is essential to security in any case, due to the many other possible threats besides spyware.

Also, it is important that effective and updated anti-virus software has been installed. Since many of the spyware programs are variants or hybrids of Trojans and other malware which previously had no commercial value, a good anti-virus program will usually recognize and eradicate them. Make sure the latest signature file in installed, as it may contain data to locate a newly concocted form of spyware. A full anti-virus scan may be in order if there is, in fact, a chance of a virus or worm infestation.

Once you have verified that all critical updates have been installed and that effective anti-virus software has been installed with the most recent signatures,

there are a series of steps that should be taken to ensure all spyware is removed from the machine. The first of these steps is installation and execution of a spyware removal application.

Of the many anti-spyware applications currently being offered, a few of them have proven to be the most effective and up-to-date. Two that see a great deal of use are AdAware, by Lavasoft, and SpyBot, by Safer Networking Limited. Using these applications in tandem will identify and eliminate the majority of spyware on any Windows machine. Please note, however, that AdAware offers a licensed version and a version for personal use. The personal use version is free and should not be used for corporate purposes. SpyBot is freeware but a donation is requested. Also, a promising entry into the anti-spyware field is the new Microsoft AntiSpyware. When installed on a thoroughly infected computer, it was able to remove all spyware files, plus provided the option of restoring a hijacked browser to the original settings. Although currently available in beta for download at no cost, it remains to be seen how Microsoft will incorporate this application into its product offerings.

On a corporate scale, an important feature to look for is enterprise deployment and management for anti-spyware applications. Some of the firms now offering centralized anti-spyware management are Computer Associates, Finjan, Websense, and McAfee.[6] Shavlik is scheduled to release NetChk Spyware in the second quarter of 2005.[7] When we look at the number of major players entering the enterprise anti-spyware market, it shouldn't be surprising if Microsoft does the same.

Anti-spyware programs work by scanning the registry and other files against a signature of spyware files compiled by the program developer, similar to the way anti-virus applications work. Depending on whether or not the spyware has been identified and added to the most recent signature, the application will locate spyware files and mark them for deletion. The user may then review the selections to ensure they are valid and delete them. It is important to always check for anti-spyware updates and download them prior to running a scan.

NOTE: Of the large number of spyware applications offered, there are a number of them that actually install spyware on the machine. If you're not sure about the legitimacy of an application, consult the list provided at the Spyware Warrior web site. [8] It is also a good precaution to read the EULA before continuing with the program installation. Examination of the license agreements for Spybot, AdAware, and Microsoft Anti-Spyware indicates that these applications are strictly spyware removal tools, with no other programs included, and no gathering of personal data.

Taking into consideration the rapidity which with new variants of spyware are being created and disseminated, it is entirely possible, if not probable, that running scans with multiple anti-spyware applications will not locate all of the

undesirable files. Further steps are necessary to ensure total eradication of the threat. Also, AdAware (and others) may indicate that some files were missed; and the option is given to remove them on reboot. If the file paths are displayed, take note of them, as they may need to be removed manually. If the application enables log files to be viewed and saved, these may also be of value. As stated previously, an understanding of how spyware becomes resident on the machine is critical to removing all spyware. Analysis of log files may be required to locate and delete spyware files. The following AdAware log file records the deleted and quarantined midADdle files:

```
MIDADDLE
»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»»
obj[0]=Process : C:\documents and settings\user\local settings\temp\9MGJC.exe
obj[6]=Regkey : typelib\{ecb25a48-e6e0-49af-99af-07c763e31389}
obj[7]=Regkey : appid\searchhelp.dll
obj[8]=RegValue : appid\searchhelp.dll "AppID"
obj[9]=Regkey : typelib\{ecb25a48-e6e0-49af-99af-07c763e31389}\1.0
obj[10]=RegValue : typelib\{ecb25a48-e6e0-49af-99af-07c763e31389}\1.0 ""
obj[11]=Regkey : interface\{e318d698-27b3-44d5-8998-c35eafb9c034}
obj[12]=RegValue : interface\{e318d698-27b3-44d5-8998-c35eafb9c034} ""
obj[14]=RegData : appid ""
obj[15]=RegValue : software\microsoft\internet explorer\main "Updater"
```

The log file clearly shows where spyware files were installed in the directory and the registry. Even though AdAware eliminated the midADle problem, the quarantine log may still prove to be useful in the future, especially in the case of a persistent parasite like this. In cases where future variants can not be located easily, log files like the one shown above would be prove to be valuable resources. It may also be used as a pointer to a specific user's proclivity for downloading spyware.

In some cases, the items that can not be deleted are Browser Helper Objects. There is an excellent tool available for download, designed to locate all BHOs on a machine, called BHODemon. It also provides the option of disabling the BHO. If anti-spyware software did not find and delete all spyware, BHODemon will often provide the final death blow. It can be downloaded from the Definitive Solution, Inc. web site. [9]

Depending on the degree of infestation and the type of spyware variants, removal steps may need to be performed in a different sequence, different tools may need to be used, or drastic measures may need to be taken. Since total reformatting of the hard drive and reinstallation of the OS can destroy important user data, not to mention that it can be a lengthy process, it is assumed that it would be possible for a trained analyst to accomplish the removal task in a much shorter period of time, using the knowledge and procedures presented in this document. Many of these procedures are also good practices to follow for the general health of the machine.

Because the anti-spyware removal tools may not have detected all undesirable files, it follows that the files will need to be manually identified and removed.

Manual Removal of Spyware Files

1. *Delete unused profiles*. Using Explore in Windows, locate and open Documents and Settings. A logon profile folder will exist for each user who has logged on. Delete any profiles that are no longer in use.

2. *Delete Temp files*. Next, open the folder for the primary user profile, so that Local Settings is displayed. If Local Settings is not displayed, with My Computers open, open Tools, Folder Options, and Select the View tab. Under Advanced Settings, ensure the first six boxes are checked. Also make sure "Show Hidden Files and Folders" is selected under the Hidden Files and Folders header and that "Hide Extensions for known file types" is not selected. Select Apply to All Folders and click OK. All applicable files and folders will now be displayed.

   Look for the Temp and Temporary Internet Files under Local Settings. Open Temp, select all files, and delete them. The Temp folder is a familiar hideout for spyware files, as indicated by the AdAware file logging discovery and termination of midADdle, seen below:

   midADdle Object Recognized!
   Type : Process
   Data : 9MGJC.exe
   Category : Malware
   Comment : (CSI MATCH)
   Object : C:\documents and settings\user\local settings\temp\

   Warning! midADdle Object found in memory(C:\documents and settings\user\local settings\temp\9MGJC.exe)

   "C:\documents and settings\user\local settings\temp\9MGJC.exe"Process terminated successfully

   Note that the midADle process 9MGJC.exe was located in the Temp folder of the primary user's profile, showing how important it is to delete files in this folder during the spyware removal process.

   Occasionally, you may receive an error message that the file cannot be deleted because it is in use. Make sure all applications are closed. It is possible that you are not able to delete a file because it is a spyware executable running a process. If this is the case, make note of it and move on.

3. *Delete Temporary Internet Files*. Open the Temporary Internet Files folder and delete everything. These files are also referred to as the IE cache and may be deleted within the Tools/Internet Options/General Tab, but the browser may be choked by spyware to the point where it is preferable to empty it through the file explorer. As with the Temp folder, the IE cache is also a favorite depository for many spyware files. It is possible, however, that the IE cache may be so full that it may not respond. It may be necessary to empty the IE at some later time, provided other spyware removal procedures have succeeded in significantly increasing machine performance.

4. *Use Add/Remove*. Windows also provides a means of purging the system of all files associated with an installed program, in the Add/Remove function of the Control Panel. This is often the first place many technicians go to in order to remove spyware, and many times the spyware program is listed there. In many instances, however, the Add/Remove selection fails to do what it is designed to do, either because the spyware was designed to reappear or simply remain resident after being "Removed", or because performance degradation has made it impossible for the machine to process anything other than the ongoing activities of the spyware. Nevertheless, it is necessary to attempt to remove the program using this feature. If the program can be removed with Add/Remove, without it returning to the list again, then definite progress has been made towards removing all spyware.

5. *Delete Program Files*. Sometimes removal of programs via the Add/Remove function leaves additional spyware folders and files in the Windows Program Files directory. Inspect the list of Program Files in Explorer and delete any unwanted folders. This process requires knowledge of what is supposed to be on the system. If you aren't sure, review the programs in the All Programs list and consult the user, if it's someone besides yourself. As with the Temp and Temporary Internet folders, you may receive notification that the file cannot be deleted because it is currently in use, most likely by spyware. This is a good time to look into registry editing.

6. *Edit the Registry*. In Windows, select Start, Run, key "regedit", and hit Enter.

   a) Before making any changes, save the registry file by selecting File, Export, and saving the .reg file to a safe location. Failure to do so may result in irrevocable damage to the operating system, in the event necessary files are inadvertently deleted. As with the Program Files, it is beneficial to know what belongs in the registry and what doesn't. One way of doing this is to take a snapshot of a known good system and save it for future reference. Otherwise, registry editing is an educational and somewhat risky process.

   b) The first and most important key in the registry, at least in reference to spyware removal, is HKEY_LOCAL_MACHINE\ Software\Microsoft\ Windows\

CurrentVersion\Run\. Entries in this key determine which programs are run when Windows 95/98/2000/XP is run. Examine each Registry String; some of them should be for familiar applications, such as "C:\Program Files\Common Files\Symantec Shared\ccApp.exe". This string is one of the entries for Symantec anti-virus software, which you certainly don't want to delete. On the other hand, if you notice something similar to "C:\Program Files\Common Files\H8LxP0d.exe", then strongly consider deleting it. Persistent spyware applications such as midADdle often insert files with names like skmzxlii.dll into various locations; if you see these in the registry and can ensure that they aren't valid files, delete them.

c) How do you ensure which files belong in the registry? Key, or cut and paste, the name of the file into the Google search field and look for it. A plethora of web sites are available just for the purpose of identifying registry file names.[10] Check out the file definition in several of these, until you are satisfied that you know whether or not the file is valid. You may learn that the file is a required driver, that it is a well-known variant of spyware, or that it is totally unknown. In the case of the unknown files, use your best judgment. I personally have never damaged a machine by deleting a file with a name like xzcvzxilm.exe or MyGroovyWebSearchTools.exe. In doing this, you are manually duplicating the process by which anti-spyware applications search and delete files.

d) Use the registry Find function to located known file names and delete them. Every time a file is located, use F3 to continue the search until all files are found and deleted. Within the HKEY_LOCAL_MACHINE\Software key, look for entries for spyware files previously identified in previous steps and delete them. Depending on the severity of the spyware infection, this can take some time; but the process speeds up after several drills.

7. *Boot into Safe Mode*. Now suppose, after following all of the prescribed steps, spyware continues to run on the machine? It's time to boot into Safe Mode, which in Windows XP requires you to hit F5 on boot. When Safe Mode is selected, the computer boots up with only essential drivers, which removes some of the spyware application's ability to "defend" itself. Disconnecting the system from the network (provided Safe Mode with Networking has NOT been selected) also prevents the spyware from communicating with the spyware web server, if that is what it has been doing. Removal procedures may resume as before. Another option is to boot into Safe Mode immediately upon identifying the threat. Anti-spyware and anti-virus programs work fine in Safe Mode, but the machine will need internet access to update the signatures prior to logging on to the machine independent of a network. Also, a corporate environment may necessitate logging on to machines via remote terminal using an application like Remote Desktop Connection, which comes with Windows XP. In this case, it is not possible to boot into Safe Mode, which requires the user to log onto the machine locally. Fortunately, it is

usually not necessary to go into Safe Mode, even in advanced degrees of infestation, provided all other possible measures are taken.

8. *Empty the Recycle Bin*. There is one more step to take before the removal process is complete. Empty the Recycle Bin. This ensures that any files that were manually removed from Program Files, Temp, or the Internet Explorer are no longer in a position to create havoc on the machine.

9. *Test the Machine*. Test the system by accessing web sites using Internet Explorer, sending e-mail, and by using any other typical applications. In almost all cases, the primary symptoms were sluggish performance and slow or non-existent internet access. If the system is still infected with spyware, you will soon know. If, however, you have followed all of the steps covered, it is highly doubtful that there would be any functioning spyware left on the machine.

For inspection and removal of spyware on large numbers of machines, a spreadsheet similar to the following is very helpful:

Spyware Removal Spreadsheet

User	Hits	Check for Critical Updates, Anti-virus	Run anti-spyware apps	Empty User's IE Cache and Temp	Delete Uneccessary User Profiles	Remove Bogus Apps w/ Add/Remove	Delete Bogus Program Files Folders	Delete Bogus Registry Settings	Empty Recycle Bin	Test, Follow-up, Boot into Safe Mode if Required	User Education, Notes		
ZZ327	324	x	x	x	x	x	x	x	x	x	x		
ZZ821	235												
ZY005	125												

Figure 1

Spyware Prevention

What if the machine is turned over to a user who proceeds to surf to his or her heart's content, randomly clicking on every banner ad and free offer that pops up? In that case, the machine will be quickly re-infected. However, if the user is made aware of the causes of spyware infestation and given suggestions on how to best prevent it, the system will have a much better chance of remaining healthy. For corporate environments, it is important to note here that users will rarely admit to web-surfing out of work-related boundaries; but once educated, they manage to keep their machines relatively free of spyware. It makes a

particularly large impression to make users aware that a web-content filter such as Websense is being used, not only to block objectionable material, but also to track the amount of spyware on each machine.

Content filters can also block outgoing connections to spyware servers once they have been identified and added to the URL filter list. Besides being useful for identification and monitoring purposes, the ability to block web connections helps to prevent reoccurrence of the spyware invasion once the unwanted files have been removed.

Fliers or e-mail may also be sent out to all users, educating them on spyware awareness and prevention. This type of user education seeks to prevent users with non-infected machines from making the mistakes others have already made. Company security presentations are also an excellent way to get the word out. For corporate users, it is also important to show how adherence to prescribed usage policies prevents spyware contamination. Once computer users understand how machines become infected with spyware, they tend to respond in a positive manner, as it is their data, computers, and work that are at stake.

An effective client firewall is a must. For home users and organizations that depend on web access, perimeter firewalls or routers utilizing NAT addressing do nothing to prevent the threat, because blocking the web via Port 80 is not an option. The threat must be stopped at the machine. Examples of client firewalls are ZoneAlarm, Symantec Client Firewall, and the Windows Firewall included with Windows XP Service Pack 2. Users are alerted to possible spyware threats in the form of ActiveX Controls, executables, and Trojans, and are given the option of blocking them or allowing them to pass through. Granted, most spyware threats enter the machine as a result of user action; but by adding another layer of defense, the user is given another opportunity to block such exploits, regardless whether being aware of allowing it or not. The firewall will also identify and block attempts being made by spyware to connect with external servers.

As mentioned earlier, it is also essential to install anti-virus applications and keep them updated with the latest signatures. In addition, install critical updates and patches as soon as they are available. Good defense against viruses, worms, and Trojans often equates to good defense against spyware. Also, the anti-spyware applications referred to in the Spyware Removal section may have auto-update and auto-scan features, as well as blocking alerts, features that all add another important defensive layer. Enable these features if they are available.

Another preventive solution to the spyware problem is legal action. The State of California has passed a law, the Consumer Protection Against Spyware Act, that bans the installation of software that takes control of another computer. Consumers are able to seek up to $1,000 in damages if they think they have fallen victim to the intrusive software. It only goes so far, however, as to penalize

those who transmit viruses from another user's computer, use a computer as part of a DDOS attack, or fool the user into installing software by offering an option to decline installation, which is, in fact, the selection to install. (A Distributed Denial of Service, or DDOS, attack is an attack in which multiple computers are used to send a large amount of packets to a server or network, thus overwhelming it and rendering it useless.) It is doubtful that this law will have much impact on the enormous distribution of spyware with which we're being assaulted today.[11]

Prior to the passage of the California bill, the State of Utah passed the Spyware Control Act, effective in March 2004. This law has gone much further towards dealing with the real problem and not without criticism from those who stand to lose out due to it. There have also been concerns voiced by legitimate firms, who may view such laws as the beginning of massive government regulation of internet commerce. The intent of a well-written anti-spyware law, however, is to protect the computer user. The Utah bill has done just that, by defining spyware and prohibiting it's installation on a user's computer by another person. It also defines methods of installation that are unacceptable and forbids them as well.[12]

It is hoped that a spyware bill, titled the Securely Protect Yourself Against Cyber Trespass Act, or SPY ACT, recently presented in Congress will go even further towards eliminating spyware. Under SPY ACT, software could not be downloaded without the user's permission. It would also make provisions against browser hijacking and keystroke logging, as well as many other spyware functions. The sponsors of the bill feel it has a good chance of being signed into law. It is a given, however, that spyware developers are already gearing up for exploitation of any legal loopholes built in to this legislation.[13]

On a smaller scale, the FTC is currently conducting a civil suit against "spam king" Sanford Wallace, charging him with installing spyware on user's computers, bombarding them with pop-up ads, and offering to sell them an anti-spyware application (that didn't actually work). Wallace recently agreed to restrict the sending of ads to those users who visit his web sites. The court hearing is still pending, but this is a step in the right direction.[14] This illustrates that existing laws can be used to put a stop to spyware. Until definitive laws are made at the national level, though, and more cases are won in court against spyware purveyors, all Windows users must continue to take all necessary measures to prevent and remove spyware.

The last option I'd like to discuss is that of not being a Windows user. One general security advantage to using Linux is that most Linux users do not log on as Root, which is similar to Administrator in Windows. This means that it much easier for a Windows XP Home user to run an executable file than a Linux user, but it doesn't necessarily prevent spyware installation. Anyone using a web browser in Linux is subject to many of the same ploys that Internet Explorer is exposed to; but because Linux software installations by default require the user to log on as Root, the user may be alerted to suspicious activity. Another reason

Linux and MacOS platforms are free of spyware is due to the fact that, in comparison to Microsoft, they represent a much smaller segment of the internet market and are not considered targets by firms that depend on the number of ad views to generate income. Were Linux to gain a much more sizeable share of the PC market than it now has, the platform would become more attractive the spyware marketing firms. The same is true for Apple's MacOS. For a long time to come, though, Microsoft will probably continue to dominate the OS market, so using a Linux distribution will still be a safe bet for spyware prevention. Unfortunately, almost all corporation, and most home users, have an appetite for applications that depend on Windows-only functionality, such as that offered by ActiveX controls. For this reason, Linux may not be a viable option for many.

Conclusion

If the thorough examination of spyware installation, removal, and prevention were to make only one impression on the reader, it is hoped that it would be the enormous amount of time and effort that must go towards eradicating the spyware threat. It is highly doubtful that any computer user or business organization would willingly seek to have this type of software installed on a machine unless, of course, they were somehow profiting from it. Where else in our market economy do we see advertising conducted in such an invasive manner, with such a high probability of harm coming to both privately and publicly owned computers and data? Perhaps lawmakers are now beginning to understand the full extent and nature of the problem and will take the actions necessary to protect individual and corporate property. The day an effective, fair anti-spyware law is passed on the national level will be cause for celebration among IT security professionals until, of course, the next big, new threat arrives.

References

1. "Sophos Plc", Virus Information, Analyses, URL:
http://www.sophos.com/virusinfo/analyses/trojmidaddlee.html

2. Skoudis, Ed; Zeltser, Lenny; Malware: Fighting Malicious Code, 2004, Chpt. 4 p148-160, 178-181, Chpt. 6, Prentice Hall PTR

3. "MidADdle", Service Overview, URL:
http://www.midaddle.com/service_overview.html

4. "MidADdle", URL:
http://www.midaddle.com/

5. "Websterflooble", Animus Pactum Consulting, URL:
http://websterflooble.com/programs/program27.html

6. Edward, Mark Joseph; "Update: A Flurry of Enterprise Spyware Solutions", December 2, 2004, WindowsITPro, URL:
http://www.windowsitpro.com/Article/ArticleID/44624/44624.html

7. Edward, Mark Joseph; "Shavlik Enters Antispyware Market", January 6, 2005, WindowsITPro, URL:
http://www.win2000mag.com/Article/ArticleID/45046/45046.html

8. Howes, Eric L.; "Rouge/Suspect Anti-Spyware Products and Websites", January 13, 2005, SpywareWarrior.com, URL:
http://www.spywarewarrior.com/rogue_anti-spyware.htm#products.

9. Defintive Solutions, Inc., BHODemon 2.0, URL:
http://www.definitivesolutions.com/bhodemon.htm

10. Return on Google search of "jusched.exe", URL:
http://www.liutilities.com/products/wintaskspro/processlibrary/jusched/
http://www.neuber.com/taskmanager/process/jusched.exe.html
http://startup.iamnotageek.com/srch-jusched.exe.html

11. Edelman, Benjamin; "California's Toothless Spyware Law", September 29, 2004, benedelman.org, URL:
http://www.benedelman.org/news/092904-1.html

12. Edelman, Benjamin; "A Close Reading of Utah's Spyware Control Act", May 12, 2004, benedelman.org, URL:
http://www.benedelman.org/spyware/utah-mar04/

13. “Symantec Corporation”, Public Sector Solutions, 1995-2005, URL: http://enterprisesecurity.symantec.com/publicsector/article.cfm?articleid=5207&EID=0

14. Quainton, David; “Latest News”, January, 2005, SC Magazine, URL: http://www.scmagazine.com/news/index.cfm?fuseaction=newsDetails&newsUID=26c4e3b3-7ea4-4909-93ee-77de7e0ff6cc&newsType=Latest%20News