Global Information Assurance Certification Paper

Adware and Spyware: A Growing privacy and Security problem.

David Saurino
SANS GSEC
1/8/2004

Abstract

Adware and Spyware have been around for several years and so have the removal tools. The spyware has been evolving ever since and can now pose a serious privacy and security risk as well as lost productivity. Many free Internet "helper" applications and plug-ins come with this ad or marketing based software. Not all adware and marketing based products are bad. This paper will discuss the dangers of what is seen as bad adware, the symptoms and the removal process. We will also look at some alternative products that can be used to avoid the requirements of the worst offenders.

Introduction

Recently a friend told me about strange behavior on his PC. Later he reported to me that he had many different variants of adware on his machine and used special tools to remove them. Adware and spyware removers have existed for some time yet I didn't use one. I had always believed I would be spyware free since I am careful about what I download and install. Recently, while doing my SANS coursework, I noticed slow browser startup times, and frequent crashes of the browser. Surprisingly Spybot Search and Destory was able to find several adware and spyware components on my computer. After the offending software was removed my web browser began responding faster and it no longer crashed when loading PDF files. In the next sections we discuss the dangers of the worst offenders, the symptoms to look for, how to remove the adware/spyware. We are mostly interested in the spyware that sends back data and/or leaves services running in the background.

Adware and Spyware

You probably have a good idea about what adware and spyware does by the names themselves. The definition from Glossary of Communications, Computer, Data, and Information Security Terms maintained by Rob Slade at the University of Illinois for adware states:

> adware
>
> > while not necessarily malware, adware is considered to go beyond the reasonable advertising that one might expect from freeware or shareware. Typically a separate program that is installed at the same time as a shareware or similar program, adware will usually continue to generate advertising even when the user is not running the [originally] desired program. (Slade)

The definition of Spyware also applies to some forms of adware that send information about you to the marketing agency or subscriber. These are the particular types of adware we are concerned with. This is the definition of spyware from same resource as above.

> spyware

> a type of malware that reports on the contents, status, or operation of the computer to a remote system or user. Generically this could be almost any type of information gathering software. More specifically, it usually refers to modules or functions in software that reports to the author, publisher, or service provider of an otherwise legitimate system. Spyware ranges from functions that report on version levels to the host system, through packages that report the presence of other software from the same manufacturer, through systems that gather information on all software installed including those from competing vendors, all the way to modules that report on the user's Web surfing. Justifications proposed for spyware include the need to ensure versions are kept up to date in order to provide proper service, concerns about software piracy, concerns about use for illegal or unacceptable purposes, and the gathering of marketing information. (Slade)

Basic operation of adware/spyware

The most basic adware is built by marketing and advertising firms as a way of reaching potential customers through the Internet. Adware provides targeted popup advertisements to the user based on the URLs visited. It also tracks the advertisements the user clicks on. (Gain Publishing, 2003) Other types of more invasive Adware are labeled Spyware as they gather information about what the user does with their computer. Most of this information is based on browser usage and anonymous demographic data. This information is transmitted back to the marketing firm for later analysis. Unfortunately there is no good way to know exactly what information is gathered or that there is no personally identifiable information sent to the marketing company. This information could be computer configuration such as hardware and software installation, browser history, browser favorites, Email addresses and files on the computer. Granted, if your hardware configuration of favorites were revealed you may not be concerned but what if they were interested in gathering a list of your email addresses then used them send them targeted ads. This would be crossing the line.

The article “Spyware—It's lurking on your machine” from PC Magazine does a good job of explaining what marketing based spyware captures: “Spyware like Xupiter and Gator eWallet is different. According to Xupiter's privacy policy, the company records more, including Web log information, IP addresses, browser type and versions, screen resolution, time zone, and version numbers of some software installed on your computer. Gator claims not to collect IP addresses, but it gathers "what software is on the personal computer," your "first name, country, and five-digit ZIP code," and more.” (Metz, 2003)

The adware and spyware is packaged with another piece of software that may be of interest to the user such as a browser plug-in or a small application such as a file sharing tool or file compression utility. The makers of the adware/spyware typically pay the developer to include their marketing adware or spyware with the installation of the software or host program. This is how the developer can make money and still give the program away. When the user installs the software the software installer is supposed to notify the user that the marketing components will also be installed. The license agreement will require the use of the marketing

portion of the software to continue using the host software. The point of this is similar to watching over-the-air television. The programs you watch appear to be free but the advertisers pay them for through the broadcast of commercials. (PC Stats, 2003, 3)

Other, more dubious, software installs the advertising portion or the spyware portion of the software as a separate component from the host program. These separate services consume system resources and transmit demographic data back to the spyware maker's servers. This happens even while the user is not using the host software. Some new types of spyware have the ability to install itself when you visit certain web sites by using browser vulnerabilities and mis-configured security settings. (Webb, "Trouble With Spyware & Advertising-Supported Software")

An Important note about the adware/spyware we are concerned with is the type of spyware that is bundled with other software with little notice that it is installed.

A final category of spyware is a type of software that is used to monitor users' activity on a particular machine. These abilities include logging keystrokes from the keyboard (keyloggers), ability to see what the user sees on the desktop, and the ability to access any files stored on the disk. This type of software can have legitimate uses such as for parents to monitor their child's Internet use. One example of this type of spyware is the SubSeven Remote Administration tool. The makers of this software claim there are legitimate uses for "monitoring" computer users. This tool is actually recognized by antivirus software since it can be installed by using Trojan program functions and is used by hackers. (Trend Micro, 2000) This kind of software isn't bundled with software for legitimate use.

Adware and spyware can be much more than annoying popup ads or loss of some browser history. Most adware spyware can cause system performance degradation and instability. In some cases users may have several pieces of this software running simultaneously.

Potential to collect any information

As discussed earlier the spyware software usually collects lists of URLs visited but there is the potential to collect any information stored on the computer.

Because there is no mechanism to audit or control what information is being collected by the spyware software any information on your computer could be collected. Unfortunately since the spyware runs as a separate program executable in the context of the user that installed the software, it can access anything the user can access. This includes reading any file on the system or accessing network resources the user has access. This is verified by William Webb at cexx.org. "since a spyware program is an independent executable program residing on your PC, it will have all the privileges of the user that installed it. On the majority of single-user systems, including Windows 95 and 98, these privileges allow software to read, write and delete files, download and install other software, change the default homepage, interrogate other devices

attached to the system, or even format the hard drive." (Webb, "Trouble With Spyware & Advertising-Supported Software")

If you look closely at the license agreement for adware/spyware supported software it reserves the right to update the spyware software components at any time and that you consent to these updates in the license agreement. (Coursey, 2003) Usually this upgrade consent is buried within the license agreement in convoluted text such that most users may not understand its true meaning. The user may not even realize the spyware software is installed and gathering the current set of information. This could give the spyware authors the legal right to gather almost any data from your machine or possibly your entire network. Brazen spyware developers or marketing firms may use this to push the boundaries of acceptable practice potentially revealing company secrets or personal information.

System Reliability and performance impact

Spyware can virtually create a denial of use of the subjected computer. These processes run in the background without knowledge of the users. They consume system resources such as CPU time during their execution, Network bandwith while receiving and transmitting ads and data, and disk storage space where they cache their offline data. Some of the components that integrate with Windows or the web browser can crash Windows or the browser if they fail.

Spyware that is installed to with with the browser has caused me problems as well as other users on the Internet. PC Magazine reports that some users had problems with IE crashing due to URL tracking spyware installed. One article on the PC Magazine web site refers to a Microsoft Knowledge base Article #259684. The knowledge base article states:

> "When you quit the last or next to last instance of multiple instances of Internet Explorer, you may receive one of the following error messages" … "This issue can occur if the Aureate Radiate program is installed on your computer. Note that this program is included with over 250 shareware programs." (Microsoft Support #259684, 2003)

Aureate Radiate is an adware application that, according to the cexx.org web site downloads ads and pop-ups from their home server and displays them at anytime. This system and network utilization occurs even while users are not running the host program. These programs load when the system starts by residing in the startup folder or the registry run lines. (Webb, "Trash Apps")

Many of the user forums have postings from average users stating that their system performance and stability have improved once the spyware has been removed. (Home of spybot search and destroy 2003)

One adware company, Brilliant Digital, attempts to sell your unused computing power, disk storage, and network bandwidth to a third party. The license

explains that you will have no right to compensation for their use of the distributed computing system. Brilliant isn't the only company trying to implement the distributed computing method. (Coursey 4/3/2003)

Some spyware is targeting and removing the spyware removal tools. According to Damien Cave at Salon.com, the Radlight installer removes Lavasoft's Ad-aware spyware removal tool. Since this discovery Lavasoft has built in code to prevent the removal of Ad-aware. (Cave 4/26/2002) Programs such as Radlight push the boundaries of marketing based software by tampering with the user's computer configuration.

In a letter to the Cexx.org staff an administrator describes a problem he had on his small network. It is good example of how adware and spyware can not only affect one system but the entire network. An Internet advertising company named Conducent closed their business leaving all of its adware installed base software without a server to contact. A component of the adware system, TSADBOT, on a networked PC sent a flood of DNS requests to the local DNS server in an attempt to find the advertiser's site. This in turn exploited a memory leak crashing the operating system the DNS service was running on. Later the firewall also crashed due to the number of name service requests. (Myran) Periodic system audits and spyware scans would help an organization avoid this type of network disruption.

I personally have seen advertisements in the "Outlook Today" window of Outlook Express. It is disturbing knowing that the adware can become so closely integrated with an Email Client.

Installed and running spyware components are hidden and usually have no uninstaller. With enough different pieces of spyware on a computer there is potential to render the computer useless to the user. Since the user isn't fully aware of the loading of this software they cannot make a decision about system resource usage. In this case spyware essentially creates a denial of service situation on "infected" machines.

Future Security implications

Spyware can introduce additional security vulnerability to your system. Newer spyware installs services allow the spyware maker to download newly updated spyware software and install it on the user's machine. These applications run a network service on the machine to listen for updates from the marketing firm. Some of these services may not have strong encryption or authentication or simply have software bugs that could allow anyone to access this update service. Hackers could use this service to install their own version of spyware to gain total control of the system, as discussed in the SANS GSEC reading. This could be disastrous if there are thousands of installations of the spyware running on machines without user's knowledge or if there is no easy way to uninstall or stop the service. It is difficult enough task to patch machines when the administrator

knows what software is installed, it is much worse when the administrator or user does not know if software is installed on their system. This is a good argument to the user of proactive network scanning by the network/systems administration staff.

Symptoms

Before you actually decide to download and run a spyware removal tool here is list of symptoms that you may notice while using your computer with spyware installed:

- Longer than usual browser startup times – Since some spyware tracks user's browsing habits by integrating with the browser. This will delay the startup of the browser. This may also be a result of a large browser cache. Delete the cache and check if the start up time improves. Internet Explorer is integrated with Windows therefore most of the browser libraries are loaded while Windows is running. On a 650MHz computer the browser loads with little perceivable delay.
- Browser home page has changed or keeps changing after you reset it.
- Increased network traffic and slower than normal dialup response times – Specifically look for out-bound traffic when you are not actively using the Internet. Keep in mind that instant messenger and other legitimate always-on application may be sending data.
- Unexplained Browser crashes or system instability may be caused by spyware – I have noticed that embedded Acrobat file viewing crashes have gone away since I have cleaned my system.
- Unexplained popup messages with ads - Some spyware will pop-up windows with advertisements even while you are not actively using the Internet. (Gain 2003)

While these symptoms may not simply be caused by spyware on your system, checking for spyware may be one way to eliminate system instability.

Removal tools

If user suspects there are adware and spyware on the system it is time find a way to remove it. Because some spyware operates covertly within the system, it can be hard to remove.

- Spyware makers typically provide no uninstaller or the uninstaller only removes the host software. This leaves the spyware on the system to continue running.
- Some spyware resides in the Windows directory as a set of DLLs. These DLL are hard to trace in the list of legitimate files included with Windows.
- Spyware applications configure themselves to start from within the Windows registry and other system startup files. These entries should be removed also.

Using a good adware/spyware removal tool is the best and fastest method to remove unwanted software. These tools operate similarly to virus scanners in looking for certain files and patterns to detect the unwanted software.

Two free spyware removal tools are Ad-aware by Lavasoft and Spybot S&D by PepiMK Software. They both work well. Lewis Edge has discussed Ad-aware in a previous SANS paper (Edge). This paper will discuss the use of Spybot S&D.

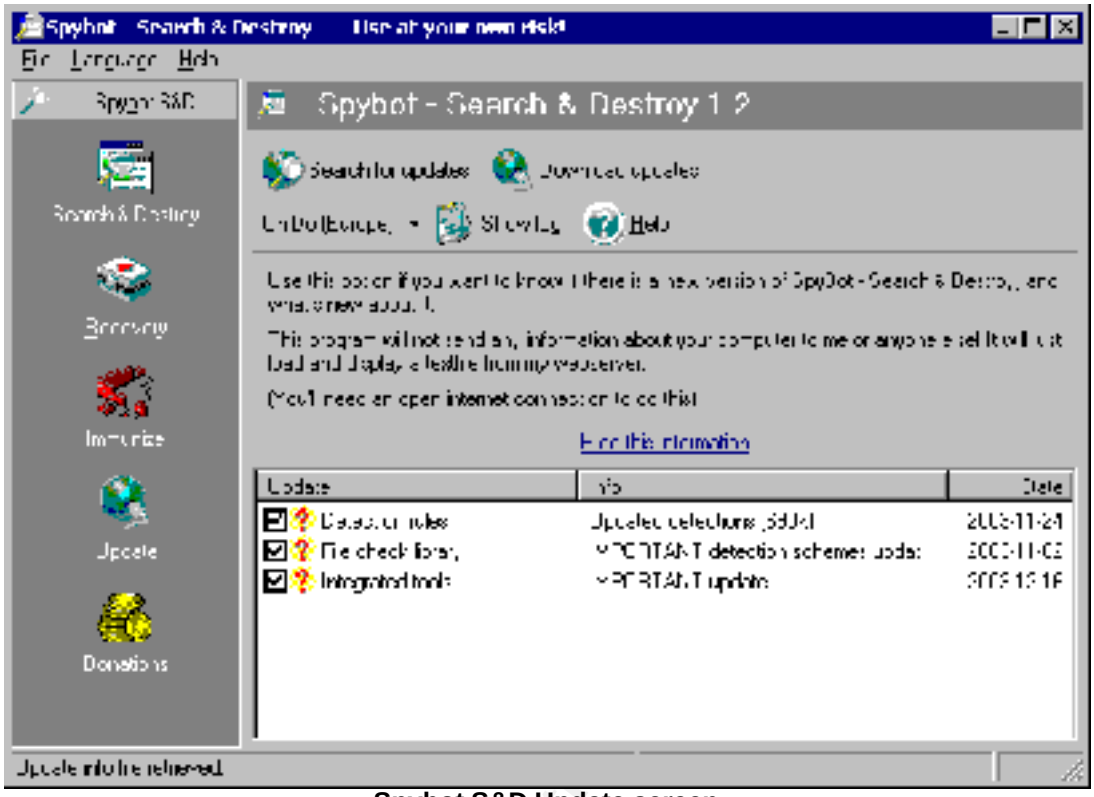
Before we remove the addware/spyware we must first acknowledge that the license agreements that are provided with the host software typically require that the adware/spyware remain on the machine and functional for you continued use of the host software. Therefore removing the adware software may legally require you to stop using the host software and remove it from your system. (Kolla 2003)

Some of the features in Spybot S&D are:

- Easy to use interface provided by an "easy mode" that hides advanced settings and tools from new users.
- Document shredder to provide a secure erasure of files
- Spybot can download updates to the program and the spyware recognition database directly from the spybot web site with the click of a button.
- Background scanning for new spyware installation.
- System tools to view running processes and executable paths.
- Automated browser configuration, or immunization, to block self-installing spyware from exploiting vulnerabilities in Internet Explorer.

SpyBot S&D is Freeware and can be downloaded from their web site at http://www.safer-networking.org. Be sure you go to the .org site, as there is rival site in the .com domain, one example of how cutthroat the spyware anti-spyware business can be. To install Spybot S&D run the downloaded executable. After the program in installed you can start it by using the desktop Icon.

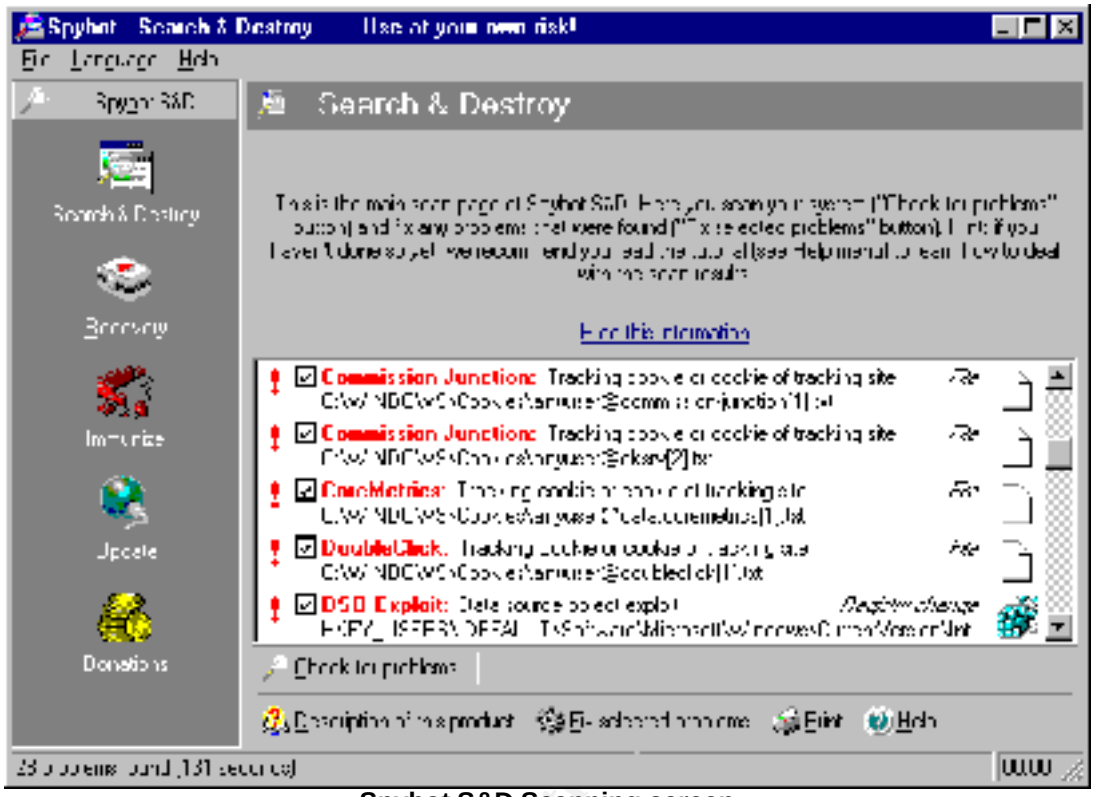
Before scanning it is a good idea to run an update to get the latest database updates. Select "Update" from the left-hand pane and press the "Search for Updates" button. If update items appear select "Download Updates" button from the top of the main screen. This will download and apply the updates. The program will restart automatically.



Spybot S&D Update screen

You will notice that the program has more tabs on the left-hand pane when it restarts. This is an example of the advanced mode. The default installation sets the desktop Icon to load Spybot S&D in easy mode. The start menu icon will start Spybot in advanced mode. The Advanced mode provides more functionality for administrators.

Once the program is up to date it is ready to scan. From the left-hand tool menu select “Search & Destroy” then “Check for Problems”. The scan may take several minutes. The problem list will update as issues are found.



Spybot S&D Scanning screen

When the check completes you can browse the list of problems and uncheck the items you wish to leave unaffected. When you are ready to commit the changes press “Fix Problems” Spybot will make the changes to the system. Spybot S&D saves backup copies of all of the files it deletes or modifies. This allows you to undo any of the removal procedures if you need to.

Spybot S&D saves undo information in its program directory and may cause false alarms from other programs that scan for spyware.

Spybot S&D also provides a function to protect Internet Explorer and the Internet Explorer configuration. These are located under the “Immunize” tool menu. To user the Immunize feature select Immunize from the Left-hand menu. The program will do a brief scan of the Internet Explorer configuration to determine if any of the immunization settings have been applied. When the Immunize feature is set Spybot configured the browser security settings to prevent ActiveX and Browser Helper objects from automatically installing themselves on the machine when visiting web sites. The Immunize settings also blocks installation of known spyware objects listed in the Spybot Database.

Additional tools are included with Spybot and are available in the advanced mode. The process viewer lists running processes on the system. The system startup tool allows an administrator to easily view the list of programs that will

start from the Windows registry run key. Spybot S&D can offers details of known startup programs and their danger factor.

The Browser Helper Object Viewer will display a list of helper applications registered to run within Internet Explorer. The ActiveX tool displays Active X objects installed on the system. The Spybot interface recognizes most spyware objects and will show those with a different Icon. All of the objects registered are displayed. This allows an administrator to remove objects that may not be listed in the Spybot removal database. There are many other features in Spybot S&D. These are discussed in more detail in the Spybot S&D help file or the Frequently Asked Questions (FAQ) section of the web site.

As the Spyware issue grows there are an increasing number of spyware removers and blocking tools. Some of the currently available ones include are, Ad-Aware by Lavasoft, PestPatrol by Pest Patrol inc, Spybot S&D by Pepi MK software, and SpySweeper by Webroot. Internet service providers are getting into the market by providing a free privacy tool to their subscribers. A privacy tool from Earthlink is bundled with a package called Total Access. The privacy component starts by removing web site tracking cookies. Users can also download and activate Earthlink Spyware Blocker, a spyware scanning tool to search their computer for spyware. (Earthlink 2004) The Earthlink tool is based on the WebRoot spyware removal product.

Alternatives to using Adware/spyware supported software

To prevent continued spyware infestations users should look for alternatives to the adware/spyware supported host software they use. Many ad supported software products have an option to purchase an ad free version. For example the Kazaa file sharing application offers an ad free version with additional features and support. The Eudora Email client also provides an ad free version with license purchase.[10] (PC Stats, 2003)

Mozilla is a free web browser package that includes an Email client. (Mozilla 2003) The Mozilla Email client can be used as a direct replacement to Eudora. Using the Mozilla Web Browser will also protect you from some of the Internet Explorer vulnerabilities that URL tracking software can use to install itself. I find the popup and advertisement blocking features of the Mozilla web browser worth using.

Corporations and other large organizations can afford to pay system administrators to scan for and remove spyware as it comes out. Home and small office users are at the most risk. They usually don't have the technical knowledge to discover or manually remove spyware. Home users are naive about the Internet and are willing to install software given away for free thinking that when the software is uninstalled it will be completely removed.

Unfortunately there are many dialup and broadband home computer users that run their computers unprotected. Not only are they vulnerable to worms and

viruses and hackers they are also vulnerable to any spyware that they unknowingly install on their system. Home users should protect their systems with a firewall product, a virus scanner, and with this new threat, an adware/spyware scanner. Some of these adware/spyware removal tools are easy to use and freely available. As the spyware and anti-spyware business continues to evolve don't be surprised if your spyware removal tool itself is attacked as discussed in"Spyware vs. anti-spyware" at salon.com. (Cave 2002)

References

Cave, Damien,"Spyware vs. anti-spyware", Salon.com, 04/26/2002, URL:http://www.salon.com/tech/feature/2002/04/26/anti_spyware/ , (12/19/2003)

Coursey, David, "Caution! Don't let Brilliant hijack your PC", Zdnet, 4/03/2003 URL:http://reviews-zdnet.com.com/4520-6033_16-4207124.html (12/15/2003)

Earthlink, "Earthlink Spyware Blocker", Earthlink.com, URL:http://www.earthlink.net/home/software/spywareblocker/ , (1/6/2003)

Edge, Lewis, "Spyware – Identification and Defense", SANS Reading room, December 14, 2000, URL:http://www.sans.org/rr/papers/index.php?id=688 (12/08/2003)

Gain Publishing, "About Gain Ad Vehicles", URL:http://www.gainpublishing.com/about/ , (12/24/2003)

Kolla, Patrick, "Spybot Search and Destroy web site", URL:http://www.safer-networking.org, (12/06/2003)

Metz, Cade, "Spyware—It's lurking on your machine", PC Magazine, April 22, 2003, URL:http://www.pcmag.com/print_article/0,3048,a=39275,00.asp (12/06/2003)

Microsoft Support, "Knowledge base Article 259684", 11/26/2003, URL: http://support.microsoft.com:80/support/kb/articles/Q259/6/84.asp (12/06/2003)

Mozilla,"Home of the mozilla, firebird, and camino web browsers", Mozilla.org, URL:http://www.mozilla.org/ (12/19/2003)

Myran, Letter to CEXX.org relating to DNS Issues and TSADBOT, URL:http://www.cexx.org/tsad-wingate.txt

PC Stats, "Beginners Guides: Spyware Protection and Removal", PCStats.com, 09/04/2003,URL:http://www.pcstats.com/articleview.cfm?articleid=1458&page=1, (12/19/2003)

Pest Patrol, “Most Prevalent Pests”, PestPatrol.com, 12/24/2003, URL:http://pestpatrol.com/Support/Stats/MostPrevalentPests.asp,(12/24/2003)

Slade, Rob (maintainer), “Glossary of Communications, Computer, Data, and Information Security Terms”, URL:http://sun.soci.niu.edu/~rslade/secgloss.htm, (12/05/2003)

Trend Micro, “TROJ_SUB7”, Trend micro, 1/26/200, URL: http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=TROJ_SUB7 &VSect=T, (12/20/2003)

Web Root Software, “Products – Spy Sweeper”, Web Root Software, URL: http://www.webroot.com/wb/products/spysweeper/index.php, (1/6/2003)

Webb, William, “The Trouble With Spyware & Advertising-Supported Software”, URL:http://www.cexx.org/problem.htm (12/06/2003)

Webb, William, “Trash Apps”, URL:http://www.cexx.org/startup.htm (12/08/2003)