Global Information Assurance Certification Paper

BE AWARE OF SPYWARE – A Hidden Threat to PC's Security and Privacy

Jack Truong
GSEC Practical
Version 1.4b
June 7, 2004

Introduction

The personal computer, or PC, is very affordable nowadays; almost every home has at least one. Although people use their computers for many different reasons, almost all of them have a connection to the Internet. The proliferation of broadband connections, both cable and DSL (Digital Subscriber Lines), has seen not only the rise in viruses, worms, Trojan Horses, but also the rise in spyware and/or adware.

The majority of home computer users today know that computer viruses and PCs go hand in hand, so they are aware of the need to purchase anti-virus software. Some, more knowledgeable users take the next step and install a firewall. However, even the most computer savvy users may not realize the need to purchase anti-spyware software to protect their PCs from privacy threats and identity theft. Spyware and adware do not generally cause as much damage to computers as viruses do. They are hidden, sneaky, behind-the-scenes programs. As a result, they don't get the same media attention that viruses do (even Gartner Inc. gives more attention to viruses then spyware), and so today, most people are generally unaware of the problem.

The purpose of this paper is to educate computer users on spyware and adware, outlining what these programs do, how computers become infected, how to detect and remove them, and then detailing some best practices to avoid these and other types of deceptive software.

Terminology and Definitions

Before we move on, let's take a moment and define some of the common terms used today to identify spyware, viruses and the like. First off, let's start with the term *Malware* – it is short for malicious software or code that is designed to execute actions of malice on a computer without the users consent. This is a broad term used to encompass three main types of uninvited programs: viruses, worms, and Trojan Horses.

Virus: A program that attaches to other software. A boot virus inserts its code into the boot record or master boot record of a disk, so that when the machine starts from that disk, the virus code is executed. A file virus inserts its code into an executable file, so that when that file is executed, the virus is executed as well. (i.e. Melissa, ILOVEYOU, Netsky, Sasser, etc.)

Worm: A program that propagates itself by attacking other machines and copying itself to them. Both worms and viruses have, as their first objective, merely propagation.

They can self-replicate, which mean they can travel from machine to machine by various means. Both can be destructive, depending on what payload, if any, they have been given. But there are some differences: worms may replace files, but do not insert themselves into files. In contrast, viruses insert themselves in files, but do not replace them. (i.e. Bubbleboy, Code Red, SQL Slammer, etc.)

Trojan: A program with a hidden intent. Trojans are one of the leading causes of unauthorized entry into computers. They are programs that allow hackers into your machines without you knowing. (i.e. Back Orifice, SubSeven, NetBus, etc.) Up until now, Trojans were thought of as viral in nature, or hidden programs with some kind of payload. But that is no longer the case. Trojans can now also be non-viral and non-malicious in nature. Meaning spyware, adware, and P2P (Peer-to-Peer) file sharing type programs.

These new types of Trojans are designed for monitoring, spying, and snooping type of activities, rather than causing immediate damage to the PC. This is much worse because of the potential for fraud, privacy and identity theft. Users could continue to operate their computers for months, or even years, without realizing anything is wrong, because the deceptive program is hidden and does not provide any kind of malicious or destructive payload.

There are several terms used to categorize these types of non-viral Trojans. They have been labeled such names as Sneakyware, Pestware, Stealthware, Parasiteware, Snoopware, and Scumware. All refer to deceptive programs that fall under one of the following three main categories:

Adware: A program that displays popup advertisement. Adware typically will track the user browsing habits and report this information to a central ad server. The software is usually available via free download from the Internet, and it is the advertisements that create revenue for the company. Although seemingly harmless (aside from intrusiveness and annoyance of pop-up ads), adware can install components onto your computer that track personal information (including your age, gender, location, buying preferences, surfing habits, etc.). Most advertising supported software do not inform the user that it installs adware on their system, other than via buried reference in the End User License Agreement (EULA), which most people never read. Some adware can install itself on your computer even if you decline the offer. Also, in many cases the free software will not function without the adware component.

Spyware: Any program that covertly collects information about your computer activities and then sends that information to another individual or company without your knowledge or permission. Spyware arrives bundled with freeware and shareware, through email or instant messenger, as an Active X install, or by someone with access to your computer. Spyware is difficult to detect, and even more difficult (if not impossible) for the average user to remove. It is a potentially far more dangerous threat than adware because it can record keystrokes, browser history, passwords, credit card

numbers, online banking information, and any other confidential and private information stored on your computer.

Spyware is often sold as a spouse monitor, child monitor, and a surveillance tool, or simply as a tool to spy on users to gain unauthorized access. You do not have to be connected to the Internet to be spied on; because once your Internet connection is reconnected the next time you log on, all the logging information is sent back to the spy, piggybacking on your existing Internet bandwidth without your knowledge.

P2P (Peer-to-peer): P2P is a file-sharing network – a process made famous by Napster. It enables users to connect directly with other users rather than only to a Website. It lets one individual share directly with any other individual on the P2P network. P2P generally describes a communications model in which each PC has the same capabilities and either party can initiate a communication session. Even though Napster was effectively shutdown by the U.S. courts a few years ago, the use of P2P applications continues to proliferate. Today, there are several different P2P applications freely available to the Internet community, and the use of P2P applications has now expanded to include much larger and different type of files. Meanwhile, with the Internet now integrated into the corporate workplace, employee-based P2P usage still exists in alarming numbers, and the magnitude and types of 'threats' to corporations that permit P2P activity has also increased.

Since the downfall of Napster, other P2P networks have been launched. KaZaA, Grokster, iMesh, and Morpheus are a few that are currently dominating the P2P file-sharing network. They've opened up homes, businesses, and government agencies to potentially serious security risks that are neither widely recognized nor easily remedied. Recent studies involving some of the more popular P2P networks suggest that a significant number of their users are inadvertently sharing personal and highly sensitive data over these networks, including tax returns, bank account information, passwords, e-mail inboxes, and personal identifying information. While the true scope of this problem is still unknown, studies have shown that potentially malicious parties are searching P2P networks for personal emails and credit card numbers. This alone is disturbing. In fact, many P2P networks require their users to install spyware/adware programs before they can use the file sharing utilities. P2P file-sharing networks are also a staging ground for virus-infected files to be shared or distributed across the Internet. The technology has great promise, but until the risks can be eliminated or minimized, all PC users (corporation or home users) should be weary of them.

The chart below summarizes the terms identified above:

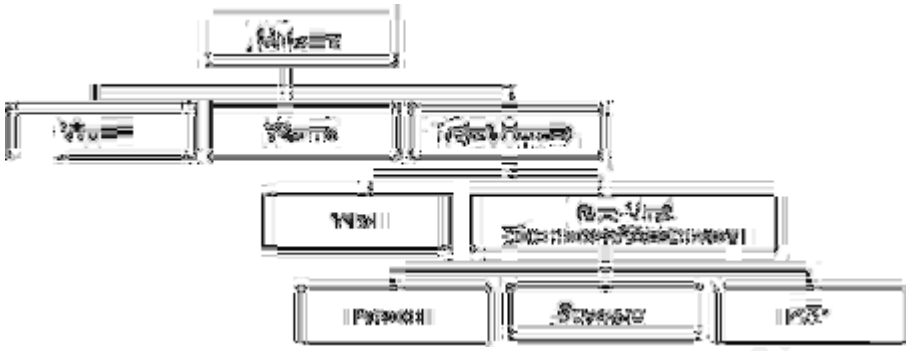


Figure 1

How to determine if a computer is infected

Spyware and adware programs are mainly distributed by being bundled with free software or through P2P file-sharing programs. More and more software is created and distributed, as freeware or shareware, for people to download. They may be legitimate programs, but many times they are bundled with some kind of deceptive software. If users don't read the EULA (End User License Agreement) carefully before they click the "OK" button to install the tool, they are now being monitored and tracked as they surf the Internet. Too many computer users, in general, are "clicker happy". If they see anything that provides a cool, free service, they'll download it without a second thought. That is how so many computers are infected with these hidden spyware/adware programs.

Having said that, there are other illegal ways for these deceptive programs to get onto PCs without the knowledge or even intervention of users. In some cases, just visiting a site can cause a hidden deceptive tool to be downloaded. There are some sites that will launch several pop-ups. Sometimes one after the other, other times all at once. When users try to close them, another one simply takes its place. These are very clever scripting techniques that are not only annoying, but also very covert in nature. Clicking the 'X' to close the pop-up may actually be triggering a download of spyware behind the scenes. In this situation, the best option is to end the Web browser task with the "Windows Task Manager". This effectively shuts down all Web browser processes at once.

The seven signs of adware/spyware infection

The following are the most common signs that a computer has been infected with adware or spyware.

1. **Homepage Changed** – The Internet browser's home page has mysteriously changed. Changing it back manually may work, but before long it changes back again.
2. **Pop-up Ads** - Pop-up advertisements appear when the browser is not running or when the system is not even connected to the Internet.

3. **900 Numbers** - The phone bill includes expensive calls to 900 numbers that you never made - usually at an outrageous per-minute rate.
4. **New Item in Favorites** - A new item appears in the Favorites list or on the Desktop without you putting it there. No matter how many times it is deleted, the item always reappears.
5. **Performance** - The system runs noticeably slower than it did before. In Windows 2000/XP, launching the "Windows Task Manager" and clicking the Processes tab reveals a lot of unfamiliar processes.
6. **Lights Blinking** - The send or receive lights on your dial-up or broadband modem blink just as wildly when you're not doing anything online as when you're downloading a file or surfing the Web.
7. **Toolbar Appears** - A search toolbar or other browser toolbar appears even though you didn't request or install it. When you remove it, it comes back after removal.

There are other symptoms. The above are simply the most common ones.

Why are spyware and adware programs on the rise?

Based on a recent article from InformationWeek, the author stated the following:

> Dell Inc. reported that, 12% of its tech-support calls involved spyware, a problem that has increased substantially in recent months. Scans of one million Internet-connected PCs, conducted last quarter by Internet service-provider EarthLink Inc. and desktop-privacy and -security vendor Webroot Software Inc., found an average of 28 spyware applications running on each PC and more than 300,000 programs at large that can steal data and give hackers access to computers.[1]

In addition, Microsoft believes spyware "accounts for more than 50 percent of the Windows failures reported to Microsoft." [2] Their partners "report that spyware is the number-one support problem and is costing the industry millions of dollars a year in support costs."[3]

One of the main causes of spyware proliferation in recent years is advertising revenues. As more homes and businesses are hooked up to the Internet to do business, advertisers cannot resist tapping into this market. Traditional advertising (TV, radio) is not effective during office hours, and standard banner ads on the Internet are not delivering as well as expected. As a result, advertisers started using targeted online advertising, which performs much better. There are three parties that are involved here: advertisers, developers, and users. Advertisers want to get users to view and click on their ads, so they hire developers to make software that allows them to deliver targeted advertising to users while they surf the Internet. The average user loves getting free software, so the advertisers often provide their software in forms of freeware or shareware. This is a win-win situation for everybody. The user gets the free software, the developer gets paid handsomely, and the advertiser has the capability to track users surfing habits through the hidden features that these tools often provide. These tools

are also installed without alerting anti-virus or firewall programs. As a result of this, more and more advertisers have made various freeware and shareware programs available on the Internet for download.

One of the popular online advertisers is GAIN Publishing.

> GAIN Publishing has distributed software applications to millions of consumers free of charge in exchange for consumers' agreement to receive online advertising from the GAIN Network. The GAIN Network has a unique permission-based relationship with over 43 million users. The GAIN Network enables consumers to download and use some of the Web's most popular software applications -- for free. In return, consumers agree to receive targeted promotions and ads from GAIN Network advertisers.[4]

Some of the free software available from GAIN is Gator eWallet, DashBar, WeatherScope, Precision Time, Date Manager, and the most popular WebSecureAlert. These are useful programs being distributed as freeware. In return, the advertisers gain the ability to install adware and/or spyware to track surfing habits and to deliver targeted advertisements.

There are many other advertisers, besides GAIN, that distribute these kinds of program, and the list is growing each month. The other company worth mentioning is FunWebProduct.com. Visit this site at your own risk. One click on a graphic may kick off a download of one of the company's many freeware programs. Even clicking 'no' to prevent the download does not work. You have to do it three times, instead of just one click, to make the download pop-ups go away.

Spam (unsolicited emails), is another type of nuisance that is also on the rise. Spam and spyware are many ways directly related. Unfortunately, only Spam has been hitting the news relentlessly in the past few years. However, the attention of spyware is slowly hitting the limelight. It is my belief that within a year everyone will be talking about it, because spyware is here to stay. If advertisers are already snooping on a PC for information like surfing habits, sites visit, the ads clicked on or downloaded, it won't be long before they gather a complete profile about a user's basic identity. What's more alarming is that hackers are starting to get on the bandwagon and utilizing the same method of getting the stealth software onto a PC, undetected by the firewall and/or anti-virus program. However, hackers are less interested in gathering stats on what ads a user clicked on or web sites visited. They'll be more concerned with id/password keystroke logging, email logging, screen shot capturing, instant messaging logging, etc. Some of the popular spyware includes Spector Pro, SpyAgent, and IamBigBrother. Is it any wonder that this process has now started to be implicated in the seemingly inexorable rise in spam? If you want to combat spam, you must address the main root of the problem – spyware!

Why is spyware such a threat?

Spyware and adware are becoming a big threat to those using computers to access the World Wide Web. The Internet is attracting greater numbers of daily users every year. According to the Consumer Internet Barometer, produced by the NFO WorldGroup, Forrester Research and The Conference Board, consumers are logging on in greater numbers than ever before.

> Now, 39% say they log on daily, up from 36% a year ago. More than 71% of users who primarily log on to conduct work-related activities do so daily. Close to 64% of consumers engaged primarily in personal communication go online every day, while only 49% of those using the Internet primarily for personal research log on with the same frequency.[5]

That is why it is not surprising that more employees are installing spyware and adware on corporate systems – usually without knowing that they are doing so. The IT department is unaware until they get a call to the Helpdesk about a PC that has gone awry. The immediate problems or threats due to spyware are fourfold: consumption of computing capacity, consumption of bandwidth, legal liabilities, and security and privacy issues.

Consumption of Computing Capacity – If the hard drive's green light is constantly blinking as if it is processing something and performance has really degraded, chances are that the computer is infected with spyware or adware. These programs typically do not show up in the Windows Task Manager nor are they listed under the Add/Remove Programs section. They quietly and covertly collect data about the user while using the user's computer processing power. It is also worth noting that many adware programs will use the user's disks to store the advertisements. Since it is not unusual for a user to have many different covert programs running at the same time, the cumulative effect on the system's processing capacity can be dramatic.

Consumption of Bandwidth – If several PCs on a network are infected with deceptive software, the detrimental effect to the whole network can be costly. Especially, with a network of, let's say 2000 users, and half of that number may be constantly receiving pop ups and banner advertisements, with the hidden programs covertly phoning home to the ad servers with user information. Spyware often locates email addresses and phone home with them. The addresses will then be traded between spammers. As a result, the network will see a dramatic increase in spam. According to the washingtonpost.com (March 13, 2003) about "40 percent of all e-mail traffic in the United States is spam, up from 8 percent in late 2001 and nearly doubling in the past six months."[6] The amount of spam received is directly proportional to the number of spyware/adware program running on the network. When you combine the cost of the bandwidth consumed and the staff time taken to handle spam, it becomes a very expensive problem. Over time, that problem will be a major burden to a company's business.

Legal Liabilities – Napster was brought down using copyright laws. Today there are many other, more sophisticated, P2P file-sharing programs, which would make Napster look like child's play. KaZaA for example, is a very popular P2P program that, like Napster, allows all KaZaA users to share their music files with each other. However, unlike Napster, it is not limited to sharing just music files, but any files in any format. Also unlike Napster, KaZaA does not require a central server for it to work. Because of this non-centralization feature of KaZaA, they can make the argument that their network cannot be shutdown. This is one of the main reasons that persuaded the Supreme Court of the Netherlands to rule in December 2003 that "the creators of Kazaa can't be held liable for the copyright-infringing actions of users of the popular file-sharing application."[7] In its decision, the court cites international rulings including the 1984 U.S. Supreme Court ruling that said device makers, a VCR maker in that case, can't be held liable for user infringement."[8] What this all means is that, the onus is now on the users of the file-sharing product, that can potentially be sued for 'trading' copyrighted materials, not the maker. In addition, if employees are doing these types of activities during work hours, the company they work for can potentially be sued as well.

The U.S government is starting to recognize this growing spyware problem. In fact Senator John Edwards introduced the "Spyware Control and Privacy Protection Act" in late 2000.

> Under the spyware bill, software providers that use codes to track the activities of Internet users would have to notify consumers in plain language when the users buy or download programs. No information on Internet surfing habits could be collected without first obtaining each consumer's permission. Businesses that gather data would have to let individuals know what information has been assembled, provide a way to correct errors, and safeguard the data against unauthorized access by hackers.[9]

While they may have taken steps in the right direction, the majority of users downloading software never read the EULA before downloading and installing software. The information in the EULA tends to be vague and buried deep inside, which makes it hard for the average users to understand.

In terms of anti-spyware legislation, the state of Utah was the first state in the U.S. to pass a law on May 3, 2004 called the "Anti-Spyware Act". This act "bars companies from installing software that reports its users' online actions, sends any personal data to other companies, or pops up advertisements without permission."[10] This act has the online advertising agencies up in arms. Some are suing the state of Utah for violating free speech and unfairly harming their businesses.

Security and Privacy Issues – Deceptive software uses users Internet connections without their knowledge to continually report back to the company. Most companies' customer service and privacy statements claim that they won't collect or subsequently distribute sensitive information about you, but a gaping security hole remains. You are

unknowingly leaking information to another company, which invites unsolicited advertising campaigns and other nuisances, like spam. Most users have concerns about privacy, and they want companies that use spyware to address these concerns. Although privacy-conscious companies disclose in their privacy statements the nature of data that they send to and receive from spyware, users have little control over this data. Moreover, even if it's not used now, spyware has the potential capability to gather and send much more than just usage data later on. Many Internet users who have advertising-supported spyware products installed on their machines don't even seem to be concerned about this security breach. But they should be!

Last year one person pleaded guilty in a U.S. federal court to installing key-logging software at several Kinko's Inc. locations in Manhattan. For more than a year he collected the keystrokes of the customers of the printing and copying chain, including passwords and user names, and used that data to fraudulently open bank accounts.

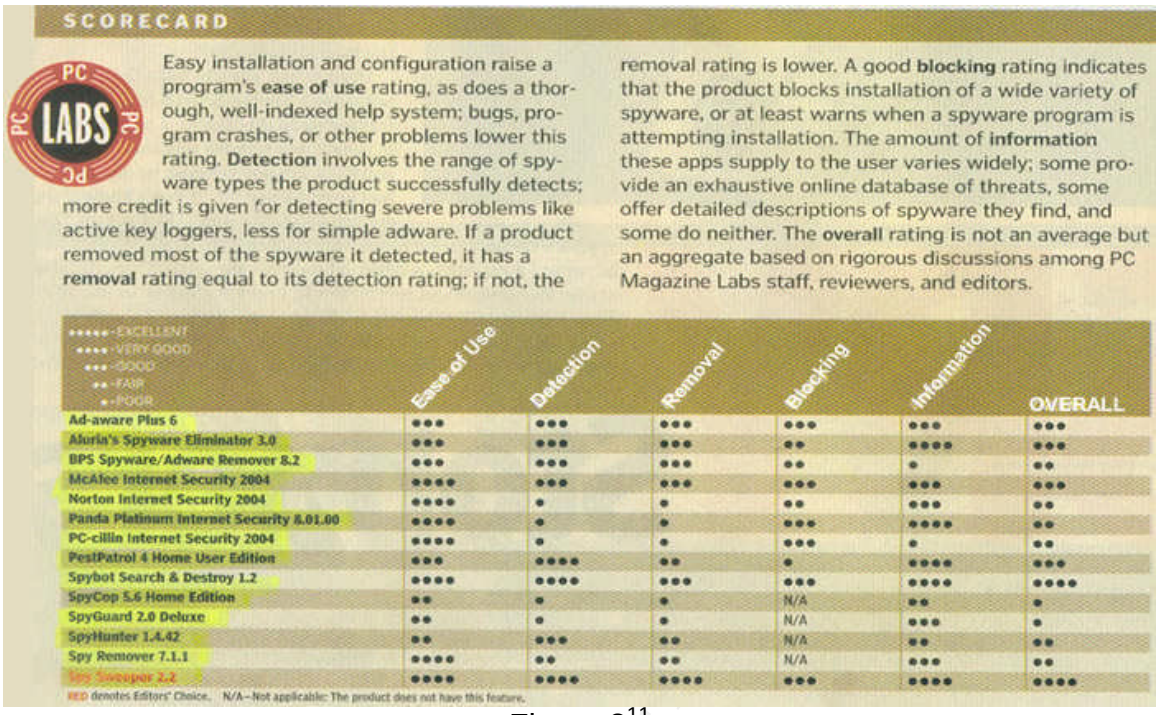
Cyber café is another potential target for spyware software, because so many different people log on to the same computer to do web surfing. I would recommend that you not do any sort of online banking or purchasing at these public places - even at your place of work. Unless, you're able to run an effective anti-spyware program to clean up the computer system before keying in any private information like passwords, bank accounts or credit card information. You never know who might be spying on the other end.

How to detect and remove adware and spyware

To detect and remove covert software, it is strongly recommended that an anti-spyware program be purchased and installed. Anti-virus and firewalls will not be enough to eradicate spyware. Anti-virus software is designed only to detect programs that are virus in nature, and firewalls are designed to block Internet ports and do network translation of IP addresses to keep hackers out. Spyware programs will bypass both of these defenses, because they are usually downloaded through websites (using port 80). This type of stealthware is not only hard to detect, but also very hard to remove. This is why a good anti-spyware tool, in conjunction with anti-virus and firewall programs, is so essential.

There are various types of anti-spyware programs available and the majority of them do a reasonable job of detection and eradication. The criteria for purchasing anti-spyware programs should be their effectiveness, ease-of-use, ease of installation, customization, helpful support, and useful features. Also, anti-spyware program should include features such as auto detect, auto scan, quarantine, etc. The cost criterion is left out, because there are some freeware programs that do a pretty good job. Before going out and purchasing an anti-spyware program, it is important to do the research.

PC Magazine (March 2004 issue) did some tests on 14 well-known anti-spyware products, and the results are displayed in the chart below.



SCORECARD

Easy installation and configuration raise a program's **ease of use** rating, as does a thorough, well-indexed help system; bugs, program crashes, or other problems lower this rating. **Detection** involves the range of spyware types the product successfully detects; more credit is given for detecting severe problems like active key loggers, less for simple adware. If a product removed most of the spyware it detected, it has a **removal** rating equal to its detection rating; if not, the removal rating is lower. A good **blocking** rating indicates that the product blocks installation of a wide variety of spyware, or at least warns when a spyware program is attempting installation. The amount of **information** these apps supply to the user varies widely; some provide an exhaustive online database of threats, some offer detailed descriptions of spyware they find, and some do neither. The **overall** rating is not an average but an aggregate based on rigorous discussions among PC Magazine Labs staff, reviewers, and editors.

●●●●●-EXCELLENT
●●●●-VERY GOOD
●●●-GOOD
●●-FAIR
●-POOR

	Ease of Use	Detection	Removal	Blocking	Information	OVERALL
Ad-aware Plus 6	●●●	●●●	●●●	●●●	●●●	●●●
Aluria's Spyware Eliminator 3.0	●●●	●●●	●●●	●●	●●●●	●●●
BPS Spyware/Adware Remover 8.2	●●●	●●●	●●●	●●	●	●●
McAfee Internet Security 2004	●●●●	●●●	●●●	●●●	●●●	●●●
Norton Internet Security 2004	●●●●	●	●	●●	●●●	●●
Panda Platinum Internet Security 8.01.00	●●●●	●	●	●●●	●●●●	●●
PC-cillin Internet Security 2004	●●●●	●	●	●●●	●	●●
PestPatrol 4 Home User Edition	●●●	●●●●	●●	●	●●●●	●●●
Spybot Search & Destroy 1.2	●●●●	●●●●	●●●	●●●	●●●●	●●●●
SpyCop 5.6 Home Edition	●●	●	●	N/A	●●	●
SpyGuard 2.0 Deluxe	●●	●	●	N/A	●●●	●
SpyHunter 1.4.42	●●	●●●	●●	N/A	●●	●●
Spy Remover 7.1.1	●●●●	●●	●●	N/A	●●●	●●
Spy Sweeper 2.2	●●●●	●●●●	●●●●	●●●	●●●●	●●●●

RED denotes Editors' Choice. N/A=Not applicable: The product does not have this feature.

Figure 2[11]

According to PC Magazine, their results showed that Spy Sweeper 2.2 is the best product for 2004.

> Webroot Software's Spy Sweeper 2.2 is the most effective standalone tool for detecting, removing, and blocking spyware. Although the program didn't perform perfectly in our testing, it was successful in inhibiting most spyware and was one of only three products that were able to scan a system successfully with the key logger SpyAgent installed."[12]

It should also be mention that Spybot Search & Destroy 1.2 (last year's Editors' Choice) came in a close second. The price range is very comparable between the fourteen products tested. The cost would be anywhere from $15.95 to $69.99 for any one of the products tested, except for Spybot, which is free.

For a large company, concerned with maintenance and bulk licenses, the standalone tools like Spybot and Spy Sweeper may not be appropriate. An enterprise version may be the better alternative. Companies like McAfee and Norton (who are leaders in the anti-virus field) are just starting to roll out tools to combat spyware this year. They are fairly new to the arena of spyware detection and eradication. Their new spyware security product suites cannot compare to some of the standalone tools currently available. It is recommended that businesses not invest in McAfee or Norton until 2005, when they roll out their next version of spyware tools. Analysts say McAfee's and Norton's enterprise products should be more comparable in the next version or two. When that happens, great standalone products like Spy Sweeper and SpyBot Search & Destroy may see significantly decreasing sales.

Home users, especially those that share their home PCs with their spouse or kids, should install anti-spyware program as soon as possible. When these pests are detected and removed, their systems will operate much better.

Microsoft's five tips to avoid spyware

Microsoft also recently posted on their Web site information about how to avoid and remove deceptive software:

1. **Use Appropriate Web browser Security Settings** – When you first installed Microsoft Internet Explorer browser, the default "medium" security level setting should be sufficient. Setting the level higher than that may make it harder for you to access certain sites, and any lower than "medium" will not be secure and is not recommended.

2. **Don't Accept Download from Strangers** – Just like we tell our kids not to talk to strangers, we should also follow the same mentality when visiting web sites we do not know. Only buy or download software from sites you know and trust. And always read the fine print (the EULA) before you click on "I Agree" or "OK". In addition, be wary about sites that offer freeware or shareware, like free music, free movies, free toolbars, file-sharing programs, or any free software that may sound cool to use. The majority of these freeware, if you read the fine print, will include some spyware with the download. Once installed, the PC security is now opened up to the whole world through the Internet, and your privacy will be breached without you knowing.

3. **Pay Attention to Signs of Spyware/Adware on Your Computer** – When you launch your Internet browser, does it connect to a site you do not recognize? Do you see an increase in pop up advertisements? Is your computer taking longer to boot up or performance seems sluggish? Spyware is a pesky threat. (Refer to the "seven signs of infection" at the beginning of this paper for more information).

4. **Install an Anti-Spyware Tool** – Many companies offer free anti-spyware tools for download, like SpyBot and Ad-aware. These are popular standalone tools that allow you to detect and remove deceptive software from your computer. Keep in mind these tools operate very similar to anti-virus software, meaning they require daily definitions update to be able to detect the new and latest spyware/adware available. Ensure that you obtain a tool that provides automatic definitions download.

5. **Keep Windows up-to-date** – Stay current with the latest Windows security patches. If you have Windows XP, ensure "automatic update" is enabled so you don't have to worry about what security patches are current.

By following the above tips you'll be able to have more peace of mind when you surf the Internet. You will not only be more abreast of the latest security threat to your computer, but also taking proactive steps to be more aware of what you are downloading and installing on your computer.

Conclusion

As long as we rely on computers to help us in our daily lives, spyware will never completely go away. However, by being aware of the signs that indicate spyware is present, and by taking the proactive steps outlined in this paper, we can minimize the effect of spyware.

Now that you know what spyware programs are, why they are on the rise, and what they can potentially do to your computer, I hope your next computer purchase would be an anti-spyware tool. These tools are getting more effective and affordable with each new version. Just like we must have an anti-virus program running at all times, we must have an anti-spyware tool running on our computer at all times. Defense in depth is the key! Anti-virus and firewalls programs by themselves are not sufficient. We must use all three defenses simultaneously if we plan to connect our computers to the Internet, in anyway.

Spyware is such a big threat not only to your computer security and privacy, but also the legal complications that it introduces. Quite simply, the existence of adware and spyware is incompatible with the concept of a secure system. These programs need to be found and removed.

End Notes

1. Hulme, George. “Tiny, Evil Things”. April 26, 2004. URL: http://www.informationweek.com/showArticle.jhtml?articleID=19200218 (May 18, 2004).

2. Furman, Keith. “Microsoft Presents Antispyware Strategy”. April 21, 2004. URL: http://www.winnetmag.com/article/articleid/42432/42432.html (May 18, 2004).

3. Furman, Keith. “Microsoft Presents Antispyware Strategy”. April 21, 2004. URL: http://www.winnetmag.com/article/articleid/42432/42432.html (May 18, 2004).

4. GAIN Publishing. URL: http://www.gainpublishing.com/advertise (May 20, 2004).

5. Unknown Author. “Internet Usage on the Rise, With More Consumers Logging on Daily”. July 2, 2003. URL: http://www.yenra.com/how-many-people-use-the-internet (May 26, 2004).

6. Krim, Jonathan. “Spam's Cost To Business Escalates”. March 13, 2003. URL: http://www.washingtonpost.com/ac2/wp-dyn/A17754-2003Mar12 (May 26, 2004).

7. Evers, Joris. “Dutch Supreme Court rules Kazaa is legal”. December 19, 2003. URL: http://www.infoworld.com/article/03/12/19/HNcourtkazaa_1.html (May27, 2004).

8. Evers, Joris. “Dutch Supreme Court rules Kazaa is legal”. December 19, 2003. URL: http://www.infoworld.com/article/03/12/19/HNcourtkazaa_1.html (May27, 2004).

9. Unkown Author. “Senator Edwards Proposes Spyware Law”. January 29, 2001. URL: http://edwards.senate.gov/press/2001/jan29c-pr.html (May 27, 2004).

10. Olsen, Stefanie. “Adware maker challenges Utah anti-spyware law”. April 13, 2004. URL: http://news.com.com/2100-1024_3-5190880.html (May 27, 2004).

11. Metz, Cade. “Spy Stoppers”. PC Magazine March 2004 (2004): 79 – 94.

12. Metz, Cade. “Spy Stoppers”. PC Magazine March 2004 (2004): 79 – 94.

References

Evers, Joris. “Dutch Supreme Court rules Kazaa is legal”. December 19, 2003.
URL: http://www.infoworld.com/article/03/12/19/HNcourtkazaa_1.html (May27, 2004).

Furman, Keith. “Microsoft Presents Antispyware Strategy”. April 21, 2004.
URL: http://www.winnetmag.com/article/articleid/42432/42432.html (May 18, 2004).

GAIN Publishing.
URL: http://www.gainpublishing.com/advertise (May 20, 2004).

Gibbs, Mark. “The Rise and Rise of Scumware”. January 23, 2004.
URL: http://www.itworldcanada.com/Pages/Docbase/ViewArticle.aspx?ID=idgml-74e7e818-220f-4e0c-8201-5af2409c90b9 (May 28, 2004).

GSEC Course Materials

Hassell, Jonathan. “Spyware - Part1”. June 1, 2001.
URL: http://www.winnetmag.com/article/articleid/21272/21272.html (May 28, 2004).

Hulme, George. “FTC Takes Aim at Spyware”. April 19, 2004.
URL: http://www.informationweek.com/showArticle.jhtml?articleID=18901980 (May 28, 2004).

Hulme, George. “Tiny, Evil Things”. April 26, 2004.
URL: http://www.informationweek.com/showArticle.jhtml?articleID=19200218 (May 18, 2004).

Kandra, Anne. “Avoid helping friends and family”. April 13, 2004.
URL: http://www.itworldcanada.com/Pages/Docbase/ViewArticle.aspx?ID=idgml-d567574a-b1e0-428e-97fe-a6f267a4681b (May 28, 2004).

Keizer, Gregg. “Security: From Bad To Worse?”. Dec. 29, 2003.
URL: http://www.informationweek.com/showArticle.jhtml?articleID=17100254 (May 28, 2004).

Krim, Jonathan. “Spam's Cost To Business Escalates”. March 13, 2003.
URL: http://www.washingtonpost.com/ac2/wp-dyn/A17754-2003Mar12 (May 26, 2004).

Luna, J.J. How to Be Invisible, Revised Edition : The Essential Guide to Protecting Your Personal Privacy, Your Assets, and Your Life. New York City: Thomas Dunne Books; Revised edition, March 18, 2004.

Metz, Cade. “Spy Stoppers”.
PC Magazine March 2004 (2004): 79 – 94.

Olsen, Stefanie. “Adware maker challenges Utah anti-spyware law”. April 13, 2004. URL: http://news.com.com/2100-1024_3-5190880.html (May 27, 2004).

Roberts, Paul. “NAI's McAfee the latest to add anti-spyware”. January 23, 2004. URL: http://www.itworldcanada.com/Pages/Docbase/ViewArticle.aspx?ID=idgml-bf06414d-052d-4bbf-862a-e2fbc913bc14 (May 28, 2004).

Schuchart, Steven. “Invasion of Privacy: Web Sites Are Going Too Far Now”. January 7, 2002. URL: http://www.networkcomputing.com/1301/1301rant.html (May 28, 2004)

Unknown Author. “Internet Usage on the Rise, With More Consumers Logging on Daily”. July 2, 2003. URL: http://www.yenra.com/how-many-people-use-the-internet (May 26, 2004).

Unknown Author. “Senator Edwards Proposes spyware Law”. January 29, 2001. URL: http://edwards.senate.gov/press/2001/jan29c-pr.html (May 27, 2004).

Unknown Author. “What you should know about spyware”. April 16, 2004 URL: http://www.microsoft.com/security/articles/spyware.asp (May 28, 2004)

Last Updated: October 18th, 2017

Upcoming Training

SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201710,	Oct 23, 2017 - Nov 29, 2017	vLive
SANS San Diego 2017	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	Live Event
San Diego Fall 2017 - SEC401: Security Essentials Bootcamp Style	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	vLive
SANS Seattle 2017	Seattle, WA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Gulf Region 2017	Dubai, United Arab Emirates	Nov 04, 2017 - Nov 16, 2017	Live Event
Community SANS Vancouver SEC401^	Vancouver, BC	Nov 06, 2017 - Nov 11, 2017	Community SANS
Community SANS Colorado Springs SEC401~	Colorado Springs, CO	Nov 06, 2017 - Nov 11, 2017	Community SANS
SANS Miami 2017	Miami, FL	Nov 06, 2017 - Nov 11, 2017	Live Event
SANS Sydney 2017	Sydney, Australia	Nov 13, 2017 - Nov 25, 2017	Live Event
SANS Paris November 2017	Paris, France	Nov 13, 2017 - Nov 18, 2017	Live Event
SANS San Francisco Winter 2017	San Francisco, CA	Nov 27, 2017 - Dec 02, 2017	Live Event
Community SANS St. Louis SEC401	St Louis, MO	Nov 27, 2017 - Dec 02, 2017	Community SANS
SANS London November 2017	London, United Kingdom	Nov 27, 2017 - Dec 02, 2017	Live Event
Community SANS Portland SEC401	Portland, OR	Nov 27, 2017 - Dec 02, 2017	Community SANS
SANS Khobar 2017	Khobar, Saudi Arabia	Dec 02, 2017 - Dec 07, 2017	Live Event
SANS Austin Winter 2017	Austin, TX	Dec 04, 2017 - Dec 09, 2017	Live Event
SANS Munich December 2017	Munich, Germany	Dec 04, 2017 - Dec 09, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Dec 04, 2017 - Dec 09, 2017	Community SANS
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201712,	Dec 11, 2017 - Jan 24, 2018	vLive
SANS Bangalore 2017	Bangalore, India	Dec 11, 2017 - Dec 16, 2017	Live Event
SANS Cyber Defense Initiative 2017	Washington, DC	Dec 12, 2017 - Dec 19, 2017	Live Event
SANS Cyber Defense Initiative 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Dec 14, 2017 - Dec 19, 2017	vLive
Community SANS Nashville SEC401^	Nashville, TN	Jan 08, 2018 - Jan 13, 2018	Community SANS
Community SANS Hawaii SEC401	Honolulu, HI	Jan 08, 2018 - Jan 13, 2018	Community SANS
SANS Security East 2018	New Orleans, LA	Jan 08, 2018 - Jan 13, 2018	Live Event
Mentor Session - SEC401	Memphis, TN	Jan 09, 2018 - Mar 13, 2018	Mentor
Northern VA Winter - Reston 2018	Reston, VA	Jan 15, 2018 - Jan 20, 2018	Live Event
SANS Amsterdam January 2018	Amsterdam, Netherlands	Jan 15, 2018 - Jan 20, 2018	Live Event
Mentor Session - SEC401	Minneapolis, MN	Jan 16, 2018 - Feb 27, 2018	Mentor
SANS Las Vegas 2018	Las Vegas, NV	Jan 28, 2018 - Feb 02, 2018	Live Event
Las Vegas 2018 - SEC401: Security Essentials Bootcamp Style	Las Vegas, NV	Jan 28, 2018 - Feb 02, 2018	vLive