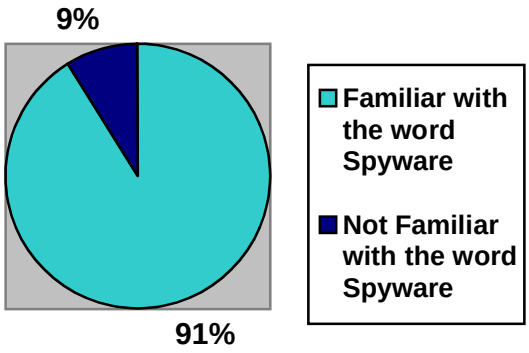
Anti-Spyware: Knowledge and Software for Securing the Home PC

Nicolle Johnson
DTEC6823

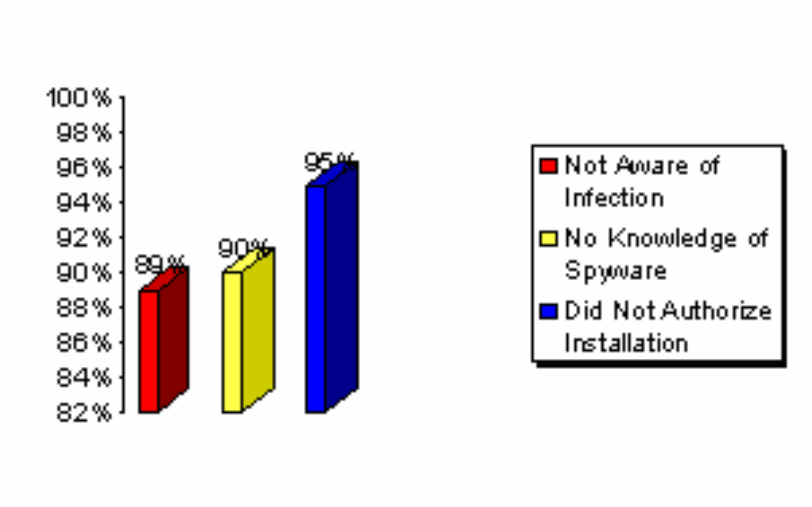
Anti-Spyware: Knowledge and Software for Securing the Home PC

It only takes a moment and you do not know until it is too late, if even then. While you are checking your email or looking up a website, a silent predator is downloaded onto your computer to watch your every move. OnGuard Online, a multimedia Internet safety campaign run by the Federal Trade Commission, defines spyware as "software installed on your computer without your consent to monitor or control your computer use." As easily as that, your privacy is invaded, your PC is slowly grinding to a halt, and you are left wondering what happened and what you can do about it.



According to a 2004 survey by America Online and the National Cyber Security Alliance, 91% of users questioned were familiar with the term spyware. Only 53% believed their computers were infected, but a scan found that 80% of their PCs had some type of spyware installed on them.

Following the scan the participants were shown a list of the known spyware found on their computers. 89% did not know the programs were there, 90% had no idea what they are or what they do, and 95% did not give their authorization for the spyware to be installed. The average number of spyware components per computer was 93 with one computer having well over a thousand. In order to understand how these numbers can be so high, it is necessary to first understand how spyware attacks.



Spyware is as insidious as its name and the results of the survey imply. It comes in through pop-up ads and email spam, rides in with software bundles from shareware sites and CD's, or simply waits for you to go online and invites itself in. It is made even more difficult to fight because it comes in a number of forms. Adware is software that displays advertisements through pop-ups, bars, or banners. It can watch the sites a user visits while online, then send them ads targeting their interests. Some even report that and other information to its source. Trojan horses look like innocuous programs but like their namesake, they are far more dangerous than they appear. Each program contains a malicious code that can quickly destroy or damage stored data once it is activated. Keyloggers record keystrokes as a user makes on an infected computer then sends the information across the Internet. They can capture any and all information typed in, including passwords and credit card information.

Browser hijackers alter browser settings to take unsuspecting users to undesired web sites. They often change the default home page and search page and can add bookmarks or produce a sudden flurry of pop-up ads. Hijackers frequently include or direct to pornographic or other unsuitable material. Spyware can also include a rootkit, or group of programs designed to

gain control over your computer, or make a backdoor that allows them administrative access. Using this method an attacker can make changes and gather information from your system, then cover their tracks completely. This makes them very hard to detect and leaves your computer open to a wide range of other attacks.

Piggybacking, or riding in on programs you intentionally download, is yet another way spyware gets in. End User License Agreements (EULA) can add to the problem by confusing users and fooling them into compliance. Often when you download a program you are presented with an generally a small window that lists all of the fine print that you must agree to before installing the software. These lists of rules and regulations can be extremely long. For example, the peer-to-peer file-sharing program Kazaa sports a EULA with more than 5,000 words in it. Some agreements may not even include information about the spyware, instead referring to another document that does talk about it, or even leaving it out completely. The typical EULA is also full of confusing legalese that generally says "you cannot blame us for anything that happens to your computer" in the most complex way possible. In those cases the companies backing them are trying to shift the responsibility to the user. Happily, the FTC is going after companies such as Advertising.com, whose EULA neglected to mention the adware packaged with their SpyBlast program. However there is currently no law requiring actual user approval at all. So a distributor such as behavioral marketing company Claria can show users a 56-page EULA and install their module without bothering to ask for approval. New ways to sneak in spyware are constantly being found and new forms are continually in development. No computer is safe without the proper protection and constant vigilance.

There are currently a number acts before the United States Senate that will provide some level of protection from the malice of spyware if approved, such as the Internet Spyware (I-Spy)

Prevention Act of 2004. I-Spy aims to make accessing a computer without proper authorization or intentionally exceeding authorized access a criminal act punishable by imprisonment. The Securely Protect Yourself Against Cyber Trespass Act, known as Spy Act, would target keylogging and browser hijacking, make all spyware easy to detect and uninstall, and require it to gain explicit user consent before collecting personal data. A third measure is the Software Principles Yielding Better Levels of Consumer Knowledge (SPYBLOCK) Act, which seeks to unmask spyware rather than allow it to install itself covertly, force it to include easy removal options, and forbid malicious installations. Until things such as these are made law, the FTC and other agencies can only catch some of the worst perpetrators and work toward educating the public about the risks that lie in wait.

That still leaves just you and your computer against the enemy. Luckily, there are plenty of products out there for the web-savvy and wary home PC user. Simply running an online search for anti-spyware protection can yield a variety of results. Countless websites claim their products have the best spyware protection available and offer free downloads. Others say the same thing and offer their services and software for a fee. Some anti-spyware detection and removal tools are indeed what they claim, but there are many programs that are just the opposite and cause far more problems than they fix. Aggressive advertising and deceptive names are commonplace for these malicious utilities. For example, Scumware-Remover hijacks the browser home page and HOSTS file and Ultimate Cleaner is supported by adware. SpyBlast is one of many whose distributors have faced prosecution by the FTC. Only careful research in combination with reliance on trusted sources can help you to protect your computer and your privacy. Which this brings up the all-important issue of figuring out how to choose which products and manufacturers to place your trust in.

A good place to start your search for home PC protection against spyware is the Online OnGuard web site (http://onguardonline.gov/index.html). This user-friendly, multi-media enriched page offers an assortment of computer security information and a listing of recommended anti-spyware programs and tools. Another good resource is The Spyware Warrior Guide to Anti-Spyware Testing (http://spywarewarrior.com/asw-test-guide.htm), which not only features worthwhile programs, but also has an extensive listing of fakes. Just about any magazine devoted to PC information, health, or security, such as PC Magazine or InfoWorld should carry reviews and advice. The following programs are just a few of the most popular and commonly listed by legitimate sources, but it is important to remember that the absolute best protection possible involves more than just choosing the best program. Once you have anti-spyware on your computer, be sure to use it and keep it up-to-date. Some programs offer upgrades, others offer new spyware definitions to be downloaded on a regular basis. Though research is ongoing and comprehensive, no single product can offer a 100% spyware-free guarantee. Layering, or using two or more different programs on a single PC, can provide much protection than a even the best program running alone. If there is an attack or suspicious trace that one fails to catch, the others may still spot it. This greatly improves the chances of keeping your system safe and clean, particularly when at least one runs real-time detection.

Ad-Aware SE (www.lavasoft.com) is recommended by a variety of sources, including The Spyware Warrior Guide and OnGuard Online. This Lavasoft creation won the Best Internet Enhancement at the 2005 SIAF People's Choice Awards and Shareware Industry Conference and has a history of success. The program allows users to remove various forms of spyware, including adware and keyloggers.

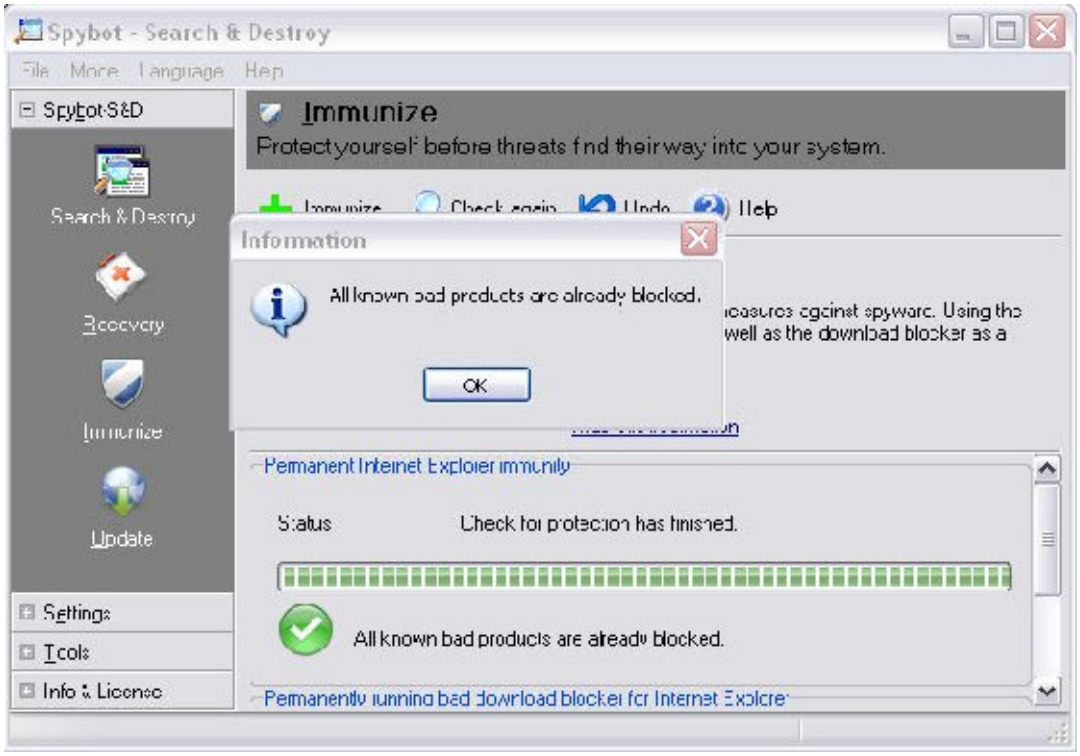
Screen shot taken November 23, 2005 on home PC showing item missed by both Spybot – S&D and Microsoft AntiSpyware Beta.

When Ad-Aware detects problems it provides links to after successfully completing a scan, Ad-Aware Plus displays a detailed summary of all problems found and provides links to sites such as Threat Assessment Chart (TAC), which offer more information on individual threats. Other features include cookie and pop-up blocking and start-up registry locking. The Plus and Professional editions, which retail at $39.95, provide the benefit of real-time blocking called the Ad-Watch module. Ad-Watch works proactively to detect known and unknown spyware and stop it from infecting your computer. According to PC Magazine, however, the program misses some incoming threats completely, or reports them but still allows some spyware programs to slip through. In addition, there are items that the scan fails to detect. In spite of these problems, Ad-Aware remains one of the most popular anti-spyware utilities and Lavasoft is continually releasing newer and better versions.

Spy Sweeper (www.webroot.com) is produced by Webroot Software, Inc. and retails for $29.95. According to their website the program identifies new threats quickly to stay ahead of the game with spyware detection. Comprehensive Removal Technology (CRT) targets hard to remove spyware, taking them out in one run. For continual protection its Smart Shields prevent incoming spyware infections. These shields target specific weak points such as toolbars, hijackers and Active X installation. Spy Sweeper lists all threats found during a scan and includes an indication of the threat-level along with the registry location of all traces, as well as additional online information. Webroot provides up to four Spy Sweeper upgrades each year for subscribers and also offers extensive free support for their clients. In addition, current spyware threat news is offered through the program itself and an overview of detected spyware is readily available. PC Magazine calls Spy Sweeper 4.5 the "most powerful anti-spyware tool" on the market and has named it Editors' Choice. It has been given the Smart Choice Award by Smart Computing and received praise from IEEE Software magazine and PC World as well. Both the Active Shields and CRT held up to their tests, detecting all eleven spyware programs and four keyloggers used in the trial. It successfully removed all but two programs and one keylogger. Spy Sweeper was able to prevent or partially disable three out of four keyloggers that tried to attack a clean PC. The program can also scan deeply enough to detect rootkits and run some features in Windows Safe Mode.

Spybot - Search & Destroy (http://spybot.safer-networking.de) is an extremely popular free anti-spyware program made by PepiMK Software. It is a past winner of the PC Magazine Editors' Choice and the PC World Class Award, and has been recommended by CNet and the Wall Street Journal. Spybot - S&D offers an online tutorial and runs on installation, allowing the user to set a system restore point and make immediate updates to the definitions and help files.

Removed items are quarantined and can be easily replaced if needed. The program offers rapid scanning and does a thorough job at removing detected problems. It also provides a wide range of tools for advanced users, including a Browser Help Object (BHO) management utility, running process list, Internet explorer security and startup options, and secure data shredding. It can also be used to clean the registry of inactive Windows installations when run from a Windows Pre-installation Environment boot CD. All of the frequent updates are free and tech support is available on their website.



Screen shot taken November 17, 2005 on home PC.

On the negative side, in the most recent review by PC Magazine, the utility rates poorly in real-time protection. It uses Immunize to prevent ActiveX controls, SDHelper to block out websites that are known to be bad and the TeaTimer function works to stop hijackers, startup changes and other events. However, each instance is marked by a window that halts all action and asks the

user to allow or deny the change or addition. The window simply lists the change without giving the source. During testing by the magazine, Spybot failed to block a number of scans even when told to. The program is recommended as a backup to a more proactive utility.

WinTasks (http://www.liutilities.com) is a process viewer from Uniblue Systems, formerly LIUtilities, and retails at $29.95. It functions as an improved version of the Windows Task Manager, listing background processes and providing detailed information about each one and access to search the process library database. The program also displays system information and view both friendly and executable names for running processes. It provides a way to close numerous windows with a single click, which can prove useful in fighting pop-up windows. WinTasks provides access to delete the registry entries of unwanted programs and has enable and disable options that allow users to reverse changes in startup settings. Users can easily identify and remove spyware and other malicious items, as well as unnecessary processes that slow bootup time and affect performance. There is an option to stop an unwanted process and another to prevent it from ever running again, plus a list setting that will allow only specified processes to run. The program has won an Editors' Choice Award from CNet.com, which calls the Professional version a "true Windows performance-enhancement utility." WinTasks was also named Editors' Choice by ZDNet.

Acronis Privacy Expert Suite 8.0 (http://www.acronis.com) is made by Acronis Inc. and provides both scanning and real-time protection against spyware. This comprehensive program costs $29.99 and was a PC Magazine Editors' Choice for two consecutive years. It can erase traces of browser and system activity, block pop-ups, and securely shred or destroy deleted data. Users can use the Expert Suite to analyze startup processes, detect and remove a wide range of spyware. It offers a fast Smart spyware scan that focuses on places past infections were found,

and a much slower deep scan that searches all files. During tests run by PC Pro, Expert Suite performed well although it repeatedly reported finding and repairing a non-existent virus. The program is only compatible with Internet Explorer and similar browsers such as AOL. Another possible issue for the novice user is the success of the data destruction feature; any files or programs accidentally wiped will be gone for good.

McAfee AntiSpyware (http://www.mcafee.com) is made by the McAfee Inc. and uses a system called On-Access to block pop-ups and fight spyware. It is priced at $29.99, is available by itself or as part of the McAfee Internet Security suite, and has received the West Coast Labs' Checkmark certification for spyware protection. The program is user-friendly and launches with a summary of past spyware and anti-spyware activity. It can also be used to improve the performance of your computer by taking out resource-hogging programs and thoroughly cleaning all traces of removed programs. In addition, McAfee AntiSpyware has privacy saving features including temporary Internet file, browser history, and cookie removal. Another noteworthy feature is Auto Protect, which scans each program that starts on your program to insure that it is spyware-free. This background process prevents the need to run regular system scans. It also allows users to uninstall spyware programs through the utility rather than with their own uninstallers, making the process quick and easy. As with most of these programs, McAfee AntiSpyware found the majority of spyware when tested, but failed to find some hidden components.

CounterSpy (http://www.sunbelt-software.com) is made by Sunbelt Software and is priced at $19.95. This product obtains its threat updates from the company research team, Microsoft's spyware researchers and users, who are part of what is called the ThreatNet Community. It uses a technology called DNR, or Do Not Resuscitate, to heighten the odds of

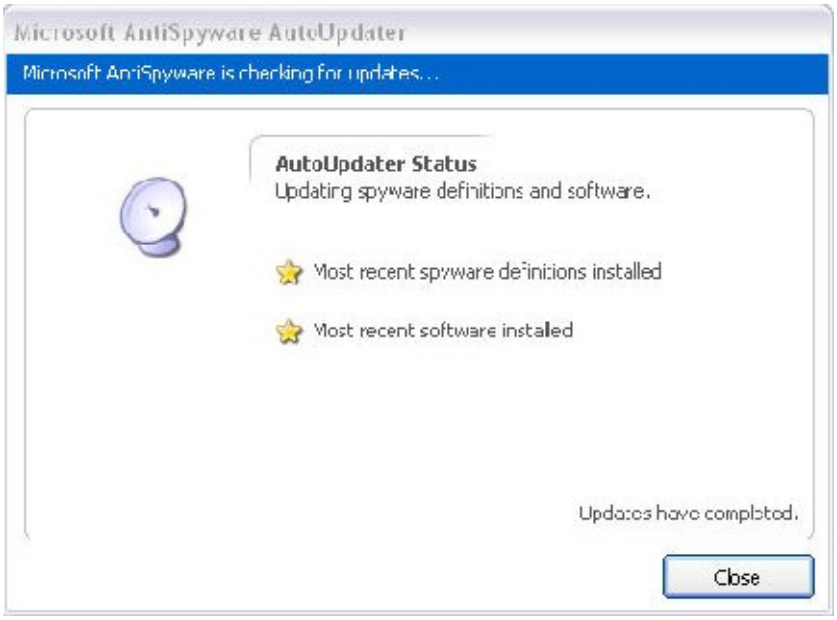
keeping deleted spyware from reinstalling itself. Full system scans and .zip file scanning options are available and CounterSpy uses Active Protection to prevent new spyware infections. It can also erase Internet tracks and modify BHO settings, and comes complete with a secure data deletion ability. In a recent test done by PC World, CounterSpy was rated 95% effective and removed 96% of the spyware components. It did allow ISTbar toolbar, a known hijacker, to be installed then add itself to the registry and run on the test system. The program was later able to detect and remove ISTbar. CounterSpy has been recommended and is also sold by Dell Inc. This year it has won both the PC World Best Buy and World Class Awards, as well as the Editors' Choice Award for Laptop Magazine.

Microsoft AntiSpyware Beta (http://www.microsoft.com/spyware), also known as Windows AntiSpyware Beta, was released by Microsoft following their acquisition of Giant Software Company and its Giant AntiSpyware program. For now it is free to download and update.

Screen shot taken November 21, 2005 on home PC.

The program detects and removes spyware and according to the website offers proactive protection that guards against new spyware infection in fifty ways. As this utility is a beta version, it is still under development and carries a number of faults, including a slow scan time.

However the price and features make it worth running as a layer in your anti-spyware regimen. In an early test run by PC Magazine it removed two-thirds of the spyware on a the test computer. It also blocked more than half of the attempts to infect a clean test PC. While these numbers are less than wonderful, program updates since that time have been definite improvements, providing better detection and removal, more support and better update delivery. On the plus side, MS Antispyware offers detailed threat information including threat ratings and color-coded warnings. Users can choose which action to take for flagged items, from removal to permanently ignoring them and even schedule the program to run daily scans. Each copy of MS Antispyware comes with an expiration date and needs to be upgraded to the newest version in order to be extended. The program also includes an automatic update feature to download recent spyware definitions, as well as advanced features and settings.



Screen shot taken November 21, 2005 on home PC.

Sources

America Online and the National Cyber Security Alliance. (2004). AOL/NCSA Online Safety Study.

Ames, Wes. (2004). Understanding Spyware: Risk and Response. *IT Professional, Vol. 6, No. 5*, 25-29.

Gottesman, Ben Z. and Konstantinos Karagiannis. (2005). Ad-aware SE Plus 1.05 review by PC Magazine. Retrieved November 12, 2005 from http://www.pcmag.com/article2/0,1895,1830047,00.asp

Harrison, Warren and Terry Bollinger. (2004). User Confidence – and the Software Developer. *IEEE Software, Vol. 21, No. 6*, 5-8.

Howes, Eric L.. (2005). The Spyware Warrior Guide to Anti-Spyware Programs: Feature Comparison. Retrieved November 11, 2005 from http://spywarewarrior.com/asw-features.htm

Howes, Eric L.. (2003-2005). The Spyware Warrior List of Rogue/Suspect Anti-Spyware Products & Web Sites. Retrieved November 11, 2005 from http://www.spywarewarrior.com/rogue_anti-spyware.htm

Landesman, Mary. (2005). Spyware Stoppers Still Improving. Retrieved November 15, 2005 from http://www.pcworld.com/reviews/article/0,aid,121411,pg,1,00.asp

Lee, Younghwa and Kenneth A. Kozar. (2005). Investigating Factors Affecting Adoption of Anti-Spyware Systems. *Communications of the ACM, Vol. 48, No. 8.*

Mendelson, Edward (2002). WinTasks 4 review by PC Magazine. Retrieved November 20, 2005 from http://www.pcmag.com/article2/0,1895,663,00.asp

OnGuard Online – Spyware. (2005). Retrieved October 16, 2005 from http://onguardonline.gov/spyware.html

Rubenking, Neil J. (2005). Microsoft AntiSpyware Beta 1 review by PC Magazine. Retrieved November 13, 2005 from http://www.pcmag.com/article2/0,1895,1749938,00.asp

Rubenking, Neil J. (2005). Spy Sweeper 4.5 review by PC Magazine. Retrieved November 15, 2005 from http://www.pcmag.com/article2/0,1895,1879983,00.asp

Schultz, Keith. (2005) Sticking It to Spyware. *InfoWorld.com, Sept. 19, 2005 edition*, 20-24, 28, 30, 38, 40, 44, 46, 48, 50.

Thomas – Library of Congress. (2005). Bill Number H.R.2929. Retrieved November 4, 2005 from http://thomas.loc.gov/cgi-bin/bdquery/z?d108:h.r.02929:

Thomas – Library of Congress. (2005). Bill Number H.R.4661. Retrieved November 4, 2005 from http://thomas.loc.gov/cgi-bin/query/z?c108:H.R.4661:

Thomas – Library of Congress. (2005). Bill Number S.2145. Retrieved November 4, 2005 from http://thomas.loc.gov/cgi-bin/query/z?c108:s.2145: -- SPYBLOCK Act

Weiss, Aaron. (2005). Spyware BeGone! *NetWorker, Volume 9 , Issue 1,* 19-25.

Winder, Davey. (2005). Product Reviews: Acronis Privacy Expert Suite 8. Retrieved November 15, 2005 from http://www.pcpro.co.uk/reviews/76254/acronis-privacy-expert-suite-8.html