Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

A Discussion of Spyware

We have secured our networks, implemented "defense in depth", enforced strong passwords, and educated our end users to report any suspicious files or activity on their computer. We have our firewall and intrusion detection systems in place. We are on top of patch management and security templates have been created and deployed. Current virus signatures are pushed out to the workstations. Then, spyware has appeared. The insidious nature of spyware combined with the lack of user awareness and spyware's potential for surv...

Copyright SANS Institute
Author Retains Full Rights

AD
CounterTack
Counter Tack Active Monitoring for In-Progress Attacks
GET THE WHITE PAPER NOW >>>

Patria Leath
GIAC Security Essentials Certification (GSEC)
Option 1, Version 1.4c
November 2, 2004

A Discussion of Spyware

Abstract

Spyware is becoming a problem that is consuming more time and resources and posing threats to individual and corporate privacy. Network security professionals need to be aware of this emerging threat, understand how it operates, what can be done to avoid it. We need to work with our users to increase their awareness of spyware and ways to practice "safe computing".

We have secured our networks, implemented "defense in depth", enforced strong passwords, and educated our end users to report any suspicious files or activity on their computer. We have our firewall and intrusion detection systems in place. We are on top of patch management and security templates have been created and deployed. Current virus signatures are pushed out to the workstations. E mail is scanned as it arrives. Just when we thought we had it covered, spyware emerges as "the next big thing". Spyware represents a significant threat to computing and networking, ranking right up there with spam, worms and virus attacks as potential security risks. The insidious nature of spyware combined with the lack of user awareness and spyware's potential for surveillance, data gathering and system hijacking pose a threat to home users and businesses. Commercial interests, the technology industry, consumers and legislators must combine efforts to address this threat. Networking security professionals must stay informed and continue educate their users.

In the 80's we began to be concerned about virus attacks to our systems. Initially the viruses would alter files, consume resources or wipe the hard drive of the infected computer. Certainly not admirable activities and outcomes ranged from a mild nuisance to quite disruptive. In the 90's network and computer security staff moved from encouraging the use of anti virus software to requiring it. We increased our efforts in educating users in the practices of "safe computing" and many companies started providing anti virus software for use on home computers in the interest of self defense. Macro viruses and worms appeared wreaking more havoc with workstations, networks and users. The combination of user education (for some users experience was the best teacher) and more sophisticated and user friendly anti virus software assisted the network professionals in addressing the threats. In 1999 the Melissa virus infected

© SANS Institute 2005 Author retains full rights.

computers and emailed word documents to the first fifty addresses in a user's Outlook address book. In 2000 the "I Love You" virus infected computers and sent username's and passwords back to the virus' author. This may have marked a new level of potential for damage and disruption by virus and worm attacks. It also marked increased vigilance and remediation on the part of computer security professionals in the areas of addressing vulnerabilities and security holes.

As we gain experience, we begin to feel more confident. Broadband connections become more available. More and more individuals and businesses are "on-line". More information is being transmitted and exchanged over the internet. The security issues and opportunities for malfeasance increase in magnitude. For many the internet is no longer optional, it is a lifeline.

In the late 90's many individuals were concerned about "cookies" and the threat that they posed to our privacy. Cookies were developed by web designers to identify users and are stored as text files by the browser. Information passes between the browser and the web server each time a page is requested from that server. Cookies permit personalized content and are necessary for applications such as shopping baskets to function successfully. They enhance the web surfing experience by permitting personalized content. Cookies come in two "flavors", session cookies and persistent cookies. Session cookies, also known as transient cookies, reside in temporary memory and are discarded when the browser is closed. These cookies store session identification and do not collect and store information about the user once the browser is closed. Session cookies are primarily used to assist with navigation of websites and the retention of preferences as the surfer moves between pages. Persistent or permanent cookies are set with an expiration date and are stored on the user's hard drive until 1) it expires or 2) the user deletes the cookie. A permanent cookie may be used to collect information about a user's Web surfing habits.

Initially cookies were advertised to identify the computer, not the user, and were described as tools to permit websites to provide customized content. A unique identifier is stored in the user's web browser, identifying the user on return visits to a site. Browsers may be configured to disallow cookies or to require permission each time a site wants to deposit a cookie. However, disabling cookies makes it difficult if not impossible to visit certain sites and users easily tire of granting permission each time s/he receives a request to deposit a cookie. It did not take long for retailers and "marketeers" to recognize the value of cookies for delivering targeted advertising, customizing content and retaining user account information. The Amazon website is a terrific example of customized content and ease of use. Users appreciate the convenience that cookies provide.

Privacy advocates justifiably raised concerns about cookies from the beginning. Fortunately they keep marketing firms such as Double Click on their "watch list".

© SANS Institute 2005 Author retains full rights.

An example of actions as a result of their vigilance was the heightened concern about privacy violations in 1999 when it was made public that Double Click intended to cross reference the data it had collected on consumer behavior with an offline consumer database that it had recently acquired. This would have permitted the linking the identities of specific individuals with web surfing and purchasing habits. "Marketeers" saw a potential goldmine. Privacy advocates jumped on the case and the Electronic Privacy Information Center filed a complaint with the FTC. (Fusco, 2004). Double Click, eager to retain its competitive advantage and to restore its credibility, countered with several privacy initiatives while reminding privacy advocates that the option to "opt out" always existed. Today a user can visit the Double Click website and review their privacy practices, information that is collected, a description of how they claim it is used and exercise the option to "opt out" of data gathering.

It is 2004 and the onslaught of viruses, Trojans, and worms has been joined by spyware and adware. For individuals concerned about the threats to privacy posed by cookies, spyware and adware have raised another red flag. There is a fine line between adware and spyware. Spyware is defined as "any technology that aids in gathering information about a person or organization without their knowledge" (http://searchcrm.techtarget.com). Spyware usually comes in the form of a cookie and is designed to secretly gather information about the user and/or the computer and to send it to an information collection point. Some spyware has the ability to install keystroke loggers. If we are discussing only adware, the information is generally sent to advertisers to permit them to target marketing efforts. However, it could cross the line to spyware and the information it collects could be sent to any "interested" party, and they may not have the most honorable of intentions. There may be legitimate uses for spyware, such as parent's installing it to track children's web surfing activities or employers concerned about employee activities. "Evil Doers" could install it on computers to harvest information and to capture passwords, financial account information and other information that could be used for identity theft or corporate espionage. Clearly not a legitimate use.

Adware is generally considered to be a variety of spyware. Adware appears on the computer as advertising banners or pop-up windows and may direct the user to a specific website. The application may track the surfing habits of the user and target specific marketing campaigns to that user. Proponents of adware defend its use as a cost recovery measure that ultimately helps hold down the costs for the user. These proponents maintain that the user has agreed and granted permission to the installation of the adware by clicking on a button in a pop up window or agreeing to an End User License Agreement (EULA). Privacy advocates maintain that EULA's have become so devious with their fine print, burying the real intent in such convoluted and hidden language that it is not comprehended by the average user. Users are used to agreeing to licensing agreements and use of the software that they just click through the agreement not realizing that they may have just agreed to the transmission of personal

© SANS Institute 2005 Author retains full rights.

information on a continual basis or that they may have given permission to install additional applications on their computer. There is a good discussion of this on the Gibson Research Corporation website at http://grc.com/oo/fineprint.htm.

For the purpose of this discussion spyware and adware will be considered synonymous. And adware should not be confused with Ad-Aware, the commercially available spyware removal software developed by Lavasoft.

Spyware installs itself on a computer in a number of ways. Perhaps the user has agreed to a EULA that accepts the spyware in the fine print. Perhaps the user has clicked on a button in a pop up window, either consciously or unconsciously agreeing to something. Or, perhaps the user is the victim of a "drive by down load". Drive by download describes a program that is automatically downloaded to a computer without the user's knowledge or consent. It may be initiated by visiting a website or viewing an HTML email message. However the spyware manages to get itself installed on the computer, it proceeds to modify the operating system, alter the registry settings, install services and execute applications. All of this is done surreptitiously, without the user's knowledge. Perhaps it will be discovered.

Adware may have implied permission, but the secretive nature of its activities groups it with spyware. Steve Gibson of Gibson Research Center further defines spyware as "any software which employs a user's Internet connection in the background (the so-called "backchannel") without their knowledge or explicit permission. Silent background use of an Internet "backchannel" connection must be preceded by a complete and truthful disclosure of proposed backchannel usage, followed by the receipt of explicit, informed, consent for such use. Any software communicating across the Internet absent these elements is guilty of information theft and is properly and rightfully termed: Spyware." (http://grc.com/optout.htm) Gibson's definition of spyware encompasses both the loss of privacy and the unauthorized use of computer resources. According to the Counterexploitation website (www.cexx.org) spyware is not limited to transmitting demographic data and websurfing information. It is also capable of viewing and recording transactions as they are processed and retrieve data and other information stored on the hard drive. Other spyware applications will collect data and then "phone home" with the information.

Not only does spyware surreptitiously reside on the PC, many spyware applications resist removal or deletion from the computer. Some spyware rebuilds itself each time it is uninstalled. If the user is able to remove the spyware, the application that it was installed with may fail to run. There are certain programs that claim to be spyware removal tools that actually are spyware programs themselves and use this ploy to become established on a computer. The unsuspecting user installs one version of spyware thinking that s/he is removing malware. Generally this is delivered via a pop up that announces "Spyware has been detected on your computer…click here to remove

© SANS Institute 2005 Author retains full rights.

it". www.cexx.org is a helpful website that includes a listing of known spyware programs and the specific tools and applications that may be used to remove specific types of spyware. Spyware is similar to other types of malware with the remediation lagging behind the introduction of the threat. Companies such as Webroot, Lavasoft and PestPatrol attempt to keep up with the "Evil Doers" but must first detect the signature before developing the counter measure. Unlike anti virus software, real time detection is not as critical for spyware. However, it is important to scan and remove installed spyware and to make the best attempt to block further installations. Firewalls are not effective in blocking spyware since a user generally, albeit unwittingly, invites the spyware into the machine. At this time, the most effective defense is an anti-spyware program installed on the desktop.

The presence of spyware on a computer may be extremely difficult to detect until it affects system performance. A recent study by AOL and the National Cyber Security Alliance had some interesting results. Users in more that twenty two cities were interviewed and their computers were examined. 90% indicated that they had heard of spyware but only 53% thought that they might have spyware on their computer. Scans found spyware on 80% of the computers. The average number of spyware components found on a computer was 93, with the highest number being 1,054. Approximately 40% of the users indicated that their computer had symptoms of a spyware infestation, i.e. their browser or search engine was redirected, etc. (AOL/NCSA On line Study, 2004). Another study conducted by Dell Computers and the Internet Education Foundation as a part of the Computer Spyware Initiative found that over 90% of the computers have spyware and, again, users are unaware and unable to remove it (Press Release, 2004). On the basis of these studies it would be safe to say that the majority of users are unaware of the presence of spyware on their computer and unsuspecting of the threat posed by spyware.

In addition to compromising privacy and the potential for identity theft for individuals, the threats and costs to businesses must be considered. Most businesses do not monitor employees' internet surfing and pop up windows and outbound TCP/IP traffic is not restricted. Spyware can just as readily be installed on a corporate computer as it can be on a home computer. (One could hope that there is increased security awareness in a business setting). Just as spyware applications can collect personal information from home computers it can collect both personal and corporate information from businesses. In some cases, businesses might be more lucrative targets.

Spyware is also taking its toll with computer support vendors. Dell reports that spyware is the culprit in 12% of the support calls in the hardware division and Microsoft feels that half of the computer crashes reported by customers is caused by spyware (Zaney, 2004). The cost of dealing with these customer support issues not only cuts into the company's profit, but eats into the customer's productive time as well. The customer is not limited to the home

© SANS Institute 2005 Author retains full rights.

user, the corporate user and the corporate technical support staff also expends time and effort in dealing with spyware. All of this is non productive time and a waste of resources, and additional costs to businesses.

Companies and individuals are fighting back. In addition to suing adware firms and the advertisers directly, there are proposed regulations in Congress. Bills have passed in both the Senate and the House of Representatives aimed at regulating spyware. The House passed the SPY ACT (Securely Protect Yourself Against Cyber Trespass) bill by a 399-1 vote and it makes computer technology that downloads programs onto users' computers without their permission illegal. It also makes it illegal to download personal information, modify personal setting, hijack a user's computer and to present pop up ads that cannot be closed. A similar bill, the SPYBLOCK (Software Principles Yielding Better Levels of Consumer Knowledge) Act has been introduced in the Senate. This bill would outlaw the installation of software on a computer without the user's consent. It would also require a reasonable "uninstall" procedure for all downloadable software since some spyware is nearly impossible to uninstall. The proposed laws would make distributing spyware a criminal offense and would be enforced by the Federal Trade Commission. And, although they would only apply domestically and many of the "Evil Doers" are thought to be off shore, proponents intend that these laws serve as a model to the international community.

It should not be surprising that the technology industry is not in favor of this legislation and prefers self regulation. This may be some of the momentum behind the some of the efforts of organizations such as the Internet Education Foundation (www.neted.org), which describes itself as "a 501(c)(3) non-profit organization dedicated to educating the public and policymakers about the potential of a decentralized global Internet to promote democracy, communications, and commerce." Board members include individuals from Microsoft, AT&T, AOL Time Warner, and VeriSign. The organizations efforts include educational projects aimed at educating consumers and legislators. They strive to "assure informed policy making on internet related issues". The National Cyber Security Alliance (www.staysafeonline.info/) is another not-for-profit 501(c)(3) organization. They are a public private partnership with sponsorship by the FTC, the Department of Homeland Security and "many private sector organizations". They state a goal of providing cyber security awareness and education to small businesses, educational institutions and to the home user. Supporting organizations include AOL, Cisco, Hewlett-Packard, Symantec, and Dell, among many others.

The industry is making effort towards self regulation, consumer and legislator education. One project in the works is P3P, the Platform for Privacy Preference Project by the WWWConsortium. P3P has the goal to develop a standard for a browser feature that will analyze a website's privacy policy towards handling personal information and compare this to the consumer's preferences that have

© SANS Institute 2005 Author retains full rights.

been set in the P3P enabled browser. Theoretically it would provide consumers with knowledge and provide tools to address the manner in which websites are handling personal information. Additionally, some businesses have adopted a policy of not doing business with companies that use adware or pop ups for advertising. Wells Fargo and Major League Baseball are two businesses that have announced that they will not deal with adware and forms of pop up advertising (Zaney, 2004).

Whether the controls are legislated by the government or self regulated by the industry and the market place, it is clear that something must be done and any solution will encompass the education of the user. The studies cited above suggest that there is a lot of ground to be covered in effectively educating users about spyware and its dangers.

The first step in user education is increasing their awareness that spyware exists and familiarizing them with the ways that spyware propagates and the danger that it poses. The next step is educating them in the signs and symptoms of a spyware infestation. According to the Cyber Security Tip ST04-016 from US-CERT (www.us-cert.gov) the following symptoms may indicate that spyware is installed on a computer:

- Endless pop up windows
- Redirection to websites other than what is typed in to the browser
- Unexpected tool bars appear in web browser
- Home page is changed
- Default search engine has changed
- Certain keys fail to work, e.g. the tab key
- Random error messages appear
- Computer is sluggish when opening programs or processing tasks.

This bulletin also provides guidance on avoiding the unintentional installation of spyware on a computer by observing the following:

- Avoid clicking on links within pop up windows and to close the pop up window by clicking on the “X” icon in the titlebar, not the “close” button.
- Choose “no” when an unexpected question appears
- Be wary of free software
- Be cautious of links that offer anti-spyware software. Frequently these links may actually install spyware on the computer.
- Adjust browser preferences to limit pop up windows and cookies. Privacy settings may be adjusted to permit cookies for the website that is being visited.

The complete bulletin is available at: http://www.us-cert.gov/cas/tips/ST04-016.html and also provides recommendation for the removal of spyware.

© SANS Institute 2005 Author retains full rights.

As a network security professional we must continue to work with our users and educate them about the presence and danger of spyware and to encourage them to "just say no!" and to adopt the following guidelines:

- Don't click on email attachments unless they are expecting them. Call the sender and verify that they sent it.
- Don't believe the return address on an email. Call the sender and verify that they sent it.
- Don't believe the message. If they get an unsolicited message indicating that they have spyware, just click here to install anti spyware software, they could unwittingly install spyware.
- Don't download browser code.
- Just say "no" or hit the "X" when asked an unexpected question.

Do not underestimate the value of actually sitting down with some of the more challenging users. Frequently time spent one on one, assessing a user's knowledge level and addressing his or her individual concerns can be time well spent. This may also provide insight into potential future problems. Continued user education and communication should compliment technology.

A discussion in the October 22, 2004 newsletter at www.spywareinfo.com raises some good questions about the new Google search tool, Google Desktop Search. The author raises the question about whether or not it is spyware. (Spyware Info, 2004) According to the author, Google Desktop is able to search the contents of every file on a hard drive, including another user's private folders. The application also collects information on the machine on which it is installed. It creates a unique id, communicates with Google over the internet and uses the same cookie that is set by google.com. The potential exists to associate disparate sources of information processed through Google searches and services. It also installs a backdoor with an auto updater that cannot be disabled. I agree with the author that this sounds a lot like spyware. The program does have a clearly written and understandable privacy policy. The policy describes what information it collects and how it will handle it. It also provides instructions on how to protect files from indexing and display. The program may also be uninstalled at any time through the "Add or Remove Programs" feature of the operating system.

Google Desktop Search has all of the features of spyware. It also incorporates the features that the technology industry proposes to incorporate into software as a part of its efforts towards self regulation instead of legislative solution. It is not designed to be spyware, but in the wrong hands it could be used as spyware. This provides another situation for user education, both in the areas of appropriate use and the potential dangers of the software.

Spyware is becoming a problem that will be consuming more time and resources. The proliferation of spyware programs over the past year has been linked to

© SANS Institute 2005 Author retains full rights.

organized groups using these programs to steal data for identity theft or extortion and to hijack machines for denial of service attacks (Roberts, 2004). We must remain vigilant, be aware of developments in the technology industry and continue to educate our users. We cannot afford to become complacent if we want to keep the internet a safe place for business, education and information.

References

"AOL/NCSA Online Safety Study, conducted by America Online and the National Cyber Security Alliance" October 2005. http://www.staysafeonline.info/news/safety_study_v04.pdf. (accessed 26 October 2004).

Brain, Marshall. "How Internet Cookies Work". http://computer.howstuffworks.com/cookie1.htm (accessed 25 October 2004).

Fusco, Patricia. "The Way the Cookie Crumbles". ISP-Planet. 16 February 2004. http://www.isp-planet.com/politics/cookie_crumbles.html (accessed 26 October 2004)

"Internet Education Foundation, Dell Launch Consumer Spyware Initiative". Press release 15 0ctober 2004. http://www1.us.dell.com/content/topics/global.aspx/corp/pressoffice/en/2004/2004_10_15_dc_000?c=us&l=en&s=corp#tn2. (accessed 26 October 2004).

"Is New Google Software Spyware". Spyware Weekly Newsletter: October 14, 2004. www.spywareinfo.com/newsletter/archives/1004/22.php (accessed 26 October 2004).

Jesdanun, Anick. "Sneaky Spyware becomes the Scourge of the Internet". Yahoo news. 31 October 2004. http://news.yahoo.com/news?tmpl=story&cid=562&u=/ap/20041031/ap_on_hi_te/tangled_in_spyware&printer=1 (accessed 31 October 2004).

Kumler, Emily. "Spyware's Victims Spread." PCWorld. 19April 2004. http://www.pcworld.com/news/article/0,aid,115735,00.asp (accessed 25 October 2004).

McDowell, Mindi and Lytle, Matt. "Recognizing and avoiding spyware, Cyber Security Tip St04-016". 2004. http://www.us-cert.gov/cas/tips/ST04-016.html (accessed 25 October 2004).

© SANS Institute 2005 Author retains full rights.

Martin, Richard. “Spy vs Spy”. Fortune Small Business. 28 April 2004. http://www.fortune.com/fortune/smallbusiness/technology/articles/0,15114,614397,00.html (accessed 25 October 2004).

Martin, Richard. “How Spyware Attacks”. Fortune Small Business. 28 April 2004. http://www.fortune.com/fortune/smallbusiness/technology/articles/0,15114,614390,00.html (accessed 25 October 2004).

Metz, Cade. “Spy Stoppers.” PC Magazine. 2 March 2004. http://www.pcmag.com/article2/0,1759,1524249,00.asp (accessed 25 October 2004).

Moore, John. “Arming Against Viruses, Security Community Members Try to Keep up with Constantly Changing Threats.” 16 August 2004. http://www.fcw.com/fcw/articles/2004/0816/feat-arming-08-16-04.asp (accessed 25 October 2004).

Roberts, Paul. “New Trojan program squased adware”. 6 October 2004. http://www.computerworld.com/securitytopics/security/holes/story/0,10801,96455,00.html (accesses 27 October 2004).

http://searchcrm.techtarget.com (accessed 25 October 2004).

“The Trouble with Spyware and Advertising Supported Software.” http://www.cexx.org/problem.htm (accessed 26 October 2004).

Zaney, Kevin. “Corporations Must Join the Fight Against Adware Menace”. 18 October 2004. http://www.computerworld.com/managementtopics/management/story/0,10801,96604,00.html. (Accessed 25 October 2004).

Resources

www.spywareguide.com: an online guide to spy and anti spy software

http://grc.com/oo/news.htm: a website with information and links providing information on privacy and spyware.

http://www.us-cert.gov: an online resource providing guidance on preparation of computer systems and responses to threats.

© SANS Institute 2005 Author retains full rights.

Last Updated: June 18th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Melbourne 2013	**Melbourne, AU**	**Sep 02, 2013 - Sep 07, 2013**	**Live Event**
SANS Capital City 2013	**Washington, DCUS**	**Sep 03, 2013 - Sep 08, 2013**	**Live Event**
Network Security 2013	**Las Vegas, NVUS**	**Sep 14, 2013 - Sep 23, 2013**	**Live Event**
SANS Canberra 2013	**OnlineAU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**