Global Information Assurance Certification Paper

Spyware

GIAC Security Leadership Certification (GSLC)
Practical Assignment
Version 1.0

Kay Seidner
Submitted April 15, 2004

Abstract: This paper discusses the security threat caused by Spyware, what it is, and how to defend against this threat. Though there is no clear definition for Spyware, there are many definitions for it. The concern over a lack of clear definition has prompted the Federal Trade Commission (FTC) to schedule a public workshop to better define Spyware.[1] Whatever the definition, the threat Spyware poses is real and significant from the point of view of information security and privacy. This paper concludes with recommendations to defend against spyware based on accepted industry best practices.

Introduction

Ad-supported applications, or Adware, have been around for a long time. Adware is software that is supported through a targeted advertising model. That is to say, a vendor agrees to provide advertising through their software and in return, furnishes information to the advertiser such as number of times the ad is accessed by consumers. This defers the development costs of the software product to the advertiser rather than the owning company passing costs on to the consumer.

Generally speaking, adware is considered spyware because it gathers information about the user and their habits, and delivers that information to a third party. So where's the problem? The problem lies in the aggressive and even deceptive nature that some forms of software have taken. Such software is classified as Spyware. This is because spyware can be installed on a computer without the user's knowledge or consent, or without revealing its intent.

How Spyware Works

According to the Webopedia Computer Dictionary, "spyware is any software that covertly gathers user information through the user's Internet connection without his or her knowledge, usually for advertising purposes."[2] Webopedia[3] describes spyware as an executable program that gathers and returns information to its author. These executables have the ability to monitor keystrokes, scan files, eavesdrop on other programs, install other programs, read cookies and change the default browser homepage.

Often, spyware will piggyback on freeware or shareware downloaded from the Internet. If a licensing agreement is provided to the consumer, it may or may not include notification regarding the additional software. The more dangerous the software, the more covertly it is installed.

[1] Federal Trade Commission – Spyware Workshop
[2] Webopedia Computer Dictionary
[3] Webopedia Computer Dictionary

Damages Caused by Spyware

Spyware runs in the background, using memory resources to gather information and network resources to report its findings as it "phones home" via the consumer's Internet connection. Spyware activities can cause system crashes, that famous "blue screen of death," and general system instability. It has also been known to modify system settings, write and delete files, reformat hard drives, install other programs, send and receive cookies to other spyware thus inviting them into your computer, and adding Trojan horses.

Here are some signs that spyware has infected your computer:

- Your phone bill includes charges to 900 numbers
- Unfamiliar sites handle your search requests
- Your protective programs stop working correctly
- New items appear in your Favorites list
- System response time is noticeably slower
- When not working online, your modem blinks as if you're connected to the Internet
- Pop-up advertisements appear when your browser isn't active
- The homepage has been changed

Privacy and Spyware

Spyware is not illegal, yet it can reach your computer without your consent simply through the download of another application. Once on your computer, it can collect information without your knowledge and leave a potential backdoor open for hackers to intercept data and enter your computer. Depending on the aggressiveness of the spyware author, your privacy can be violated or your identity can be stolen.

Concerns and Business Impacts

The Counterexploitation[4] web site identifies several concerns with regard to spyware that include: consumer privacy implications, hostile behavior, potential violations of child protection laws, information security issues and software license agreement violations.

Consumer Privacy Implications

Obviously, there is a privacy concern. Most commonly, this is thought of in terms of private users who can have their information harvested and sold to the highest bidder. There is a privacy issue for business as well. Any business that allows its employees to have access to the Internet can be open to the same potential threat. Not only employee personal

[4] Counterexploitation web site, author unknown. "The Trouble with Spyware and Advertising-supported Software".

information is siphoned off, but also customer information the company is supposed to safeguard is at risk. This could be in the form of corporate trade secrets or customer information covered by the Health Insurance Portability and Accountability Act (HIPAA) that the company is charged to protect. An article in Information Week[5] sited a privacy invasion case where a person installed key-logging software (considered a type of spyware) at several Kinko's Inc. locations, was able to collect customer information, and used that information fraudulently. The costs that could be incurred to businesses go beyond monetary value. Exposed customer information could result in lost customer confidence and cause significant damage to a business's reputation in today's competitive markets.

Hostile Behavior

Hostile behavior occurs when programs stealthily install themselves on a computer, impacting the computer's performance and functionality. For example, activity from malicious spyware can impact network traffic, produce operational errors, or worse yet, disable other functionality when attempting to terminate the rouge program. The impact to business is potential productivity loss from down time of employees whose computers aren't working properly and the costs to repair and reload computers, if necessary.

Child Protection

Child protection is another area where spyware can be a concern. The U.S. Children's Online Privacy Protection Act[6] prohibits the collection of personal information from children under the age of 13 without written consent from a parent or guardian. Most spyware may not be targeted at children, yet the software does not distinguish between child and adult end users when collecting personal information in violation of such laws. For software vendors who produce adware or vendors that bundle adware with their products, this is a business liability they must be aware of. Such vendors may try to provide the appropriate notification to their software users. However, because they may not be certain their users are adults, they must be willing to accept the consequences of actions taken by their product.

Information Security

The security concerns surrounding spyware start when it's installed. Spyware inherits all the privileges of the user who approved the install. With some legacy operating systems, this may be "Administrator" level privilege which provides full systems and resources access. With such a privilege, Spyware can install other programs and change system settings and leave the computer as a prime target for malicious hackers. Hackers who are looking for ways to infiltrate a corporate network can now

[5] Hulme, George V. "Security Threats Won't Let Up". Information Week. January 5, 2004.
[6] Federal Trade Commission - Children's Online Privacy Protection Act of 1998.

leverage this vulnerability created by spyware to steal customer or company information. In today's business environment, such hacker activity becomes a great threat to corporate security—especially when employees use their personal computer for business or connect to the company network via an unprotected access point from home, a hotel or a coffee shop. Many times this is how the spyware slips into the network.

Software Licensing Liabilities

Disclosure of information contrary to software licensing agreements is a serious breach of contract. Normally, when downloading or installing new software, users are asked to read and agree to terms of use in an End User License Agreement (EULA). The statements in the EULA are usually long and verbose, with disclosure liabilities buried in text that is difficult or confusing to read. Some agreements are purposely misleading or lack caution of disclosure all together. Regardless, users will accept the terms of the agreement and move on, not realizing that they've opened the door to disclosure breaches because of spyware. In the business environment, sophisticated contracts are put in place when buying software for a vendor to prevent liabilities from software use in a manner prescribed by vendors. When individuals nonchalantly agree to download software from the Internet, however, they have limited legal recourse available against disclosure liability "signed" via acceptance of an online agreement.

Solutions

Since "more than 78,000 spyware programs are on the loose,"[7] and since, according to Gartner, spyware will get more malicious in the future,[8] the time to proactively look for solutions to ward off spyware is now. To manage spyware threats, businesses can take effective steps that include updating their information security policy, putting in place technical controls and seeking legislative action.

Information Security Policy

Updated information Security Policy is the first line of defense. If a policy is not already in place, one has to be created. It should contain rules for downloading from the Internet or other sources. Procedures should be included for documenting business case and obtaining approval before downloading programs to computers owned by the business.

Many companies already have Security education programs that include awareness of the dangers of downloading and Internet usage policies. What such programs may not include is information on safe surfing of the Internet.

[7] Metz, Cade. "Spy Stoppers". PC Magazine. March 2, 2004.
[8] Radcliff, Deborah. "The Scoop on Spyware". Computerworld. January 28, 2004.

Ian Poynter, chief security officer for Bit9, says, "Keep user education simple,"[9] and outlines four points to follow:

- Don't download anything you're not sure of.
- Don't click on images, no matter how innocent they look.
- Don't download software without following procedure (i.e. follow Internet Usage Policy).
- Don't do anything that isn't business related.

Getting everyone in an organization to understand these simple rules can go a long way.

Technical Controls

Technical methods to mitigate spyware from impacting systems of an organization include:

- Provide a secured connection for telecommuters and traveling associates to work by, such as a Virtual Private Network (VPN) and personal firewalls. "Even the most security-conscious businesses can find themselves at risk if, for example, a mobile user's notebook is infected with spyware and then the user logs on to the corporate network."[10]
- Configure browsers and Outlook using Microsoft domain security policies.
- Filter web content through an HTTP proxy.
- Use firewalls. Intrusion detection, blocking, content filtering and other controls may reduce spyware penetration and can alert you to increased, unexplainable network traffic that may be caused by spyware.
- Use anti-virus software. Antivirus vendors are starting to include spyware detection and removal with their antivirus products.
- Consider segmentation of the internal network. Overall business practicality needs to be reviewed and this will only be helpful to limit the spread of spyware in the event the network gets corrupted.
- Purchase a spyware removal tool for use by your organization. It may not be necessary to deploy to every computer in the organization, but it can be helpful in cleaning up corrupted desktops when all other options have failed to stop the spyware from getting through.

  Many organizations are already employing some of these measures. Some organizations will accept additional measures as the cost of business continuity, while others will fight more security in the environment. How each organization reacts is likely dependent on two

[9] Radcliff, Deborah. "The Scoop on Spyware". Computerworld. January 28, 2004.
[10] Hulme, George V. "Security Threats Won't Let Up". Information Week. January 5, 2004.

factors; cultural acceptance level (or lack there of) or past experience dealing with such a threat.

Legislation

Legislative activity is on the rise. The Software Principles Yielding Better Levels of Consumer Knowledge (SPYBLOCK) Act[11] was introduced in March by Senators Barbara Boxer, Ron Wyden and Conrad Burns. This bill requires dialog boxes giving users a choice to download; requires strict disclosure for creation of pop-ups, collection of information and its distribution over the Internet, or computer setting modifications; prohibits redirection to counterfeit web sites; will be enforced by the Federal Trade Commission (FTC) and the state attorneys general office; and includes provisions for fines and injunctions.

For those in the adware business, this will put more stringent standards in place, making the development and sales environment more complex but in part, protecting them as well as the consumer. For the business consumer, this should reduce unwanted spyware when coupled with the previous solutions, thus making the business environment safer from spyware. But is it enough? There is still the issue of governing the Internet on an international level. If spyware originates outside of the US, can this law be enforced? The good news is that international focus is being given to digital privacy issues. The European Union implemented an Anti-Spam law that covers spyware last October.[12] I believe along with international focus, international enforcement will come in time too.

Additional Strategic and Tactical Steps

Regarding the impact on productivity for businesses, the threat from spyware is similar to that of SPAM, viruses and worms. In the short term, businesses need to be conscious of the spyware threat and take steps to protect their computers and networks. Many of those steps have already been outlined in the form of technical and non-technical methods for mitigating spyware infestation. In the long run, businesses need to take a strategic approach to protect their resources from spyware just as they have to viruses; be constantly learning more about spyware, monitor activity within the network to identify threats early, and keep a mindful eye on development of new technical solutions and upgrade as necessary.

[11] TechWeb News. "Senators Take on Spyware". InternetWeek. March 4, 2004.
[12] The Associated Press. "Anti-Spam Law Goes Into Force in Europe". Information Week. October 31, 2003.

Best Practices to Defend Against Spyware

According to Cade Metz at PC Magazine, "That best way to protect against spyware is to run an application that identifies and removes it."[13] But how does one choose the right product? Research and technical evaluations may reveal the right product to deploy.

First, you have to understand your environment and what kinds of spyware applications have infiltrated your business organization. Does your organization use file-sharing software? Have you found key loggers on your computer? Once you know what you're dealing with, then you can study the many products available in the industry to find those that can best fit your needs.

The next step is evaluation. Test several products to see how well they work in your environment and if they indeed do what they say. Many operate in similar ways to antivirus software by identifying and removing files, folders and registry keys associated with known spyware programs.

Step three is deployment. How you deploy in your organization will depend on need and the cost your organization is willing to incur. Earlier technical controls suggested only deploying as needed when a computer showed signs of infection. This is a conscious decision that needs to be made based on risk assessment. If your organization has a low rate of infestations, then selective deployment may be appropriate. In that case, use spyware removal products to clean up the offenders on specific machines only. On the other hand, if your company has a large number of people who connect through their personal networks or you've already experienced what you consider a high incident rate, full deployment may be the appropriate choice for your organization.

Lastly, monitor your environment. As with viruses, there are constantly new spyware programs being written with new, enterprising ways of intruding. Working closely with the vendor you've chosen for a removal product to provide updated definitions on a regular basis will go a long way to keeping spyware in check.

Summary

Spyware, though less known than SPAM or viruses or worms, has the potential to do just as much damage to individual consumers and organizations. By taking the appropriate steps to protect computers and networks through policy, technical solution or legal action, users and company employees can be equally successful at mitigating the threat that spyware poses.

[13] Metz, Cade. "Spyware – It's Lurking on Your Machine". PC Magazine. April 22, 2003.

References

Federal Trade Commission – Spyware Workshop. URL:http://www.ftc.gov/bcp/workshops/spyware/ (March 22, 2004)

Webopedia Computer Dictionary. URL:http://www.webopdedia.com/TERM/s/spyware.html (March 22, 2004)

Counterexploitation web site, author unknown. "The Trouble with Spyware and Advertising-supported Software". URL:http://cexx.org/ (March 19, 2004)

Hulme, George V. "Security Threats Won't Let Up". Information Week. January 5, 2004. URL: http://www.informationweek.com/story/showArticle.jhtml?articleID=17100340 (March 22, 2004)

Federal Trade Commission - Children's Online Privacy Protection Act of 1998. URL:http://www.ftc.gov/ogc/coppa1.htm (April 4, 2004)

Metz, Cade. "Spy Stoppers". PC Magazine. March 2, 2004. URL:http://www.pcmag.com/article2/0,1759,1523357,00.asp (March 22, 2004)

Radcliff, Deborah. "The Scoop on Spyware". Computerworld. January 28, 2004. URL: http://www.computerworld.com/securitytopics/security/story/0,10801,89489,00.html (March 22, 2004)

TechWeb News. "Senators Take on Spyware". InternetWeek. March 4, 2004. URL: http://www.internetweek.com/allStories/showArticle.jhtml?articleID=18202025 (March 22, 2004)

The Associated Press. "Anti-Spam Law Goes Into Force in Europe". Information Week. October 31, 2003. URL: http://www.informationweek.com/story/showArticle.jhtml?articleID=15800297 (March 22, 2004)

Metz, Cade. "Spyware – It's Lurking on Your Machine". PC Magazine. April 22, 2003. URL:http://www.pcmag.com/article2/0,1759,977889,00.asp (March 22, 2004)

Last Updated: July 24th, 2017

Upcoming Training

SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS New Orleans MGT512	New Orleans, LA	Aug 21, 2017 - Aug 25, 2017	Community SANS
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
Community SANS New York MGT512	New York, NY	Aug 28, 2017 - Sep 01, 2017	Community SANS
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Toronto MGT512	Toronto, ON	Sep 18, 2017 - Sep 22, 2017	Community SANS
Community SANS Columbus MGT512	Columbus, OH	Sep 25, 2017 - Sep 29, 2017	Community SANS
SANS Oslo Autumn 2017	Oslo, Norway	Oct 02, 2017 - Oct 07, 2017	Live Event
SANS Tysons Corner Fall 2017	McLean, VA	Oct 14, 2017 - Oct 21, 2017	Live Event
Community SANS Banff MGT512	Banff, AB	Oct 23, 2017 - Oct 27, 2017	Community SANS
SANS San Diego 2017	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	Live Event
Community SANS Memphis MGT512	Memphis, TN	Nov 06, 2017 - Nov 10, 2017	Community SANS
SANS San Francisco Winter 2017	San Francisco, CA	Nov 27, 2017 - Dec 02, 2017	Live Event
SANS Cyber Defense Initiative 2017	Washington, DC	Dec 12, 2017 - Dec 19, 2017	Live Event
SANS Security East 2018	New Orleans, LA	Jan 08, 2018 - Jan 13, 2018	Live Event
Northern VA Winter - Reston 2018	Reston, VA	Jan 15, 2018 - Jan 20, 2018	Live Event
SANS Miami 2018	Miami, FL	Jan 29, 2018 - Feb 03, 2018	Live Event
SANS Southern California- Anaheim 2018	Anaheim, CA	Feb 12, 2018 - Feb 17, 2018	Live Event
SANS OnDemand	Online	Anytime	Self Paced
SANS SelfStudy	Books & MP3s Only	Anytime	Self Paced