Spyware

Jon Beedle
The University of Southern Mississippi, USA

INTRODUCTION

Spyware is a software program that runs silently in the background draining valuable computer system resources while monitoring the user's activities. Without a security suite or an antispyware software program installed on a user's computer, this security breach is difficult for a user to identify while giving hackers an electronic line of attack in hijacking personal information. Spyware applications can run in the background at boot up, slow the microprocessor with requests, and take up random access memory. Spyware may reset a startup page or redirect your search engine; it may likely produce conspicuous advertising pop-ups each time a browser loads ordinary Web pages (Coustan, n.d.).

BACKGROUND

In one variation, unbeknownst to the user, spyware collects personal information from the user's hard drive and sends this data through the Internet to a Web server. A common function of spyware is reassigning customized popup ads as the startup page to the user's browser. Spyware is often disguised within freeware or shareware applications that can readily be downloaded from the Internet albeit one must read the small print to know. While all freeware and shareware applications will not contain spyware, consumers must be aware of potential dangers. Spyware contains the capability to collect personally identifiable information such as social security numbers, credit card numbers, passwords, and addresses. Like a Trojan horse, spyware secretly installs itself while the unaware user is installing another program. Frequently these undisclosed downloads transpire through peer-to-peer file sharing networks. For example, after installing a freeware program the user begins to surf the Internet. As an unsuspecting user, most do not realize that a spyware program is tracking and recording their Web surfing habits and sending the personal data back to a third party programmer or Web server. The only way to reveal this spyware, or as it is sometimes called malware, is to install an antispyware program.

IS SPYWARE SYNONYMOUS WITH ADWARE?

There is some confusion between "adware," which is seen as legitimate software by most consumers, and "spyware." Adware is defined as advertising that is placed into downloadable products that users will "put up with" in order to gain functionality of a program in exchange for not purchasing it. There is usually some limited functionality if the user does not buy it, but many consumers will decide to try before they buy and agree to endure this adware aspect. Other authors may distribute a product with full features and choose to get paid via the advertising in their product and again the consumer will have to agree to the advertising or not be able to use the software at all. In most cases, the ads are not malicious and do not track or report any buying habits to another party like spyware. Spyware is intrusive because the consumer is not usually informed about it through an end user licensing agreement (EULA) or any other means before downloading the software. It is packaged with software but there may not be any documentation concerning the program in the fine print. The user unintentionally installs the spyware program and in the background possibly sends personal information back to a Web server. Not only can these executable programs steal personal information, but they can install other software programs that can observe keystrokes, monitor chats, read cookies, and sell information to a third party.

POTENTIAL PROBLEMS FACING EDUCATORS AND BUSINESS

Technology support personnel and school administrators should keep electronic security in schools updated through an automated weekly process. Definitions are typically updated and revamped weekly and can

Copyright © 2008, IGI Global, distributing in print or electronic forms without written permission of IGI Global is prohibited.

be a time-consuming activity if completed manually. It is important for teachers to let students know that computers, even with the best security software on the most secure networks, cannot be 100% fool proof and never send identifiable information about themselves on the internet. It also protects the schools from liability in the case of liability and hopefully there are policies in place to protect the schools and students. It is almost impossible for one teacher to monitor an entire classroom's activities in a computer lab, so it is important to have security software in place and have Internet usage agreements signed by parents to keep school liabilities at a minimum.

In some cases, even if users believe that a spyware removal tool has completely removed the spyware contamination from their computer, a user may not have entirely removed the spyware or malware because in some cases it has replicated itself to another location on the computer. It is often recommended then that you use the system restore feature of Windows to go back in time to restore your computer to a time before it became infected. There are times too that the antispyware tool being used will not detect malware because it is so new. However, some of the signs may be there are ads popping up on the screen include pornography, computer slow-down, and other annoyances. If all the latest updates have been downloaded to the antispyware program it may be possible to eliminate the malware threat by going into Task Manager and looking up each process to determine what each does in order to locate the problem or source of the problem. This can be a time-consuming task but can help alleviate the issue at hand.

According to "Keeping An Eye On Spyware" (2006), best practices include keeping operating systems updated, downloading free software from trustworthy sources, ensuring that browser security settings are set to at least "Medium," installing a firewall that has outbound alerts, and reading all end-user license agreements before downloading any software (especially freeware and shareware). Also, never click on links from a pop-up or pop-under window even if it offers to take you to a screen offering an antispyware product and it is offered for free. Always close the windows of pop-up and pop-under windows by the "x" in the corner of the window.

If you are looking for a trustworthy site to choose a highly rated security suite or antispyware program use CNET.com, *PC Magazine, MacWorld, Consumer Reports*, or public message boards for reliable reports. Another suggestion includes using Linux as an operating system instead of Windows or Mac OS X because it does not get as bogged down with spyware according to Cantor (2007). At this time, several highly rated consumer antispyware programs include *Webroot Spy Sweeper, ZoneAlarm Anti-Spyware*, and *Spyware Doctor*. There are free antispyware software programs including *Lavasoft's Ad Aware SE Personal Edition and Spybot - Search & Destroy,* but it is difficult for these programs to keep pace with some of the commercial software programs. Of course, any antispyware software is better than no antispyware software.

SOLUTIONS

In 2005, Sony introduced rootkits in some compact discs to help curtail the illegal copying of music discs (Schneier, 2005). One of the problems the company did not foresee was the software it was placing on these compact discs, a type of rootkit, was a group of files that subvert Windows and can hide from the registry and the Windows Task Manager. This keeps the code from being detected from typical spyware removal tools. A software program on the Microsoft Web site, *RootkitRevealer* (Brandon, 2007) can be downloaded and used to find any rootkits on a Windows system.

Webroot, a commercial provider of Internet security software, recently completed a survey of over 3,000 computer users. With 82% of teens in this sample indicating they visit social networking sites and almost all signifying that they surf the Internet, 92% will open an attachment, embed a link, click on a pop-up, and download a game, music, or screen-saver; this will put their computer at risk of spyware contamination (Hothouse Communication, 2007). The results of this could possibly lead to ID theft including credit card robbery, and not just personal data, but of family users as well.

As omnipresent as the mobile phone has become and with the additional technological advances of streaming live television to surfing the Internet the mobile phone has become the one technology to have. On the flip side, hackers have recognized this and mobile devices now have their share of dangers including viruses and spyware. According to Hypponen (2006), a software program called *FlexiSpy* was discovered that invisibly sends a log of phone calls and multimedia messages

2 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/chapter/spyware/16796

Related Content

Structuring CSCL Through Collaborative Techniques and Scripts
F. Pozzi, L. Hofmann, D. Persico, K. Stegmannand F. Fischer (2011). *International Journal of Online Pedagogy and Course Design (pp. 39-49).*
www.irma-international.org/article/structuring-cscl-through-collaborative-techniques/58661

Students Perceptions on Distance Education in Ethiopian Higher Education: Exploring the Experience of Haramaya University
Yilfashewa Seyoum (2012). *International Journal of Online Pedagogy and Course Design (pp. 32-48).*
www.irma-international.org/article/students-perceptions-distance-education-ethiopian/74172

Developing Literacy Knowledge Through Active Learning in an Online Graduate-Level Course
Vassiliki Zygouris-Coe (2022). *Handbook of Research on Active Learning and Student Engagement in Higher Education (pp. 174-202).*
www.irma-international.org/chapter/developing-literacy-knowledge-through-active-learning-in-an-online-graduate-level-course/298543

Field-Based Learning for Minority Educators: Developing Situationally Relevant Self-Awareness Practices in the Field Experience
Rebecca J. Blankenship, Paige F. Paquetteand Cheron H. Davis (2021). *Research Anthology on Developing Critical Thinking Skills in Students (pp. 1157-1182).*
www.irma-international.org/chapter/field-based-learning-for-minority-educators/269939

College Student Reception of Next-Generation Learning and Effective Approaches for Instructors
Donna M. Farinaand Natalia Coleman (2018). *Handbook of Research on Pedagogical Models for Next-Generation Teaching and Learning (pp. 306-324).*
www.irma-international.org/chapter/college-student-reception-of-next-generation-learning-and-effective-approaches-for-instructors/190373