

SE 4C03 Winter 2005

**Spyware and Adware
An Introductory Examination**

Author: Craig Wilson 0080018

Last Revised: April 4, 2005

Introduction

As the rapid growth of internet users began to occur in the mid – to – late 1990s, the biggest threat that most users faced were variants of the “classical” computer virus. These programs typically damaged the user’s computer in some way, by removing or corrupting files, or preventing some applications (even the entire machine) from operating correctly. While extremely dangerous, these programs were mostly easy to avoid, often giving themselves away as oddly – named attachments in unsolicited emails.

Towards the end of the 20th century, however, a new category of less obvious yet equally dangerous software was being developed and spread across the internet. Dubbed “Spyware” or “Adware”, these programs do not directly harm the user’s computer, but instead perform various tasks in the background of the computer’s operation, unbeknownst to the user. Examples of tasks performed by these programs are

- Periodically displaying pop-up advertisement windows.
- Transferring information about the user’s web browsing habits and patterns to a remote 3rd party.
- Redirecting the user’s web-page requests and default start page to different locations.

Current studies have shown that almost 90 percent of all personal computers in the United States may have at least one Spyware program installed¹. Additionally, most computers are not just infected with one program, but many. A study by US internet service provider EarthLink found more than 29 million files related to Spyware – classified programs on 1 million test machines².

Although these operations may initially seem less harmful than removal of user files, the potential exists for these programs to have an even greater impact on the user’s life. Additionally, the way in which they are transferred raises large questions as to the role users play in computer security, and the obligations software companies have in ensuring the user is properly informed about the application they are about to install.

Overview of Spyware

In general, Spyware can be considered to be any piece of software that tracks information about the end – user, and transmits this information to a 3^d party without the knowledge or consent of the user³. Similar to this, “Adware” generally refers to programs that display advertisements on the user’s screen in periodic intervals, either with or without the user’s permission. In many cases the two types of software are closely linked. The data gathered from a Spyware program may reveal the websites a user browses most frequently, and thus an associated Adware program can develop advertisements to display based on these patterns.

¹ Asaravala, Amit. “Sick of Spam? Prepare for Adware.” Wired May 2004. Retrieved March 13, 2005. <http://www.wired.com/news/technology/0,1282,63345,00.html?tw=wn_story_related>.

² Ibid.

³ “Spyware.” Wikipedia. Retrieved March 25, 2005. <<http://en.wikipedia.org/wiki/Spyware>>.

As mentioned in the previous section, most Spyware and Adware programs have two main purposes:

1. Collect and report information about the computer user, and
2. Use this information to display (unwanted) advertisements to the user; or change some of the settings of the user's software applications or operating system.

In his paper "Methods and Effects of Spyware", Benjamin Edelman outlines concrete examples relating to the first purpose using various Spyware manufacturers. In examining software made by the company WhenU, he noted that when a user visits specific websites (ex: <http://www.expedia.com>), the Spyware program displays a popup advertisement determined by an internal algorithm. Additionally, a message is sent to a web server for WhenU, containing the advertisement displayed, the URL that triggered this advertisement, how the user reached this URL, the user's MSA (akin to a zip code), and IP address⁴.

As an example of the behaviour described by 2, the "Bonzi Buddy" program distributed by BONZI Software appears outwardly harmless. It installs an animated purple ape to the user's desktop interface that checks email, delivers voice advertisements, and tells jokes. The program also changes the user's browser start page to <http://www.bonzi.com>, generates pop-up advertisements, and continually uses CPU cycles⁵. A different but also well known browser-modifying Spyware program is made by CoolWebSearch, which redirects the user's start page to <http://coolwebsearch.com> if they are using Microsoft Internet Explorer as their web browser. Along with this, unwanted pop-up windows are also displayed⁶.

In addition to all of the side effects listed above, many Spyware applications require a great deal of effort to completely eliminate them from a machine. Many Spyware applications leave behind so-called "trickler" programs when the original is removed (through either the Windows Control Panel, or an anti-Spyware program) that covertly re-installs the original program⁷. The author of this paper has personally encountered this type of situation when he attempted to remove a piece of software called "HotBar". After an anti-Spyware program was used to remove the application, the Windows Task Manager showed a trickler process reinstalling the software. Once this process was killed, the trickler files were searched out on the computer, and manually deleted. This ongoing "arms race" between the makers of both Spyware and anti-Spyware tools has left the user in the middle, struggling to keep up with both sides.

⁴ Edelman, Benjamin. "Methods and Effects of Spyware." Ben Edelman. March 19, 2004.

Retrieved March 14, 2005. <<http://www.benedelman.org/spyware/ftc-031904.pdf>>. Pg. 3 - 4.

⁵ "Bonzi Buddy." Wikipedia. Retrieved March 25, 2005.

<http://en.wikipedia.org/wiki/Bonzi_Buddy>.

⁶ "CoolWebSearch." Wikipedia. Retrieved March 25, 2005.

<<http://en.wikipedia.org/wiki/CoolWebSearch>>.

⁷ Asaravala, Amit. "Sick of Spam? Prepare for Adware." Wired May 2004. Retrieved March 13, 2005. <http://www.wired.com/news/technology/0,1282,63345,00.html?tw=wn_story_related>.

Security Implications

Although the obvious security risks posed by Spyware and Adware are the transmission of user's personal information to 3rd parties, there are other security issues that need to be examined. Referring once again to the paper by Benjamin Edelman⁸, he outlines three ways in which Spyware and Adware programs are installed onto user machines:

1. Drive – By Downloads: In this method, if the user is running Microsoft Internet Explorer web sites can send HTML code to the user's browser to begin installation of the Spyware / Adware program. Depending on the user's security settings for their browser a warning message may appear prompting the user to allow the installation, or the installation may even proceed automatically if the user has not set their security settings at a sufficiently high level.
2. Bundling: This practice involves Spyware applications being installed with other, non-malicious applications. Famous examples of this include more recent versions of RealPlayer and various Peer – to – Peer file sharing programs such as Kazaa. In these instances the fact that other programs are being installed may or may not be revealed to the user.
3. One Spyware Program Installs Others: When one Spyware application installs itself onto a user's computer, it may also install other related Spyware or Adware programs. This may be done to increase revenue for a Spyware manufacturer, if other companies pay to have their products installed along with the original programs.

From examining the first two points we see that the distribution of Spyware relies heavily on exploiting both the trust and ignorance of “average” computer users. Drive – by downloads exploit the fact that users have been trained to allow applications presented in a pop – up window to download, due to prior experience with legitimate software from companies such as Microsoft and Macromedia. Although part of the malicious program may have already been downloaded by the time the window is displayed to the user, he / she ultimately has the final say as to whether it is installed. Additionally, if a non-savvy user has low security settings on their browser, then companies can freely take advantage of this as well.

The tactic of bundling Spyware with legitimate software also exploits the trust and ignorance of users. Most computer users expect that software companies are honest, and will inform them if any other pieces of software are being installed along with the “main” application. Unfortunately this is not always true. Software companies often do not inform the user of the nature of the other components that are covertly installed. If the user is informed, it is often in a lengthy and difficult to read End – User License Agreement (EULA) displayed at the first step of installation. As an example, an old EULA by the Gator corporation weighed in at a

⁸ Edelman, Benjamin. “Methods and Effects of Spyware.” Ben Edelman. March 19, 2004. Retrieved March 14, 2005. <<http://www.benedelman.org/spyware/ftc-031904.pdf>>. Pg. 8 – 10.

hefty 5, 936 words, and spanned 63 on – screen pages⁹. This discourages the user from reading the EULA, while still allowing the company to say that they informed the user as to what components were being installed.

Conclusions

The tactics used by Spyware and Adware manufacturers expose the fact that there will always be at least one major stumbling block in the realm of computer security, the end – user. An uneducated user can easily void all of the security built into a software program with one click of the mouse. With Spyware and Adware, this can lead to potentially sensitive information being broadcast to unknown 3rd parties. As such, there is a constant race between those who choose to exploit holes in both software and human, and those who seek to plug these holes. From a human perspective, protecting oneself from Spyware and Adware involves being educated, and having a cautious, suspicious mind. If one encounters something that doesn't look “right” while browsing the World – Wide – Web, it is probably best to err on the side of caution. While there are individuals who are paid to fix errors in software, the only person who can make someone more secure online is oneself.

⁹ Edelman, Benjamin. “Gator’s EULA Gone Bad.” Ben Edelman. November 29, 2004. Retrieved March 28, 2005. <<http://www.benedelman.org/news/112904-1.html>>.

REFERENCES

1. Asaravala, Amit. "Sick of Spam? Prepare for Adware." Wired May 2004. Retrieved March 13, 2005.
<http://www.wired.com/news/technology/0,1282,63345,00.html?tw=wn_story_related>.
2. Edelman, Benjamin. "Gator's EULA Gone Bad." Ben Edelman. November 29, 2004. Retrieved March 28, 2005.
<<http://www.benedelman.org/news/112904-1.html>>.
3. Edelman, Benjamin. "Methods and Effects of Spyware." Ben Edelman. March 19, 2004. Retrieved March 14, 2005.
<<http://www.benedelman.org/spyware/ftc-031904.pdf>>.
4. "Bonzi Buddy." Wikipedia. Retrieved March 25, 2005.
<http://en.wikipedia.org/wiki/Bonzi_Buddy>.
5. "CoolWebSearch." Wikipedia. Retrieved March 25, 2005.
<<http://en.wikipedia.org/wiki/CoolWebSearch>>.
6. "Spyware." Wikipedia. Retrieved March 25, 2005.
<<http://en.wikipedia.org/wiki/Spyware>>.