Spyware

Thomas F. Stafford
University of Memphis, USA

INTRODUCTION

There is a potent threat to computer security represented by the emerging class of applications commonly known as "spyware," designed to remotely monitor and report on user activity. The threat manifests itself indirectly, unlike hacker intrusions and many virus infections. These remote monitoring applications record and transmit information on computer user behaviors to third parties, who then utilize monitored customer data for marketing segmentation and targeting, or for more nefarious violations of user computer security. Most spyware is legal, having typically been installed during free software downloads online. Some spyware is illegal, having been remotely installed by bots on visited Web sites, and can remotely monitor for illegitimate purposes such as keystroke logging and password theft and account access. Spyware is often defended by its sponsors as a means of more effectively targeting the Internet experience to users, but users typically find the costs of this purportedly customer-centric monitoring process objectionable in terms of subsequent advertising distraction and system resource monopolization.

WHAT IS SPYWARE?

Spyware is a term loosely used to characterize an emerging class of remote monitoring applications designed to run on user computers and report aspects of user computer behavior across Internet connections back to a remote third party (Stafford & Urbaczewski, 2004). It is estimated that as much as 90% of home computers (Farrow, 2003; Schmidt & Arnett, 2005) and small-to-medium-sized business computers (Zhang, 2005) are infected with spyware, and it is not unheard of for computers to come directly from the manufacturer with spyware applications already installed (Levine, 2004; Thompson, 2003).

Spyware, in the specific form known as adware, typically acts to track Internet use and subsequently target pop-up advertising to user computers (Fox, 2005), though far more nefarious uses have been observed such as keystroke logging, password theft, and commandeering user system resources for external use, which typically are performed by surreptitiously installed "backdoor" versions of Trojan horse applications (Volkmer, 2004). Trojan horses, often simply called "Trojans," are surreptitiously installed applications, often arriving hidden in parts of seemingly legitimate files such as e-mail attachments that later activate in order to capture and report user activity data.

Aside from the privacy and security issues of remote third-party monitoring of individual user computers, there is the not-inconsiderable issue of spyware as a resource-hungry application that consumes noticeable amounts of computing resources while running as an ever-present background application on PCs (Stafford & Urbaczewski, 2004). Unexpected and sudden degradations in system performance are often the first clear symptoms of spyware, as they attach system resources at the expense of legitimate applications. As difficult as it can be to detect spyware running on your machine, these applications can be tougher to clean. Typical spyware removal war stories include subsequent failures of user Internet connections, since some applications alter the Winsock stack (Foster, 2002).

The Winsock "stack" in Microsoft operating systems is an interface and supporting program that handles input/output requests for Internet applications (Whatis.com, 2006). The name "Winsock" is derived from its adaptation by Microsoft of the Berkeley Unix sockets interface, which serves to connect with and exchange data between two program processes, in this case between OS-supported user applications such as browsers and the TCP/IP protocol stack that permits computers to communication in data packets across the Internet. Since spyware applications are specifically designed to commandeer Internet communication procedures, the Winsock stack is typically implicated in infestations, and removal very often damages the operating system functionality for Internet communication.

WHERE DOES SPYWARE COME FROM?

The typical cause of spyware infestations on user computers is a free Internet download of a software application (Taylor, 2002). Spyware applications typically come bundled in downloads of popular freeware applications, such as peer-to-peer file sharing applications as well as specific accessory applications such as Bonzi Buddy, Comet Cursor, Xupiter Toolbar, and Bargains.exe (Coggrave, 2003). Many applications that users find cosmetically appealing as addition to their computer interface include graphic cursors and related animated applications, and various "effort-saving" toolbars typically represented as shopping aids or news sources. Many of these "cosmetic" applications come packaged with remote monitoring applications; indeed, even legitimate versions of such applications, such as the Google and Yahoo Toolbars, are capable of collecting information on user Internet activity and transmitting it to the sponsoring organization. In some cases, this user monitoring process is represented by the provider as a means to tailor the tool to individual preferences, and users are sometimes permitted to opt out of remote monitoring during installation. In other cases, the user installs a pretty graphic on the computer and also ends up unwittingly installing a bundled adware product that will produce noticeable increases in pop-up activity upon activation.

Among the "bundling" vectors that can provide spyware—aside from P2P file sharing applications, cosmetic applications, and shopping agents—are certain e-mail and instant messaging programs; some illegal spyware applications will even install themselves unbidden during Web site visits, which is known as a "drive-by download" (Stafford & Urbaczewski, 2004). The method frequently used to avoid prosecution for illegal installation of spyware applications involves bundling spyware with licensed commercial applications, including an affirmative installation statement in the license agreement that comes with the associated and sought after user application (Schultz, 2003).

The reason that free software downloads online often serve as a vector for remote monitoring applications is due to an emerging revenue model for supporting the provision of "free" software (cf., Gibson, 2005; Klang, 2003). Developers essentially seek to recoup their expense in creating freeware applications by selling bundling rights to sponsors of remote monitoring applications who desire greater access to information about Internet user behaviors. As noted above, users are routinely provided with a disclosure of this bundling of remote monitoring applications as part of a download in the typical "clickwrap" licensing agreement for freeware, but many users do not pay adequate attention to the licensing provisions of applications that they agree to download for free (Stafford & Urbaczewski, 2004). Since nothing of value is ever truly free, the effective exchange transaction users enter into for "free" downloads involves the (often unwitting) exchange of personal information and loss of online privacy to third parties on the Internet via remote monitoring applications that are installed on their computers (Stafford, 2005).

EMERGING TRENDS IN SPYWARE THREATS

The Gartner Group expects that spyware will become the tool of choice for identity theft in the near future (Radcliff, 2004). Remote applications that monitor user keystrokes and account access can serve to capture passwords, PIN numbers, and associated account information such that third parties would be in a position to fraudulently represent themselves using stolen user and account information for identity theft purposes. Hence, it may be expected that the illegal hacker community will continue to develop remote monitoring applications that will typically install themselves surreptitiously and illegally on user computers.

Aside from the widespread trend of seeking to install surreptitious monitoring and display applications on user computers, a frequent hacker community spyware threat has been in the form of "dialers," which cause computer modems to automatically engage in the dialing of overseas or toll-linked phone numbers in order to incur financial charges for the user. "Web bugs," which are single-pixel GIF-format files downloaded with Web pages, also have become quite popular for both illicit and legitimate monitoring purposes, serving essentially the same purposes as cookies by providing 'loggable' download events to document user actions and histories.

Businesses find vast utility in the ability to monitor computer users for marketing segmentation purposes (Foster, 2002), but businesses also find remote monitoring applications useful for providing an agent