Posted At: Tuesday, March 02, 2004 8:12 AM
Posted To: spywareworkshop2004
Conversation: Spyware Workshop
Subject: Spyware Workshop

The workshop generally will focus on four areas:

* Defining and Understanding Spyware, including a discussion of how spyware may differ from adware;

Adware is a program that runs on your computer, monitors your surfing habits and delivers targeted advertisements, typically in the form of pop-up windows. Spyware is a program that runs on your computer, monitors your Web surfing habits and reports the habits to a remote computer.

* Distribution of Spyware, including the role that peer-to-peer file-sharing may play;

If you download and install file-sharing programs, such as Kazaa, Morpheus and Grokster, you are typically at risk of downloading adware/spyware with it. Few people read the EULA before downloading and installing programs. Buried in many of these EULA's are statements like this: "During the process of installing the Software, you may be offered the possibility to download or install software from third party software vendors pursuant to licenses or other arrangements between such vendors and yourself"

Other forms of infiltration are: Security holes in browsers, Instant Messaging programs, Browser search bars/toolbars, Advertisements (usually pop-ups) displaying dire error messages or offering to stop pop-ups or spam and prompting the user to "Click Now" to immediately get the fix, Downloaded games, "Drive-by download" (a program that is automatically downloaded to your computer, without your consent or even your knowledge, via a Web site visitation), Physical access to a machine.

* The Effects of Spyware, including the extent to which spyware affects the functioning of personal computers and raises privacy or security concerns; and

This is situational, depending on the user's technical knowledge and type of spyware residing on the machine. Judging from the hundreds of emails I've received from persons infected with spyware, the effects can range from having the computer's performance slow down due to loss of system resources, having the user's browser home page setting changed to the advertisement page which the user is unable to reset (usually because of URL search hooks or added registry keys), redirecting the user's search requests such as CoolWebSearch and it's variants does essentially prohibiting the user from ever visiting a website unless it's a sponsor of CWS, delivered popup advertisement to the user based on surfing habits, scanning the user's address books and other personal information. One particular prompt to purchase a SpyWiper product includes threatening popups and scare tactics such as hardware manipulation (the opening of the user's CD rom drive door), backed up with pornographic popups. I've had several users tell me that their CD rom drive is protected behind a cover shield and the manipulation of the CD rom drive door from a SpyWiper advertisement snapped the drive door and broke it. Another user informed me that SpyWiper disengaged the content advisor in order to deliver pornographic popups. Spyware can also be later used to cooperatively engage the user's computer in a DDoS attack without the user's knowledge. If you want to go beyond the affects of computer functionality, include the many complaints of family members accusing each other of visiting pornography sites because of popups delivered through a SpyWiper hijacking (which is a drive-by installation from reputable sites). the affects of children witnessing pornographic popups during a SpyWiper hijacking, and the case of one gentleman who's job has been threatened by his employer who insists the gentleman must have downloaded something on the company computer (again, a drive-by download from a reputable site).

To summerize, spyware slows the computer's performance by using system resources to monitor and feed back information, and then to feed advertising information back to the user. Spyware hampers the user's control of the machine, such as in the form of browser hijacking and redirected web searches. Spyware can cause damage to the computer, such as displaying advertisements that manipulate hardware which may not be set up to handle the manipulation.

As for the extent of privacy and security concerns, this is limitless. No one wants their personal information scanned and distributed without their permission. InternetAntispy is a great example of an advertisement exploiting this concern. Their advertising is distributed through a browser hijack which flashes your IP address and the city and state you live in across the top of their page in an effort to frighten the user into purchasing their software. SpyWiper informs you that you are probably infected with spyware and have no other choice but to purchase and download their product if you want control of your machine back. Enigmasoftware blatantly states that it's detected a key logger on your computer and, therefore, you have to purchase their product to remove it.

*	Possible Responses to Spyware Concerns, including a discussion of what consumers, government, and industry have been doing and intend to do, by themselves or together, to address the harms associated with spyware.

There needs to be stiff laws against the distribution of any form of adware or spyware. We don't need laws requiring companies to be more forthright about what a consumer is downloading, we don't need "permission-based only" distribution, and we don't need laws holding companies and developers responsible for what their hired marketing companies are implementing. Spyware/adware needs to be outlawed, period. It's ludicrous to allow developers and distributors of spyware/adware any rights whatsoever. Allowing it to exist within a legal frame is like saying it's ok for a thief to come into your house and steal your property as long as they follow a certain set of rules. The most notorious of these distributors will not be concerned with laws and frameworks they are required to operate within. Many are elusive with false registry information, many operate their business offshore outside of US jurisdiction, and many operate through several cooperative businesses so it's impossible to pinpoint who is actually behind the distribution.

From a consumers standpoint, I see a lot of effort being exerted against the adverse effects of spyware/adware in the form of informative websites and forums. Caring citizens offer free help and advice to anyone who asks. Several good programs that help in the removal and prevention of spyware are also being distributed freely. Some of these sites and forums have recently been or are currently under DDoS attacks, presumably by unknown spyware distributors, in an attempt to remove the site or forum from the internet and causing the webmaster monitary damage. Implementers of DDoS attacks are hardly concerned with any legal issues that might be imposed on them.

My website is **http://tired-of-spam.home.comcast.net** If you want to use any portion of it, including screen shots, in your workshop, you have my permission.

Jola Harvel