Comments for the Federal Trade Commission Workshop on Spyware

A. Defining and Understanding Spyware

I believe that this is the most comprehensive definition of spyware that I have read:

"Spyware is software or hardware installed on a computer without the user's knowledge which gathers information about that user for later retrieval by whomever controls the spyware.

Spyware can be broken down into two different categories, surveillance spyware and advertising spyware.

Surveillance software includes key loggers, screen capture devices, and trojans. These would be used by corporations, private detectives, law enforcement, intelligence agencies, suspicious spouses, etc.

Advertising spyware is software that is installed alongside other software or via active x controls on the internet, often without the user's knowledge, or without full disclosure that it will be used for gathering personal information and/or showing the user ads. Advertising spyware logs information about the user, possibly including passwords, email addresses, web browsing history, online buying habits, the computer's hardware and software configuration, the name, age, sex, etc of the user."

By Mike Healan of SpywareInfo.com

http://www.spywareinfo.com/articles/spyware/

B. Distribution and Effects of Spyware

Much spyware is distributed by downloads of so-called free software on the internet. However, it isn't really free, because the computer user pays the price of the use of his/her computer's resources including bandwidth and processing power. This spyware can hog the system's resources causing significant slow downs as well as interfere with web browsing by sending the user to unwanted sites, generating unwanted ads and pop-ups, changing the content of web pages, and even changing the user's homepage setting.

Spyware is also distributed by just visiting some web pages - pages with ads that leave a payload of spyware and sometimes a hijacker behind. Sometimes there is even a delay mechanism, so that the user cannot determine what site the spyware came from. Spyware companies take advantage of security holes in Windows, Internet Explorer and of users with low security settings.

I run a blog about spyware and a spyware removal help forum. Many, many people post that their homepage has been changed; their searches redirect them to unwanted sites, sometimes porn sites; their favorites folder is filled with unwanted entries, often porn sites again; unwanted icons appear on their desktop; they have excessive pop-ups; excessive CPU usage; computer is running very slow or won't run at all; they are unable to access the internet at all; their firewall and/or antivirus is turned off mysteriously; they are unable to reach spyware help sites. Some spyware adds entries to the HOSTS file that redirect the browser to its own sites when the user enters certain URL's. These people have tried to fix the problems themselves and are unable to do so. They seek help from forums like mine, often posting in desperation.

The creators of spyware and adware do all those things to increase their own profits at the expense of the computer user. This should be illegal.

Spyware can and does transmit data back to it's creator in the form of tracking websites visited, gathering passwords, email addresses, passwords, computer configurations, information entered into websites and forms, even on secure sites in come cases. Again, this should be illegal.

Many adware/spyware companies try to hide behind the fact that the computer user has agreed to the EULA when downloading their product or the product they are attached to. It is well known and documented, however, that usually these EULA's are long, tedious, and difficult to understand and the information about the adware/spyware is usually near the end of the long, tedious document. Understandably many people do not read the EULA's carefully if at all.

C. Possible Responses to Spyware Concerns

I believe that the bottom line is that spyware should be illegal. Any code, whether on a web page, included in a downloaded program, or in an ad on a web page, that does not clearly identify what it is, what it does and without obtaining specific permission from the computer user to install, should be made illegal. That would end browser / homepage hijacking, hidden applications running that the user is not aware of, redirection of searches, altering the content of a web page, and the transmission of data from a user's computer without his/her knowledge and express consent. All of those things should be illegal.

Consumers need to be educated and made aware of spyware, informed about how to get rid of it and how to prevent. There are free tools available on the internet at spyware removal help sites. Interestingly enough, several of the most prominent spyware removal sites were recently brought down by DDoS attacks. One can surmise that the spyware companies were behind this attack. I believe that this shows how the spyware companies have no regard for computer users and are willing to do anything, no matter how immoral

and unethical, to further their own profits. Again, this should be illegal. These spyware companies should be forced to shut down.

In conclusion, I believe that spyware and adware are a very real menace to the internet and to computer users. I know people who have become wary of even using the internet because of their bad experiences with browser hijacking and spyware. I have recently read articles stating that 90% or more of computers are infected with spyware. I believe that any existing laws that can be used to stop these spyware activities should be strictly enforced. New legislation may be needed also. A multifaceted effort is needed including education and public awareness about the problem of spyware including how to rid themselves of it and how to protect themselves from it, enforcement of current applicable laws and new legislation. The spyware / adware companies, their affiliates, the webhosting companies and ISP's that support them, must be held accountable for the damage they cause; ultimately they must be stopped.

Respectfully submitted,

Suzi Turner

http://www.netrn.net/spywareblog
http://spywarewarrior.com