-----Original Message-----
From: Jay Cross, Jr.
Posted At: Wednesday, March 17, 2004 8:32 PM
Posted To: spywareworkshop2004
Conversation: Spyware Workshop - Comment, P044509
Subject: Spyware Workshop - Comment, P044509

Public Comment for Federal Trade Commission Spyware Workshop
Authored by Jay Cross, Jr.
President of Communications and Technology, IPCC
IPCC < **www.ipccouncil.com**

- In recent years, spyware applications have gone a long way toward creating discontent among the general public, and striking new, far-reaching security concerns into the minds of IT professionals and everyday consumers alike. As a company, the Internet Privacy Conservation Council (IPCC) takes a principled stance against spyware, but there is truly more to the spyware scene than meets the eye. Throughout this document, you will be made aware of not only the very real and legitimate risks posed by spyware, but also of the mudslinging, speculation, and scare tactics used by "security" professionals.

Undoubtedly, spyware applications pose a very real and immediate risk to not only PC security, but also personal privacy. It's become common for a casual PC user to open their web browser to find themselves loaded with toolbars, "helper" components, pop-up ads, search engine hijacks, and a myriad of other assaults to Internet explorer. These components aren't necessarily bad under all circumstances, and can sometimes serve legitimate, useful purposes- but the crux of the matter is that many people cannot tell you how these things ended up on their machines. They were never presented with a legally binding End User License Agreement (EULA), or in many cases, even a chance to click a "Yes" or "No" dialog box! Dishonest advertising companies, with the assistance of programming teams and what have you, have realized that there is a huge, virtually limitless revenue stream in the business of forcing content onto unwilling end users through security holes and other methods. By capitalizing on legions of technically inept computer users and an ever-increasing list of web browser exploits and security holes, these dishonest organizations have found that they can get their advertisements out to a huge group of potential customers in a manner that has yet to be legally defined. These groups avoid withstanding the scrutiny typically reserved for authors of computer viruses by protecting themselves with buried-in-fine-print disclaimers posted in inconspicuous locations on their Websites. In a nutshell, these applications are able to show unsolicited advertising to millions of individuals, harm their machines, prevent themselves from being removed, and engage in other virus-like behavior, with almost none of the penalties.

However, there is a second side to this story. As you may or may not know, very few of these spyware applications come with a means of removal, and many vendors even bundle uninstallers that add more code, or simply do nothing to remove what's already there. Because of this

nasty tactic, programs like Lavasoft's Ad-Aware, and Patrick Kolla's Spybot Search and Destroy quickly gained popularity and notoriety for removing and otherwise eradicating these harmful applications. Somewhere along the line though, things went terribly wrong, and a sort of double standard was created for the makers and advocates of these applications. Entire websites dedicated to "spyware information", containing nothing but blind speculation and mudslinging, have become reliable sources for professional security organizations, such as Symantec. It is now in the best interest of these security organizations to lull end-users into believing that every single Internet Explorer toolbar, popup ad, or sponsored link they see is a clear and immediate breach of their privacy, just because they say so. The people that get caught in the middle of this are legitimate, fair-dealing adware companies, or companies that enable the developers of freeware applications to defer software development costs through advertising. However, it is not in the best interest of established security giants that engage in fear tactics for profit to take a stand in making the public aware of this. It has now become commonplace for fair-dealing adware organizations to approach Spybot, Ad-Aware and the like, and be completely ignored as they attempt to make their case of honesty. These tactics, if allowed to continue, will be responsible for the collapse of an entire profitable (and honest) industry – legitimate adware.

The biggest problem with the current methods of dealing with spyware and other privacy threats is the clear and obvious lack of factual knowledge and evidence. As it stands today, forums and entire Websites are filled with blind claims and speculation. In the absence of hard, factual evidence against them, spyware vendors have virtually nothing to be afraid of, because any legal claims against them would be laughed out of any courtroom in this country. But let's take some time to explode some popular myths about spyware.

Myth 1- Peer-to-Peer (P2P) technology is responsible for the spread of spyware.

- While it's true that several popular P2P file-sharing applications have chosen to bundle less than honest applications alongside their own software, this stance largely represents an attempt by the Recording Industry Association of America (RIAA) and other multimedia trade groups to stop P2P technology. The RIAA's sympathy for the privacy rights of individual consumers end when they start hiring third party organizations to police P2P networks in violation of their privacy policies.

Myth 2- There is nothing wrong with a double standard concerning accountability between spyware vendors and security groups.

- By the same token that spyware vendors should be held accountable for their dishonest and harmful actions, security companies and organizations should not be allowed to promote fear and discontent amongst the general public in a baseless manner, intended only for personal profit and gain. People download an application like Spybot and see 12,000 or so blacklisted items, and thus feel safe. What they don't realize is that things are added to this list for any number of reasons – possible even for things as unreliable as a simple complaint

on a web forum. Security organizations should be required to face the same standards of accountability as the ones they propose for spyware vendors, and not allowed to hide behind the false positives put out by their applications and scare tactics.

Myth 3- Every Internet toolbar, popup ad, etc. is violating my privacy.

- Consumer attention should be directed more towards how these types of things appear on their machines, rather than what they are. There are plenty of legitimate uses for toolbars and advertising, just as there are commercials on TV and radio. Many organizations have used spyware to condition people into thinking that the Internet is an entirely free medium that costs nothing to maintain or profit from, and that simply isn't the case. However, unsolicited advertising that promotes and supports nothing but the personal profit of a shady company should not be tolerated under any circumstances.

Authored by Jay Cross, Jr.
President of Communications and Technology, IPCC
IPCC < **www.ipccouncil.com**

Additional Links
- **http://www.excedra.com/content.php?x=pressroom_ipcc**
- **http://www.wired.com/news/infostructure/0,1377,60694,00.html**