From: Becki Bell
Posted At: Thursday, April 08, 2004 2:08 PM
Posted To: spywareworkshop2004
Conversation: Spyware Workshop - Comment, P044509
Subject: Spyware Workshop - Comment, P044509

My concerns about spyware/adware are both personal and professional.

From a personal standpoint: Spyware/adware has been installed on my computer without my knowledge or consent on several occasions, usually with seemingly benign shareware or freeware software that I have downloaded from the internet. These products often come bundled with spyware and adware, which gets installed at the same time as the shareware, but usually without the knowledge of the person doing the installation.

One of the main problems with spyware is that it is very difficult to get rid of. It can't be uninstalled, it can't be turned off, and most of the time it can't even be located. I had one piece of spyware that launched a popup window every three to five minutes. If I left my computer connected without closing any of these windows, in less than an hour my machine would crash because the memory wasn't able to handle all the new windows. Now, under normal circumstances, I can just decline to visit a website that uses popups, but if I can't remove a piece of adware from my computer, I am forced to look at and then close those ads constantly, no matter what I am doing, and all of my choice in the matter is removed.

This is primarily an irritant, but the real issue is my right to control the software I use on my own computer, and the sites I choose to visit when I am on the internet.

There are also strong privacy problems created by the proliferation of spyware. I currently have a piece of spyware on my computer that dials the internet randomly. I have been unable to locate the software that is doing this, and I can't tell what it is doing when it connects or what the purpose of the connection is. What if it is sending my personal information to an unknown source? I have no way of knowing how to stop it or even what information it is compromising.

From a professional standpoint: I am the owner of several informational websites, and two e-commerce sites. I work very hard at creating content for these sites, at marketing and promoting them, and at selling advertising and products. I also spend a lot of money developing and supporting these websites, not to mention countless hours of my own time.

There are several adware products out there that can hijack the content of a website and add their own advertising and links. The two types that concern me the most are:

- Adware that embeds its own links in the content of a website. For example, someone with adware installed on their computer (usually without their knowledge or consent) may visit the "web design" portion of my site, where I advertise my design and content creation services. The adware will take the content of that page and redraw it to include links to *other* companies that provide web design and content creation services. These are advertisers that have paid the adware company for those links, and I am in no way compensated if my visitor uses one of those links to leave my site and visit an adware advertiser. If this happens, not only have I lost a potential customer, but I have also been the unwitting and uncompensated vehicle for providing business to a company I have no affiliation with.

- Adware that replaces the "sponsored links" on Yahoo and other search engines with advertisements from an adware company. I currently spend money on pay-per-click advertising. Yahoo and other search engines, in return, receive money from pay-per-click advertisers. What happens when someone with this type of adware installed on their computer does a search for "model airplanes" on Yahoo? Instead of seeing my sponsored links, they see links to the adware company's advertisers. Now not only am *I* losing potential business, but Yahoo is losing revenue, too. Again, the adware has hijacked the content of the Yahoo website (which is owned by Yahoo, not by the adware company) and stolen its revenue in doing so.

A good analogy for either of these practices: suppose a magazine spends thousands of dollars printing an advertising insert for an issue of their magazine. Then someone visits every newsstand in the country, removes the insert from each available copy of the magazine, and replaces it with an insert of their own. The magazine has just lost the thousands of dollars they invested in creating, printing, and distributing that insert. The advertisers who paid to be included in the insert have lost all the money they spent on those ads, and the potential revenue those ads might have generated. And the thief gets to distribute his message to thousands of people, counting on the magazine's popularity to do all the work for him.

Adware is the same principal, except that technology makes it extremely simple to do.

I hope some good comes out of the Spyware Convention. These practices need to be stopped in order to protect the privacy and choice of consumers, and the intellectual property of millions of internet publishers and marketers.

Sincerely,
Becki Bell