Spy/Adware, The New Real Security Problem

July 29, 2004

By Larry Seltzer

Like many of you, I spend many a visit to family and friends attempting to fix their computer problems. The No. 1 problem scenario these days involves spyware and adware, often so much of it that the computer is utterly unusable.

An infected system is a sad sight. You can't do anything without windows popping up and interfering with your work, assuming the computer is responsive at all. I've seen a couple that wouldn't even finish booting.

Cleaning up such systems is a business staple for Steven Brier of Brier IT Services. "I had a client yesterday with 13 different search help tools and another seven comparison shopping programs competing for her attention. The popup windows would see terms in other popup windows, spawning yet more popup windows to offer yet better deals. The computer was unusable."

> For insights on security coverage around the Web, check out eWEEK.com Security Center Editor Larry Seltzer's Weblog.

All too often Brier sees the cause of such problems. Unlike viruses, which attempt to sneak in under the radar, spyware and adware are invited in the front door. Brier's advice: "If your kids—or you—want to install some software because it's supposed to help you, don't do it. Get up, walk around, count to 10, and get over it."

There are a large number of programs to detect and remove the much larger number of attacks. As PC Magazine found in its most recent roundup, none of them does a really good job of cleaning up this software. Since some of the best ones are free (asking for donations) it may be a good idea to run more than one; personally I boot into safe mode, go into regedit and manually clip the wires of these little bombs.

How can spyware and adware be such a festering problem when worms and viruses are comparatively under control? Why do the major security software companies emphasize the classic viruses and worms and largely ignore spyware and adware, leaving it to a bunch of little guys and volunteer efforts? The problem is a challenging one to the software industry.

Next page: Virus authors with commercial funding.

Seth Schoen, a staff technologist at the Electronic Frontier Foundation, says, "Spyware authors are like virus authors with commercial funding." They operate as (ha ha) legitimate companies, and their products can make money, whereas viruses just make trouble. (It is believed that some worms have been written on contract for criminal organizations or spammers, but this doesn't compare to the way spyware/adware authors operate out in the open.)

Schoen also points out that virus authors focus on reproduction, even if they do try to avoid detection and removal, but spyware and adware authors put a lot of effort into making their programs difficult to

remove.

And remember, these programs present themselves as legitimate applications that the user wants, such as a cool new toolbar for Internet Explorer or a comparison shopping program. Virus writers need to install stealthily, hiding themselves from detection. Adware developers can use InstallShield, and in fact it only makes them look more legitimate.

> **Read all about Microsoft's battle to deliver secure software in eWEEK.com's special report on securing Windows.**

I have a subscription to Symantec's Deepsight Alert Services, and I'm a big fan of it, but I recently noticed that they don't track spyware or adware at all. I asked Symantec about it and got the sense that they weren't quite sure how to monitor it with the same level of quality they have for the other threats they monitor.

"What would you want us to do?" they asked. I can come up with a lot of ideas. They could track all the spyware and adware implementations, the products to which they are attached, the sites on which they appear, behaviors and how to remove them. Yeah, sure it's hard, but if something's worth doing it's worth putting in the effort. (Easy for me to say.) The next step would be tools to defend against and remove these threats. Norton Antivirus added this capability last year, but it was second rate, to put it generously.

Companies like Symantec are also in a tough position blocking or warning their users against some of these programs. There's a liability issue, since they claim to be legitimate applications. Perhaps this is the biggest reason we haven't seen the "legitimate" anti-virus companies make a real effort in this area.

I grow tired of the attention and fear that viruses generate. Much of it comes because the anti-virus companies can deal with viruses, so they warn people about them. They don't have a solution for spyware and adware, so we don't hear about new threats.

Perhaps some of the laws being discussed to fight spyware could help. Since adware vendors purport to be legit, they can be found and sued. I've had concerns about these laws, but they're working on the problems in them.

In fact, I don't see a good alternative. You can't stop users from deliberately installing programs, and you can't expect average users to understand warnings like "Browser Helper Objects are often evil tools of unscrupulous advertisers who will grab hold of your computer and not let go." So holding them to a set of rules about disclosure and what actions are permissible without the approval of the user, which is the approach of the legal proposals, has the potential to break the legal blocks that might be intimidating the security software companies.

And besides, some things are just wrong and should be illegal.

Security Center Editor Larry Seltzer has worked in and written about the computer industry since 1983.