

Panic Over Spyware

PC Magazine, 12/20/04

By John C. Dvorak

I'm chatting with the CEO of a spyware company and he tells me that he knows for a fact that Dell support lines have been getting 70,000 calls a week regarding machine performance and anomalies. Dell has been referring the callers to Web sites discussing spyware. It's spyware causing the problems. I'm thinking to myself that if Dell is getting 70,000 calls, then Microsoft must be getting 700,000 calls, since the smart money would always assume that it's a software problem. Whatever the call volume, this situation with spyware is now officially out of control.

This subject is near and dear to me, since my laptop was infected via a hotel network connection recently. The culprit is the `webrebates.exe` Trojan horse. Like many of these pests, once it gets on your machine it starts installing loaders all over the place. These are essentially spyware spies. They all look to make sure that the spyware stays in place. If you manage to erase it one of the little drones will reinstall it. You cannot erase the drones and the spyware fast enough to prevent this simple process from continuing unless you use special software to ferret out all the drones first. Many of these pests also contaminate the Registry, and many of the drones are in subdirectories that cannot be seen using any normal process.

As an aside I should mention that I've always wondered why Microsoft Windows has weird deeply rooted directories that cannot be seen in Internet Explorer, DOS, or any tool. They are scattered all over the place. The nasty spyware drones often end up buried so deep that finding them requires lengthy deep searches by antispyware tools.

Now, if you think that the free antispyware programs are going to help with the nastiest of infections, you are kidding yourself. I've chatted with four spyware vendors over the past couple of weeks and they all agree that it's gotten so bad that the public is only partially aware of the problem. Few users know that their machines are infected.

There is now a firm belief that organized crime, including the Russian mafia, is behind much of this activity. The scene is no longer dominated by kids out for fun.

So what is the spyware used for? There appear to be [four primary uses](#).

Market research. Yes, it's true. A lot of spyware is used just to track browsing and other online behavior for market-research companies. This was one of the two initial uses.

Employee and spousal monitoring. This is the second initial use for this stuff. Key loggers and other systems that are usually installed directly onto machines by the person or institution doing the spying. The FBI has been known to capture passwords using such software.

Spambots. The more recent use of spyware has been to create legions of spambots for spammers to rack up big numbers without taxing their own servers. There are probably millions of drone machines, sometimes called zombie PCs. At night they are brought to life to serve spam all over the world. Yet another reason why the 24/7 always-on Internet is a complete disaster.

Identity and credit-card theft. This is the latest twist and the fastest-growing trend. Last week, a new combination scam somehow got through my spam-filtering mechanism and tried to install a Trojan horse loader onto my system through the preview window of Microsoft Outlook Express. (Wasn't this supposed to be fixed?) My Kaspersky antivirus software saw the loader and stopped it cold. But what I found interesting was that this was one of those "Your account is temporarily closed" scams designed to collect personal information.

The notable thing about spyware is that because it isn't virulent like a virus and seldom spreads from your machine to another, it manages to stay out of the spotlight. The national media pay little attention to the problem, and many mainstream media tech writers are Mac users, so they don't get it. Who knows what will happen when the Mac community gets hit? They feel immune, and are for now. But when they get hit, there will be few resources to help them, since the antispymware community is busy with all the PC-related problems.

Since spyware has not spread quickly and tends to be installed via browsers one computer at a time, we are seeing slow—but relentless—growth. We can expect it to continue. I'm looking at all the spyware packages and I'll have a few to recommend in the months ahead. For now you'll probably need multiple systems to get rid of this stuff. This will be the number-one topic in the year 2005, guaranteed.