# The Nasty Truth About Spyware

@bsolute pc solutions

While spyware programs are nothing new, they continue to grow in virulence and sophistication. Anyone that uses a computer and the Internet should be aware of the risk these programs present. While they can be troublesome to the home user, they can pose an even bigger risk to a corporate network.

Spyware is not just one type of program. It's an entire category of malicious software that includes adware, Trojans, keystroke loggers, and information stealing programs. Some have likened it to the cancer of the computer world. Why? Because these programs have become increasingly intelligent. Many have the capability to install themselves in more than one location and just like cancer, any attempt to remove them, triggers the software to spawn a new variant in a uniquely new location.

This form of digital cancer is also capable of changing registry entries and forcing Windows to reinstall itself when the computer reboots. Spyware coders have even incorporated concepts such as Alternate Data Streams "ADS." For those of us using NTFS, this old-school hacker technique allows the spyware distributor to stream one file behind another. A quick search of the drive will find no trace of the offending executable as there is no entry in the FAT.

What are some of the worst spyware programs that you might be exposed to? Well, Webroot.com has compiled a list and the top ten includes titles such as KeenValue, a program that collects user information to target them with specific popup ads. Another is PurityScan, which advertises itself as a cleaner that removes items from your hard drive. Finally, there is CoolWebSearch. This program is actually a bundle of browser hijackers united only to redirect their victims to targeted search engines and flood them with popup ads.

Sure, home users are at risk but a compromised corporate desktop poses a real threat. These computers have the potential to access tons of proprietary and sensitive information on a scale that would be unheard of on a home computer. Corporate solutions have been slow to develop. Fortunately, Aluria Enterprise, Symantec, Sunbelt, and others are starting to respond. There are some quick fixes you can perform to reduce the probability of infection.

- Patch - Spyware programs take advantage of known security vulnerabilities, so make sure your OS and browser are patched and up to date.
- Use a firewall - Practice the principle of least privilege.
- Change browsers – Dump IE, many spyware programs are written specifically for IE. Firefox or Opera are two possible alternative browser options. Both have additional security features built-in.
- Beware of free programs – Peer-to-peer programs and other so called free programs can be supported by spyware. After all, someone must pay the bills! Don't install software without knowing exactly what comes with it. Take the time to read the end-user license agreement.
- Install Anti-Spyware programs – Programs that can remove spyware include: Search & Destroy, Spy Sweeper, SpySubtract Pro, and Ad-Aware. If you think you may be infected, I would suggest you checkout one or more of these products. For really bad infections, you may want to check out Hijack This.

A good offense is about defense, so by implementing the solutions offered above and making the decision to deploy an enterprise-class spyware solution, this problem can be addressed. While there is no guarantee you won't become infected, there are ways to reduce the possibility.