

# Adware and Spyware Protection

By Bill Hely

*Spyware is computer software that is installed surreptitiously on a personal computer to intercept or take partial control over the user's interaction with the computer, without the user's informed consent.*

*The functions of spyware extend well beyond simple monitoring. Spyware programs can collect various types of personal information, but can also interfere with user control of the computer in other ways, such as installing additional software, redirecting Web browser activity, or diverting advertising revenue to a third party.*

*Adware is software with advertising functions integrated into or bundled with a program.*

- Wikipedia

In a related article (*The Anti-virus Conundrum*) I stressed the importance of having an anti-virus package installed on your PC, and the **extreme importance** of keeping it current with updates from the publisher of the package.

Unfortunately, many people who do appreciate the need for such precautions fail to make an important distinction—one which leaves them exposed to threats they mistakenly believe they are protected against.

You see, while a good anti-virus program can detect and deal with many variations on the virus/trojan/worm theme, it can't handle all variations. An anti-virus program is a good start, but you can't stop there. Into your defensive line-up you must add a few more specialized scanner-type programs to catch some of the threats the anti-virus program can't handle.

It is beyond the scope of this article to delve into the differences between virus, trojan, worm, adware and spyware, nor is an understanding of the characteristics of each necessary in order to effectively combat them. For the more curious reader, my book *The Hacker's Nightmare*<sup>™</sup> deals with all threat types in some detail.

With regard to virus, trojan, worm, spyware and adware it is important to appreciate that:

- (a) All variations are extremely prevalent;
- (b) There are differences between each type of threat;
- (c) There can be further (sometimes significant) variations within each category;
- (d) There is no single antidote that will protect you against all types of threat.

For the average home and small business computer I generally recommend against the all-in-one security suites that purport to offer protection against a multiplicity of threats, so in that context point (d) above is still a valid observation.

A suite is a software package that embodies several modules, each intended to protect against a specific threat (E.g. an anti-virus module, a spyware/adware module, etc.)

My reason for recommending against suites is that, in my experience, you do not find the best of each type of protection bundled together. Because a developer may produce a very good anti-virus product does not necessarily mean they can do as good a job with, say, an anti-adware solution. For my money there's a lot to be said for implementing a series of smaller best-of-breed utilities that, matched task for task, can usually out-perform the equivalent component parts of an integrated suite.

## Adware and Spyware Protection

---

Now while the protective programs I use and recommend are extremely effective, they aren't all perfect. Sometimes we need to install two programs of the same type, because often one will catch intrusions that the other won't, and vice versa. These programs are usually quite small and don't place any significant load on the computer, so the extra protection is very worthwhile. A good example of this multi-application recommendation is adware/spyware detection.

Until recently the usual recommendation from "those in the know", myself included, was to install two spyware/adware scanners: *Spybot-S&D* and *LavaSoft AdAware*. It had been observed over time that no single scanner utility would ever detect all the infestations of this class that could be lurking on a PC. Those two programs were widely considered to be the best of their type and—so we thought at the time—would together detect the vast majority of adware problems.

I have no doubt that those were once well founded assumptions, but things have changed. Spyware/adware has become more sophisticated, new detection software has appeared, and some of the "old faithful" developers have failed to keep pace.

It wasn't until a qualified independent reviewer conducted thorough head-to-head testing of all the major spyware/adware scanners that we had empirical data on which to base our recommendations.

Eric Howes of the University of Illinois compared and tested more than 20 of the most popular and best respected spyware/adware applications, against hundreds of threats, and the results took a lot of us by surprise.

*AdAware SE* came in 3rd and *Spybot-S&D* was equal 7th. Not too bad, you might think, for a couple of free utilities, but the disturbing thing was the actual detection figures.

*Spybot* detected a mere 33% of the hundreds of adware components tested for, and *AdAware* didn't fare much better at 47%. There was some overlap of course, and in the final analysis those two combined could only come up with 54% of the total infections.

This is not the place to discuss Howes' results in depth, but I do need to make new recommendations based on his research.

In Howes' tests *Giant AntiSpyware* had a detection score of 63% and *Webroot Spy Sweeper* was next best with 48%. Combined they had a rate of 70%, by far the best of any possible combination of two packages.

Giant Software was acquired by Microsoft in December 2004 and the software that was tested by Howes was renamed *Microsoft AntiSpyware*, and later still changed to *Windows Defender*. At this time it is a free download. *Webroot* is a commercial product, but very inexpensive.

All such software provides a number of configuration options. If configuration options are offered you should take that as a strong indication that you won't get the most out of the application until you set those options.

Like your anti-virus program, it is extremely important that both *Microsoft AntiSpyware* and *Webroot Spy Sweeper* are updated regularly with new database information from their respective websites. These programs are very good at finding, identifying and eliminating certain types of nasties that your anti-virus program cannot detect.

There is another very important tool in this category that I always have installed on my computers. *SpywareBlaster* from Javacool Software does not scan for and clean out

## Adware and Spyware Protection

---

spyware; rather, it's job is to prevent such threats from ever getting installed in the first place.

*SpywareBlaster* is available in a free version for non-commercial use, but I do not recommend the free edition even if you do qualify for it.

Like the other applications we have discussed, *SpywareBlaster* must be regularly updated. While the free version can be \*manually\* updated at any time, it has no provision for auto-updating. For a paltry US\$9.95 per annum licence fee you can have the very significant advantage of scheduled auto-updating. There's no misprint there, you get change from ten bucks for an entire year's use.

Remember, such applications are only as good as their last update, and you certainly don't want to be relying on old data for your protection.

Product sources:

Microsoft AntiSpyware	<a href="http://HackersNightmare.com/MSAS">http://HackersNightmare.com/MSAS</a>
Webroot Spy Sweeper	<a href="http://HackersNightmare.com/WebRootSS">http://HackersNightmare.com/WebRootSS</a>
<i>SpywareBlaster</i>	<a href="http://HackersNightmare.com/SpywareBlaster">http://HackersNightmare.com/SpywareBlaster</a>

-oOOo-

Bill Hely is a technologist, consultant and author living in Brisbane, Australia. For most of the last two decades his professional focus has been on advising and supporting small business operators in Information Technology and Office Productivity issues. He is the author of several books on technology for the business operator, including the Bible of Internet and computer security *The Hacker's Nightmare*™.

To comment on this article please use the "Support" link at the bottom of the <http://HackersNightmare.com> main page.

Comments, suggestions, expressions of appreciation  
— and especially testimonials —  
are most welcome.