Spyware: is it all bad?

Ivan Trundle

Manager, communications and publishing
ivan.trundle@alia.org.au

Last month's article on spyware generated much interest and discussion on the topic. As a result it seems timely to continue the debate.

First we had hardware (well before computers arrived, too), then software, and wetware (sometimes referred to as the living organism that uses the latter two 'wares'), and now we have spyware. The term generally refers to computer code written to surreptitiously monitor your actions, and which is secretly deposited on your computer's hard disk to either record or broadcast activity — with or without consent.

In amongst all of this, there is also 'adware', or software that has similar characteristics but which is often combined with code which forces the computer user to either view or respond to advertising (pop-up advertisements are the most prevalent form). Other types of malicious software can take over a computer to send spam, or to copy and broadcast e-mail address books, confidential information or, more recently, encrypt the hard disk's data and hold the owner to ransom for a sum of money (truly!).

In essence, all of these activities sit in the 'malware' basket: code that is designed to do things that the owner of the computer would not approve of — if he or she was aware of what was happening.

However, and although national and international legislation is either enacted or pending which can both define and outlaw such activities, making malware illegal is not going to make the problem go away overnight. It hasn't worked for spam, either. Nonetheless, the Australian Government recently issued a spyware discussion paper, for comment and public consultation (consultation period was from May to 17 June 2005).

Spyware has existed for quite a long time, and sometimes for legitimate purposes. Not all spyware is malicious. Consider this: Installing commercial software on a computer generally involves consenting to a range of conditions — generally so many that it won't fit on a screen, and requires scrolling — wrapped up into an end-user licence agreement (EULA). How many people actually read the agreement before clicking the 'I agree' button?

In many instances, the EULA will inform you that your agreement indicates consent to install spyware. Of course, it might not use the term 'spyware' at all, but rather refer to the act of sending system information to the software company in order to ensure that the software is either up-to-date or being used legally. An example: Adobe (a very large software company) offers demonstration copies of its popular software suite — Photoshop, InDesign and Illustrator — as a free 30-day 'tryout' install. Upon installation, you are presented with a typical EULA, but in the process of installation, files are secretly deposited on your hard disk, which time-stamp the installation. Fair enough, you might say. But what if you wanted to try the software again, months later, because you simply didn't have time at first install? It can't be done, because of the hidden data. And even if I uninstall the software, the hidden data remains.

Other examples abound: alterations are often made to the hard disk on which software is installed to either 'phone home' or to record an action for later reference. This practice has only accelerated now that malware authors have a better understanding of how operating systems work. Or don't work. Moreover, the act of gathering data from the hard disk is now much easier than ever before, thanks to the sloppy security decisions made by operating system vendors. Even some anti-spyware tools install malicious code!

The discussion paper released by the Department of Communications, Information Technology and the Arts (DoCITA) suggests that the term 'without permission' should be the arbiter of what is secret and what is not. This is flawed reasoning, since almost no-one reads the EULA to which they grant permission — and if they did, the EULA is highly unlikely to give implicit indications of what files it deposits and what function they have.

It is likely that the conclusion of the DoCITA review will progress towards an education pack for at-risk Microsoft Windows users (because, fundamentally, the problems with spyware primarily revolve around a flawed operating system), but it is doubtful that it will be able to put any pressure on Microsoft to fix the situation.

There is no doubt that some spyware is, from the outset, of malicious intent. This should be legislated against, but it won't stop people from writing code.

There are three players here: Microsoft, the user and spyware makers. Microsoft have proved to be immune to prosecution, users are mostly naïve pawns, and malicious spyware makers can disguise themselves well enough to remain anonymous. However, existing legislation will prosecute malicious spyware makers — if they can be found and caught.

All that remains is to better educate computer users (which DoCITA proposes as part of the discussion paper), and for Microsoft to make a better operating system that is secure and immune to such threats. Or, for people to ditch Microsoft and find better existing alternatives — and there are a few. ■

...making malware illegal is not going to make the problem go away overnight.