Protection, Disclosure and Prosecution Provide Answer to Spyware Threats

A submission to the FTC

By Roger Thompson
Vice president, Product Development
Pest- Patrol, Inc.

PestPatrol, the authority in spyware protection, was founded in May 2000 by a team of security software professionals to counter the growing threat of malicious non-viral software. Today legislators and increasingly large number of consumers more readily recognize, and are beginning to understand the term spyware to describe these non-viral threats.

However while no one debates that spyware is becoming a relentless onslaught from those seeking to capture and use private information for their own ends (whether for financial gain or widespread disruption of business and government), there continues to be much debate about what constitutes spyware.

And while that debate ensues to find an acceptable definition for spyware that consumers, industry and government can agree upon and live with, we can count the cost that unfettered spyware is having on individual users as well as on corporate networks. As a security industry expert whose entire 25 year career has focused on first anti-virus software and then the emerging threat of malware, I believe that unless actively addressed now, spyware has the ability to threaten the very nature of the Internet and successful ecommerce, making it much more than a consumer “nuisance” issue.

Regardless of whether we agree to divide the term spyware into various subsets such as adware or malware, to indicate varying levels of odiousness, the truth is that any software application, if it is downloaded unknowingly or unwittingly, and without full explanation, is unacceptable and unwelcome.

At PestPatrol we have come to define spyware as any software that is intended to aid an unauthorized person or entity in causing a computer, without the knowledge of the computer’s user or owner, to divulge private information.

That should apply to legitimate business as much as to malicious code writers and hackers who are taking advantage of spyware to break into users’ PCs.

The dangers of spyware are not always known and are almost never obvious. Usually, you know when you have a virus or worm – these problems are “in your face”. Spyware, on the other hand, silently installs itself on a PC, where it might start to take any number of different and unwanted actions. For example:

- "Phone home" information about you, your computer and your surfing habits to a third party to use to spam you or push pop-up ads to your screen
- Open up your computer to a remote attacker using a RAT (Remote Access Trojan) to remotely control your computer
- Capture every keystroke you type – private or confidential emails, passwords, bank account information – and report it back to a thief or blackmailer
- Allow your computer to be hijacked and used to attack a third party's computers in a denial-of-service attack that can cost companies millions and make you liable for damages
- Probe your system for vulnerabilities that can enable a hacker to steal files or otherwise exploit your system.

Today large numbers of captured personal computers are being mobilized into "Bot Armies" and used to launch highly organized Distributed Denial of Service (DDoS) attacks aimed at disrupting major business or government activity. Individual PC users are never aware that their machine is being used to disrupt internet traffic, and that spyware on their PCs has made access to their computers an "easy-in," for writers of malicious code. And that right now, there is little or no recourse to a legal solution even if the occurrence can be monitored.

Spyware, adware and even some legitimate commercial software can be hijacked to create "backdoors" into users' data, enabling passwords, credit-card numbers and other critical data to be stolen. Identity theft is happening every day, to more and more people, many of whom have little or no idea how or when their information was stolen.

Many PC users have unwittingly loaded, or unknowingly had spyware downloaded onto their computers. Either by clicking yes in response to a lengthy and often extremely technical or legalistic end user licensing agreement, or simply by surfing the web, where self-activating code is simply dropped onto their machines in what is known as a "drive-by-download."

This misuse of technology and hijacking of spyware is just one part of the spyware picture. The costly side affect spyware has on PC functionality is the other, and cannot be discounted.

Testing earlier this month at the PestPatrol research laboratory revealed that the addition of just one adware pest slowed a computer's boot time (the amount of time it took to start up and function) by 3.5 times. Instead of just under 2 minutes to perform this operation, it took the infected PC close to 7 minutes to start up. It may not seem much in terms of seconds, but start to multiply that by any number of PCs and you have a huge productivity sink hole. Add another pest and the slow-down doubles again.

We also tested web page access, and again it took much longer once a pest was added to a clean machine. Almost five times longer in fact for a web page to load on an infected PC. The pest also caused 3 web sites to be accessed, rather than the one requested, and caused the PC to transmit and receive much greater amounts of unknown data – 889

bytes transmitted compared to 281 transmitted from the clean machine, and 3086 bytes received compared to 1419 bytes received by the clean machine.

Lost productivity nation-wide due to unnecessary consumption of bandwidth on individual PCs, and the necessary labor cost in rebuilding systems to ensure they are no longer corrupt is virtually unquantifiable. System degradation is time consuming for the individual pc user and even more so for network administrators managing corporate networks. Even new PCs straight from the factory come loaded with thousands of pieces of spyware, all busy "phoning–home" information about the user and slowing down computing speeds.

Users do not invite this spyware onto their machines and should not have to live with it. Clearly this level of infestation is stepping out of bounds of what is fair and reasonable.

We contend that only a combination of consumer education and protection, disclosure through legislation, and active prosecution will provide the answer needed to address to the spyware threat, right now. None of these solutions by themselves is enough, and while we advocate and applaud industry self-regulation, we do not believe that it alone will be speedy enough or dramatic enough to address the spyware problem.

Education and Protection. Any individual or business connected to the Internet today has to realize they are part of a complex network that is inextricably intertwined. Creators of spyware take advantage of that fact, plus the knowledge that most PC users are not sophisticated technologists. As an industry, we have begun to make computer users aware of the spyware threat by the creation of and active outreach by several groups and organizations. PestPatrol for example is a founding member of the Consortium Of Anti-Spyware Technology (COAST) group – a non-profit organization of several anti-spyware companies and software developers who are committed to best practices.

Consumer education about spyware and promotion of comprehensive anti-spyware ssoftware aimed at detecting and removing unwanted pests, in the same way as the industry has been advocating the widescale use of anti-virus software for the past decade are fundamental to our outreach. Nonetheless, we also acknowledge that consumers, precisely because of the insidious nature of spyware, can only do so much to protect themselves, and cannot be responsible alone for controlling the spread of spyware.

Disclosure Legislation. All applications, including those that are bundled and downloaded along with free software and with legitimate commercial applications, should be readily identifiable by users prior to installation and made easy to remove or uninstall. It is this transparent disclosure, and the ability of consumers to decide what does and does not reside on their systems, that needs to be legislated.

Consumers should have the ability to make fully informed decisions about what they choose to download onto their machines, while understanding the implications of doing so. They should also have the ability to easily and permanently remove those same

applications, if they determine that they are unwelcome. Legislation such as H.R. 2929, the Safeguards Against Privacy Invasions Act and the "SPYBLOCK" Act ("Controlling Invasive and Unauthorized Software Act") are aimed at making this happen.

At the same time it is incumbent upon those businesses creating and using spyware, and who are amongst those calling most loudly for self-regulation, to voluntarily respond to consumer concerns about loss of privacy and a compromised computing experience. By creating simple and easily understood user licensing agreements that fully disclose all files before they are downloaded, as well as their source and their purpose, and by providing an easy way to completely remove any applications, spyware (or adware) developers will be helping the entire industry.

Ultimately the decision by users whether to download freeware or to use P2P networks for example, should remain with users. Consumers will judge in the marketplace whether they are prepared to pay the cost of reduced performance or the intrusion of pop-up ads and changed home pages, or even the potential for identity theft. Users ultimately will have to make a determination whether a particular application is consuming more resources, or creating more risk, than is acceptable – while remembering that it is a shared risk.

Aggressive Prosecution. The deceptive practices employed by many spyware developers are already illegal under existing laws against consumer fraud and identity theft. Law enforcement agencies at the federal and state level should be encouraged however to more aggressively pursue and prosecute those who clandestinely use spyware to disrupt service, steal data or engage in other illegal activity. A greater focus on spyware and the necessary allocation of resources to pursue this criminal activity is vital.