

## **Spyware, adware, greyware, riskware – what's the difference?**

One of the more widespread problems in today's online world is spyware - something that affects both consumers and enterprises. Industry analysts suggest that up to 60 percent of computers may be infected with one type of adware, greyware or spyware meaning that the problem is particularly widespread. This article aims to clarify for the reader the difference and illustrate with examples.

### **Defining spyware:**

Spyware can be classified as a malicious kind of software that intercepts or takes partial control of a computer's operation without the user's informed consent usually for commercial gain. Spyware usually enters a computer through deception of the user or through exploitation of software vulnerabilities. Broadly speaking it is software that subverts the computer's operation for the commercial benefit of a third party. Unlike viruses, it does not usually self-replicate.

### **Riskware**

"Riskware" describes programs that are legitimate in themselves, but which have the potential for misuse by cyber criminals: for example, remote administration utilities. Such programs have a much higher profile thanks to such cases as Sony BMG's much-publicized XCP-system where rootkits were installed via a large number of Sony BMG music CDs unbeknownst to the buyers in an attempt by the company to enforce its copy control policies. Quite apart from the fact that users were effectively being spied upon through a legally purchased CD, the inherent risk created by this action was the possible backdoor it opened for viruses (or any other malicious program) to use the rootkit to hide themselves on the machine in question.

### **Adware**

There are different types of adware – the legal type where users consent to its presence in their computer to allow advertising companies to gather legitimate market data and the illegal type where they do not. In between is greyware where the program is tacitly accepted by the user but contains more inclusive and invasive monitoring of online activity. At the other end, illegal adware enters a user's computer with or without consent, hijacks the browser and starts directing traffic to certain sites or initiating pop up windows, all of which use up system resources.

### **New developments – Rogue antispyware**

Recently, spyware has also come to include "rogue antispyware" - bogus programs that present themselves as security software. In these instances, a trojan or website uses a false and misleading advertisement to trick a user into installing such a program. Typically, the program offers to scan the computer for spyware for free, but removal requires it to be purchased. Detections are often false and the removal of the so-called spyware isn't necessary. Despite their appearances, such programs function rather poorly and have no company behind them. As a result, users are left with spyware on their computer that will continue to leave them vulnerable to other malware attacks with no guarantee of future service.

### **The results of spyware**

The typical tactics of spyware infecting a computer is to include delivery of unsolicited pop-up advertisements without user intervention in the least problematic cases to theft of for instance credit card details for consumers or intellectual property from companies in its worst instance. In all instances, spyware is almost always an unwanted parasite on your computer and the more you have, the more unwell the computer will be. For badly infected systems, a complete reinstall may be required to restore the system to working order. This is a time-consuming project even for experienced users and does not discount the possibility of lost data as well as accompanying financial and intellectual property theft.

**What you can do to stop spyware**

The majority of spyware exists as a direct failure of ordinary users to think critically when installing software. Clicking on agreements indiscriminately may lead to spyware entering your machine with your consent. Think twice before you click and don't forget to read the small print! Installing a web browser other than Microsoft's Internet Explorer (IE), for instance, Opera, Firefox or Netscape is also a good practice. Until now, Internet Explorer has offered an easy route for spyware to enter a computer because of its deep integration with the Windows environment and its scriptability. Internet Explorer is also a point of attachment for spyware in the form of Browser Helper Objects (BHO), which modify the browser's behavior to add toolbars, redirect traffic or monitor browser usage to display a targeted advertisement.

Good user practices aside, the obvious first line of defense are programs designed to remove or to block spyware. As is the case with antivirus software, antispymware programs require a frequently updated database of threats. As new spyware programs emerge, antispymware developers intercept them and make signatures, which enable the software to detect and remove the offending program. In the case of the Charter Business® Desktop Security products, the most frequent updates in the industry ensure that the average user enjoys a high level of coverage against the threats posed by spyware.

*To learn more, call 888.692.8635 or visit <http://www.charter-business.com/Desktop/default.aspx>*