The Spyware Battle

Privacy vs. Profits

A Special Report by Trend Micro

For the past three years, antivirus vendors have toiled over how to handle the removal of spyware – software that logs information on user activity, collects Web browsing histories, on-line purchases, etc. Spyware programs run in the background, with their activities transparent to most users.

Such technology is often utilized by advertisers to trigger pop-up ads that target a Web user's known profile based on their prior Web searches, browsing, on-line purchases and other information gathered. When utilized by companies for these purposes, the terms "grayware" or adware are often used because, though it is not wanted, it is also not inherently malicious as some spyware can be.

Spyware/Adware – Defined

Nuisance Spyware

In most cases, spyware is more an annoyance than it is a cause for alarm – the vast majority of spyware falls under the "grayware" category, and is utilized by advertisers to divert a user's Web browser to different Web sites, which trigger pop-up ads targeting a Web user's known profile based on their prior Web searches, browsing, on-line purchases and other information. Most end users find this type of grayware to be an invasive form of data gathering. A commonly heard concern over such grayware is the unwanted interruptions and associated loss of computer productivity. Furthermore, there are serious privacy concerns relating to what can be done with a user's personal data once it has been monitored and collected. Personal data collected by grayware can be sent over the Internet where it may be sold or distributed to others.

Generally speaking, in addition to the nuisance of the pop-up ads, browser hijacks, and the breach of user privacy inherent in spyware, another major negative effect of these programs is the system slowdown they cause. According to Ed English, Vice President and Chief Security Strategist at anti-virus and content security firm Trend Micro, "These ill effects can be significant. On a system with a good deal of spyware/adware installed – there can be *dozens* of programs on a single system – pop-up ads can be seemingly relentless, and system performance can be brought to its knees." Mr. English adds, "Oftentimes grayware is loaded onto a user's machine with neither the user's permission, nor their clear knowledge."

Malicious Spyware

However, the technology can also be used to other ends, such as gathering passwords, credit card numbers, and other sensitive personal information. Though this type of spyware is "rare",

compared to nuisance spyware (Trend Micro estimates that less than 5% of all spyware is the malicious type), the problem is still prevalent enough to be of concern.

According to a study by The Poinemon Institute, 84% of Internet users surveyed said their computers were infected by spyware in 2004.

There are two major concerns with spyware – its pervasiveness and the intent behind the code. Malicious spyware is written by *thieves*, with the sole intent of stealing your information and using it for profit – whether by using your password to steal money from your bank account, using your credit card numbers to make purchases, or stealing your identity (social security number and birth date are all they need!) to open their "own" accounts.

Spyware has also been used for industrial espionage. In a recent high profile case, trojan spyware was discovered harvesting emails and other confidential information from corporate computers and sending the information to a competitor. Even governments can be affected by spyware. In a recent report from the US Government Accountability Office it is reported that eleven of 24 agencies surveyed by GAO said spyware caused a loss of employee productivity or required increased use of help-desk support.

In contrast, nuisance spyware is written by "companies", looking to protect and maintain the estimated $1.4 to $2 billion market for helping marketers better profile potential customers, based on their on-line activities, interests, and behaviors.

The Legal "Gray Area"

Spyware/adware is sometimes referred to as "grayware" since, with the exception of the "Malicious Spyware" discussed above, grayware is neither inherently good nor inherently bad.

Most users view spyware/grayware as an invasion of their privacy and want it removed from their computers – and proactively seek out tools to intentionally block, remove, and prevent it from coming back. In response, grayware companies increasingly argue that their freeware products are *legal*, since users have agreed to install them by accepting an End User License Agreement (EULA). As a result, companies that produce security software have become subject to legal threats for developing and implementing solutions for spyware removal by companies that produce this software.

To provide their customers with the protection they want, computer security companies are striking back by seeking legislation that clarifies their rights to detect and block software that customers may not want on their systems and by educating users on the nature and effects of grayware and spyware.

User Education Is Paramount

Many countries throughout the world are reviewing cases involving spyware/grayware, and considering laws to help protect users. However, the laws will likely vary from country to country. And, regardless of whether spyware and grayware are determined to be legal or illegal, the laws will be unable to stop these programs at their source. Therefore, user education coupled with a strong technical defense is – and will continue to be – the first and best line of defense against unwanted programs on a user's computer.

Computer security experts at Trend Micro recommend that users carefully read end user agreements and understand just how far-reaching certain provisions can be – prior to clicking the "Accept" button. EULAs often include terms that authorize the software supplier to download and

install a range of other software on their systems at anytime in the future without further notice or consent. Some agreements effectively require users to waive all privacy rights and allow the software to monitor their computer use and capture all input, including passwords and PINs.

Users should be cautious against clicking "I Accept" buttons for EULAs that contain provisions that give the vendor the following rights or terms:

- The right of the vendor – as well as their current and future partners, affiliates, or other customers – to send the user anything they want at any time
- The right to utilize the user's Internet connection
- The right for the vendor – and others deemed appropriate by the vendor – to access the user's computer
- The right to upload files to and download files from the user's computer
- The right to install any third-party software on the user's computer without further review or acceptance
- Vague limitations on the right to de-install the software or other third-party programs once the "I accept" button has been clicked and limitations on the right to terminate the agreement
- Permission to gather personal data from the user's computer, with relatively few restrictions on what data can be gathered, the purpose for which it can be used, and with whom that data can be shared
- The ability to modify the terms of the agreement at any time – including the privacy provisions – with or without the permission from, or prior notice of, the user. In many cases, the spyware company attempts to make it the user's responsibility to check the vendor's Web site to see if any terms have changed.

Non-EULA Versions of Spyware

In addition to the above rebuttals to the argument that a EULA somehow validates the spyware industry, it's important to note that oftentimes spyware/adware does not even display *a EULA*. Some spyware programs are installed either via "drive-by downloads", bundled along with other programs, or by hijacking legitimate software. In these cases, spyware can be silently installed, without any knowledge of – or permission from – the user.

Ed English adds, "If a user visits a spyware vendor's Web site, the program can be expected to behave well, include an uninstaller, and a clearly-worded EULA. However, this is not sufficient to now call the business legitimate – because the Web site is *just one vehicle* for distributing the spyware. But know that, even if there exists a well-behaved version of the program that can be downloaded from the vendor's Web site, the same program can be bundled silently or attached to hijacked legitimate software programs, and other secretive means – without the presence of a EULA, an uninstaller, or anything else that would give grounds for its legitimacy."

So how and where do these versions of spyware come from? One well known source of spyware is from porn sites, which are notorious for downloading spyware with neither permission from, nor knowledge of, the end user. The owners of these sites know that most users don't want to admit to visiting such sites, and will therefore not say anything, even if the spyware *is* discovered. So the more taboo the topic, the more target-rich the environment is for spyware.

User Education Is A Key Weapon Against Spyware Threats

David Perry, Global Director of Education for Trend Micro, reminds users that to minimize their risk of infection, they need to understand safe Internet practices, to avoid many of the spyware "traps" discussed above. "Once the user is infected with these rogue versions, they are difficult to detect and remove. Their successful eradication will likely require professional tools from a security vendor", states Mr. Perry.

But users also need to understand the inherent risks of simply "clicking through" a EULA for *any* software they don't implicitly know and trust. As Mr. Perry goes on to state, "by understanding the magnitude of this threat and changing their behaviors accordingly, users can enjoy a rich on-line experience, while taking comfort in the safety that they haven't unintentionally opened their computers – and on-line lives – to people they don't know".

Looking Forward – The Solution

In addition to traditional "antivirus", the AV industry is evolving into a full "computer security" industry – with enterprise and consumer customers demanding more robust, preemptive protection from their security vendor.

Users need to defend and protect their right to remove whatever is on their computer – their own personal property – and to block automatic installation of any software. Users should *never* click on a EULA that contains provisions to the contrary, thereby giving spyware companies a legal argument that the user has *waived* his or her rights.

User rights and the continuous dedication of computer security experts cannot be overemphasized in this case – particularly because we know that this is not the end. In addition to spyware as it exists today, there will be new technologies that threaten users' privacy and personal information. It is up to computer security experts to remain committed to producing technology that will protect users' privacy in spite of the constant tide of new and ethically ambiguous methods.

It is the legal rights of the user – and the unremitting commitment of security vendors to user education – that will lead to successful protection against the threat of today's spyware, as well as its future derivatives.

About Trend Micro

Trend Micro Inc. provides centrally controlled server-based virus protection and content filtering products and services. By protecting information that flows through Internet gateways, email servers, and file servers, Trend Micro allows companies worldwide to stop viruses and other malicious codes at a central access point before they reach the desktop.