The Unsuspected Privacy Threat

Irina Nock Krishnan-Wittevrongel
Lee & White Consultants, Belgium

With the advent of the Internet as a powerful gateway to accessing unlimited information regardless of physical boundaries, privacy issues become the core concern for today's society. Indeed, despite the advantages imparted by this universal network, there is a dark side to its birth.

This article briefly addresses the technological menace of parasites or spyware, as one of the many threats to the privacy of an unsuspecting individual Internet user, and seeks to create a general awareness of this threat which will be the primary step in reducing such risk when embarking into the network.

What is spyware?

It is software which displays unwanted advertising and records a user's communications. It is also known as adware and is secretly installed on the user's computer when he installs certain software, or download games, music or movie clips. Spyware usually comes from free software although it is high time users realize that nothing is ever really free. It inhabits in the unsuspecting, uninformed user's computer, collecting the computer's resources and then passing on this information to ruthless companies who are voraciously cashing in on invading the user's privacy by such installation[1]. These companies are being paid to include such spyware in a user's computer.

Parasites are tracking users' surfing practices, exploiting their internet connection by sending this data to third parties, collecting sensitive information such as credit card numbers from infected computers, outlining users' shopping inclinations, hijacking browser start page or pages, watching while you work[2] and changing important system files. Once again, all this is done without the knowledge and consent of the user. The implications of these exploits on the privacy and security of the individual user are indeed clearly undesirable.

One example of spyware is *lop* - a family of programs which set the user's start page and Internet Explorer's search features to use the site lop.com or one of its clone sites - *samz.com saoe.com sbjr.com sbnl.com aavc.com acjp.com ebch.com ebdv.com ebdw.com ebjp.com*, to name a few[3]. It also creates a registry entry to load a file named mp3serch.exe every time the user re-boots his computer. This entry causes Windows to load the lop executable file each time the machine restarts. As such, it changes the user's web browser into an apparatus

[1] For example, seventy-six percent of Belgian computers connected to the Internet have been affected, according to a study commissioned by the US-based company, Symantec. For further information, see http://www.expatica.com/source/site_article.asp?subchannel_id=48&story_id=14270&name=Belgium+invaded+by+spyware
[2] http://news.bbc.co.uk/1/hi/technology/3669213.stm "Spying software watches you work"
[3] http://www.kephyr.com/spywarescanner/library/lop/index.phtml

offering them with an unlimited stream of lop selected links to click. The user becomes a visitor to lop.com with nearly every action he takes with his browser, whether it is searching for something, typing in an incorrect URL, or simply by opening a new browser window.

To make matters worse, some websites containing and installing such parasites go on to make a further profit from the user by offering a so-called helping hand of anti-spyware programs which presumably remove these parasites - but at a fee. The troubled user is therefore left without a real choice - be forced to pay to get rid of the spyware, or keep the threatening spyware if he is not ready to pay. Thus, he is initially fooled into downloading a program for free, and later, inevitably forks out money for the payment of the anti-spyware application.

Spyware vs Virus

A virus has a clear malicious intent, whilst spyware looks as though it has a legitimate purpose but does something malicious. The former causes deliberate damage to system software, data, or both, but spyware causes inadvertent damage - usually only to the system software.

How is spyware installed?

Spyware is being designed to automatically install when a user surfs a hostile Web site or responds to a malicious pop-up ad[4]. Notwithstanding, malicious e-mail attachment also persists and the spyware is installed on a computer by a virus or an e-mail Trojan program, although this is rare. There are also cases where a spyware component is concealed within an otherwise apparently useful program which is more often than not downloadable for free in order to encourage the unpresuming user. Indeed, it is frightful to think that industrial espionage can be carried out effortlessly by the mere monitoring of people's activities on the Internet.

Does the law protect the privacy of the user in such cases?

Laws protecting privacy have existed in Western countries for hundreds of years. As early as 1361, the *Justices of the Peace Act* in England provided for the arrest of peeping toms and eavesdroppers. Such legal protection has grown over the centuries - culminating in a stricter and more thorough safeguard at an international level in recent years owing to the genesis of information technology and the Internet.

The Council of Europe's 1981 Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data and the *Organization for Economic Cooperation and Development's (OECD) Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data* set out specific rules covering the processing of

[4] http://en.wikipedia.org/wiki/Spyware - A typical piece of spyware installs itself in such a way that it starts up every time the computer starts up (using CPU cycles and RAM, and reducing stability), and runs at all times, monitoring internet usage and delivering targeted advertising to the affected system. It does not, however, attempt to replicate onto other computers — it functions as a parasite but not as an infection.

electronic data. These rules afford protection of personal information at every step from collection to storage and dissemination.

Although the manifestation of data protection varies from country to country, the essence of it is that personal information must be:

- obtained fairly and lawfully;
- used only for the original specified purpose;
- adequate, relevant and not excessive to purpose;
- accurate and up to date;
- accessible to the data subject;
- kept secure; and
- destroyed after its purpose is fulfilled.

These legal principles can be seen in a number of legislations such as the United Kingdom *Data Protection Act 1998* and the Belgian *law of December 8, 1992 on Privacy Protection in relation to the Processing of Personal Data as modified by the law of December 11, 1998* implementing *European Directive 95/46/ECand the law of 26 February 2003*. The above legal principles implemented in national data protection laws of member states may prove to be a useful tool against spyware. A person or company who unlawfully obtains an Internet user's personal information through the monitoring of his activities on the Internet (by the secret installation of spyware in his computer) may be liable to a legal suit.

Notwithstanding, *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector*[5] was adopted to provide more specific rules and guidelines for member states concerning the protection of privacy and personal data in electronic communications, including the Internet. The use of spyware and other privacy threatening technologies was also addressed.

The Directive acknowledges the serious intrusion on the privacy of the unsuspecting user and has affirmed that the use of spyware, amongst others should only be allowed for legitimate purposes, as prescribed in the Directive, with the knowledge of the user concerned.

Article 5(3) of the *Directive* provides that:

"*…the use of electronic communications network to store information or to gain access to information stored in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned is provided with clear and comprehensive information in accordance with Directive 95/46/EC, inter alia about the purposes of processing, and is offered the right to refuse such processing by the data controller…*"

For website owners, this must be complied with through privacy statements which should be available on the home page or in fact, in every page which collects data.

However, most privacy threatening technologies are installed from the moment the user visits the particular site, and it would seem that websites must be forbidden from installing

[5] http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/l_201/l_20120020731en00370047.pdf

any spyware or other privacy threatening technologies until the user has indicated that he/she is aware of the information provided regarding the use and purpose of these technologies and his/her right to refuse such storage or installation.

Belgium has finally filed a draft law[6] implementing the Directive, but it remains to be seen how far it will go in applying the framework provided.

The US is also not without its own set of laws. Federal and state governments are fiercely fighting against spyware by implementing legislation which will help curb this technology's invasion of privacy[7]. As of January 1, 2005, The State of California's *Consumer Protection Against Spyware Act* bans the installation of software that takes control of another computer and compels companies and websites to disclose whether their systems will install spyware. Damages up to USD1000 may be claimed if a consumer has fallen victim to the invasive spyware[8].

The judiciary is slowly but surely playing an important role in the fight against spyware as well. The US District Court of New Hampshire recently entered a preliminary injunction requiring that Seismic Entertainment Productions, SmartBot.Net, Inc. and Sanford Wallace, who are among the defendants, to cease exploiting security vulnerabilities to force software onto Internet users' computers without their authorization[9].

Although legislation is still new, and the courts are gradually moving in against the offenders, the fight against this unsuspected privacy threat has indeed begun and only time will tell how effective our laws are in regulating spyware.

[6] 4 November 2004
[7] http://www.ecommercetimes.com/story/US-Getting-Serious-About-Spyware-Laws-38680.html
[8] http://news.bbc.co.uk/1/hi/technology/4132143.stm "California sets fine for spyware"
[9] http://www.cdt.org/

How can we avoid it practically?

- ✓ **Run an anti-spyware application**

It is best for a user to conduct scans on his computer via an anti-spyware application to detect and destroy spyware on a regular basis. Sometimes, it is advisable to install two or more of these programs and run each of them for varying results. Ad-aware SE Personal from Lavasoft and Spybot Search & Destroy are two trustworthy and reliable applications to be considered.

- ✓ **Beware of P2P (Peer-to-Peer) File Sharing Services**

Many of the most popular applications include spyware in their installation procedures. Also note that a lot of 'free' illegal software obtained through these services are modified to include spyware.

- ✓ **Be suspicious of "free" software**

Many freeware software programs contain spyware. Before downloading any "free" programs, some research should be conducted to determine why someone is giving the software away for nothing "Free" software available on the Internet has the tendency of coming infested with spyware.

- ✓ **Avoid visiting certain types of sites**

Some web sites - especially "adult" sites, warez sites, sites for hackers and crackers, and some "free" online journal or diary sites -- endeavour to plant spyware on a user's computer. These sites seem harmless on the outset, but the effect on the user's privacy and confidentiality is real.