Diabologic: The Invisible War
by Frank Dolinar

Spam takes your time & energy, and adds to your frustration. But it can be dealt with.

Regrettably, there are more serious threats that attack and exploit your information resources without your consent or even your knowledge: like viruses, worms, phishing, and spyware – not to mention e-mail fraud, and denial of service attacks. Here are some definitions.

- A virus is a self-replicating program that spreads (much like a biological virus) by inserting copies of itself into executable code or host documents.
- A worm is similar to a virus, but can spread itself to other computers without a host file.
- Phishing is the attempt to fraudulently acquire sensitive information (e.g. credit card details) by masquerading as a trustworthy person or business with a need for such information.
- Spyware attempts intercept or take partial control of your computer without your informed consent. It typically subverts your computer's operation for the benefit of a third party.

Spyware does not usually self-replicate. It is designed to exploit the infected system for commercial gain, by delivery of unsolicited pop-up ads, theft of personal info monitoring web-browsing activity for marketing purposes, or routing browser requests to advertising sites.

According to a study done by AOL and the National Cyber-Security Alliance in October 2004, 80% of surveyed users' computers had some form of spyware, with an average of *93 spyware components per computer*. 89% of surveyed users with spyware reported that they did not know it was present, and 95% reported that they had not given permission for it to be installed. (The creators of spyware neither ask nor care that you didn't want their program to be installed.)

There are several ways for your computer to acquire spyware:

- Some spyware is delivered via a 'Trojan Horse'. The creator presents the program as a useful utility or a helpful software agent which users download and install, only to find out later that it is harmful.
- Spyware may be bundled with downloadable software and is installed with that software.
- You can be tricked into installing spyware by pop-up ads or dialog boxes.
- Some spyware infects your system by attacking security holes in your browser (especially Internet Explorer) when you load a page that forces the installation of the spyware.

So far, spyware appears to be principally aimed at Microsoft Windows operating systems. Linux and the Macintosh OS X have not yet been affected. My guess is that both Linux and Macintosh have small enough market share that it's not worth it to the spyware authors – that is, they don't get a big enough emotional payoff in attacking Linux and the Mac. Windows-based computers can rapidly accumulate many spyware components. Typical consequences of spyware infection (apart from the privacy issues) are:

- Substantial loss of system performance
- Major stability issues
- Difficulty in connecting to the Internet

Spyware infection is responsible for more visits to professional computer repair facilities than any other single cause. Often, the user suspects that the system performance, stability, and/or connectivity issues are related to hardware, Windows installation problems, or a virus – never suspecting spyware as the culprit. When a Windows-based computer has been heavily infected by spyware, the only remedy may be backing up all significant and data, wiping the hard disk clean of any software, and completely reinstalling the operating system. Not the typical user's first choice. A significant number of badly infected systems are simply replaced by their owners because the existing system "has become too slow".

Identifying and dealing with spyware is relatively simple, but does take some knowledge, time and diligence. There are several general techniques and some software that will help.

- Don't believe any popup that you didn't ask for. Malicious programmers have released fake anti-spyware programs that warn you of system problems, then direct you to purchase programs that don't remove spyware and may actually add more. (And you pay for this!)

- Use a web browser other than Internet Explorer. Mozilla Firefox has a cleaner interface, is easy to install and use, lacks Internet Explorer's vulnerabilities, and is, of course, free.

- Lavasoft's (www.lavasoft.de) *Ad-Aware* and Patrick Kolla's Patrick Kolla's (www.safer-networking.org/en/index.html) *Spybot Search & Destroy* are two reliable commercial anti-spyware programs that have rapidly gained popularity as an effective tools to remove, and in some cases intercept, spyware programs. Both are free.

- Gibson Research (www.grc.com) has a number of security tools, most notably Opt-Out and ShieldsUp. It's worth taking a look at the website.

- Buy, install, and keep up-to-date a good anti-virus product from a reputable firm such as Symantec or McAfee. Both have recently added anti-spyware features to their products.

Special Note: If you can afford it, buy a low-end computer that you never intend to connect to the Internet. Use it exclusively for your personal and financial records.

If you use your computer on the Internet, it is constantly being attacked. And, through it, so are you. The dangers are real. What are the documents and data on your computer worth to you? Think of the cost (time and money) required to recover or replace that content.

You owe it to yourself to learn about these threats and to understand what you can do to protect your assets, such as your identity, your finances, and any other data personal or business data you keep on your computer.

Make no mistake. It is not an exaggeration to say that there is a war being waged in cyberspace.