

Spies in our Midst

Safeguarding your systems in the age of spyware

By Charles Bennett, MBA
Principal Consultant, Triella



It could happen to you – and your law practice. A lawyer visits a client and connects his laptop to their network. Unbeknownst to him, a piece of spyware running rampant on the client's network is transmitted to his laptop during the connection. When the lawyer returns to the firm and reconnects (which sidesteps the firm's normal security defenses), that spyware is quickly introduced into the internal network and begins its invasion. This is just one example of a very real and worrying security dilemma that more and more firms are facing. How safe is your practice from spyware today? And how can you be sure that it remains safe tomorrow?

Spyware Defined

It's a buzzword we've all heard ... but what is spyware and how does it work? Spyware is a class of malware: malicious software programs designed to perform undesired actions on your computer without your knowledge. Once loaded on your system, spyware tracks your activity and reports back to a central location that can then, in turn, act on the information it receives. With 'Adware' (spyware developed for advertisers) the effect is more intrusive than harmful. Here, the information tracked allows these advertisers to tailor annoying pop-up ads to your browsing preferences. *See sidebar Types of Malware.*

A Growing Threat Motivated by Profit

Spyware is one of the fastest growing threats on the Internet. The number of websites distributing spyware has quadrupled since the beginning of 2005. Today it stands around 300,000 unique URLs and growing, as spyware purveyors expand their distribution channels and enter new markets. The motivation for this new breed of Internet invaders? Profit. Whether it's a penny per pop-up for an advertiser who is collecting and delivering valid email addresses to a spam marketer or a thief trying to gain access to a personal or corporate bank account. The latest malware sites are even taking advantage of the Katrina hurricane disaster in the name of making money. Known malware sites exploiting the Katrina storm that should be avoided include katrinahelp.com, katrinarelief.com and katrinacleanup.com. **Do not go to these sites!**

Is Your Computer a Zombie?

Some hackers are mobilizing networks of innocent unprotected 'Zombie' computers to attack a company they wish to blackmail. How does this happen? The hacker will anonymously call or contact an online casino or other

organization that depends on the Internet for revenue, as an example. "Send us a cheque for \$40,000 or we'll take your site down", they'll say. If the company does not respond, the hacker will enlist your computer as part of their vast network of zombies to make a direct attack on the web site of the business. They do this by getting thousands of computers in their malware-infected arsenal to send simultaneous requests to the business's website in order to overload the site so that it cannot process genuine requests.

TYPES OF MALWARE

- **Adware:** Programs that monitor the sites you visit in order to better target you with pop-up ads.
- **Browser Hijacking:** Spyware that hijacks your browser so that when you access Internet Explorer, you are directed to a site you did not request. Alternately, it can make your browser so small that it appears as if it isn't working. For many users, this can seriously hamper their ability to use Internet Explorer. Worse, it becomes nearly impossible for you to return your browser to its original settings.
- **Dialers:** Programs that focus on calling high cost long distance numbers, often off shore to run up your long distance bill and transmit stolen data. These threats are rare these days as most people have upgraded from dial-up modems to high-speed access. But beware if you still use a phone line to access the Internet.
- **Keyloggers:** Programs that record your keystrokes and send them off to hackers' sites. There are both general keyloggers and others designed to operate only when a secure site is accessed.
- **Phishing/Identity Theft:** Forged email ostensibly from your financial institution that asks you to update your password using an embedded link. Typically, you are sent to a phony bank site that looks very much like the original. Upon sign you will automatically begin providing confidential information to the hacker.
- **Rootkits:** Fairly new, difficult to detect programs that can be almost impossible to remove. The infected system will often require reformatting and reinstallation. The rootkit operates at the lowest level of the Windows operating system posing as a core system process. From there, it has the potential to control the entire system.
- **Spyware:** Programs that work behind the scenes to examine what you are doing on a computer and where you are going. This information can be used for targeted advertising purposes or to facilitate identity theft.
- **Trojans:** Malware embedded within a program that purports to provide a valuable function. The Trojan can spread viruses, load invisible keyboard loggers, install other malware, steal information by monitoring your online activity or turn your computer into a zombie.
- **Viruses:** Programs designed to harm your computer or give notoriety to its writer. They are usually in the form of programs that end with .com or .exe. Please note that most programs with these extensions are not viruses.

Sadly, a lot of this activity goes unreported, as few companies want to admit that they are victims of extortion. Many simply pay the money up front, rather than fight back and risk losing precious days of revenue through downtime.

Client Confidentiality is Paramount

Firms constantly work with confidential client information and malware means big trouble. If you are unlucky enough to be infected by malware, it could mean that a conduit has been established for a hacker to peer in to your network. Outsiders could have unlimited access to watch what's happening within your firm, including client files.

Surprisingly, current statistics show a growing awareness by law firms of the worsening spyware threat – but a shocking reluctance to take action. According to a recent survey¹, more than half of UK law firms think IT security threats – spyware and viruses in particular – are on the rise, but are taking little action in terms of increasing safety and investing in disaster planning. The survey actually showed that despite there being more than a one in ten chance of a UK law firm suffering a digital security breach over the last 12 months, more than half of respondents still ask colleagues to check their emails. One quarter never even change their password. We hope that Canadian law firms are more motivated to protect themselves.

Spyware Symptoms

The real problem with spyware – whether you are a small business, an individual or a law firm – is not knowing whether you are infected. As consultants, we have encountered many organizations experiencing a long list of network complaints they can neither understand nor rectify. Slow response time. An inability to get to certain websites. Corrupted files. In many instances, these are symptoms and side effects of spyware. Recently, we helped a company whose computers were completely unusable ... and subsequently discovered thousands of pieces of malware, including a dozen or so Trojan horse viruses, at the root of their problem. Unfortunately, there is no way to know how much information was lost nor, if it had gone unchecked, how it might have eventually impacted their business.

The Best Defense

When it comes to defense, a multi-tiered approach to protecting your system is necessary. Despite heroic claims and strong advertising, no one software Internet security program does it all, especially for a law firm's high security needs. In fact, at least one program we're aware of on the market actually

¹ August 2005 survey of 100 UK law firms, conducted by NOP World.

gives firms a false hope as it purports to stop malware but does a very poor job of it.

Keep Windows Up-to-Date

Most of the malware in circulation takes advantage of known and published vulnerabilities in Windows software. One good security measure is to keep your Windows up-to-date to minimize the chance of infection.

Download Mozilla Firefox

Another good defense is to download Firefox, a free browser that works in a similar manner to Internet Explorer. The benefit of loading it on your computer is that you have an alternate operational browser in the event that your browser gets hijacked. Firefox will also allow you to download the fixes needed to repair your computer should this be required. You can download Firefox at <http://www.mozilla.org/products/firefox/>.

Invest in Appliances

The latest highly recommended advances that work in tandem with your anti-malware software are called “appliances”. Every law firm should have them. Think of an appliance as you would a utility – a piece of hardware designed for a specific purpose that can be plugged in whenever you need it. Firms should specifically look at installing three types:

- an appliance that provides a firewall between your firm and the Internet
- a spam appliance to reduce junk mail
- a spyware appliance to remove suspected spyware.

In some cases, you can find one appliance that can handle multiple features – such as firewall defense with virus and spyware protection. This is certainly a viable option.

Appliances have many advantages for busy firms. They are kept up-to-date without staff/IT team involvement, there is no software to install and you can easily set a security threshold for the devices. Another benefit is that they pre-screen information before it gets to your firm’s server which means the server doesn’t have to use its cycles for non-business related work.

While appliances represent a slightly more expensive investment up front, they do a superior job and provide better security that will likely save you money and peace of mind in the long run.

THE SPYWARE MOST WANTED LIST

- **Clickoptimizer** -- tracks Web surfing habits and populates computers with pop-up ads. It might download third-party programs and usually installs via ActiveX downloads.
- **CoolWebSearch** -- a Web page hijacker that redirects web searches through its own search engine and might change Internet Explorer settings. It usually installs via malicious HTML applications or flaws in the Java Virtual Machine.
- **Elite Bar** -- a Web page hijacker that tracks Web visits and delivers pop-up ads on the basis of surfing preferences. It also can change settings. Its usual distribution method is with freeware.
- **Look2Me** -- a new breed of spyware that monitors Web surfing activity and reports to a centralized server. It updates itself and installs other spyware applications at the system level, making it difficult to detect and remove. It usually installs via ActiveX downloads and by vulnerabilities in common Web applications.
- **PowerScan** -- tracks Web habits and displays pop-up ads. It also can download and execute third-party programs without user consent. It usually infiltrates via ActiveX downloads from Web visits.
- **PurityScan** -- difficult to remove, it monitors Web surfing activity and reports to a centralized server. It updates itself and installs other spyware applications. It delivers pop-up ads and can degrade browser performance. It is typically bundled with popular peer-to-peer, music-sharing software such as Grokster and Kazaa.

Yearly Assessments by a Third Party Consultant

Appliances and security software, as we've established are certainly important. Your best defense against spyware, however, is an annual consultation by a third party consultant. Due to the rapid evolution of the number and kinds of threats, a firm would be ill advised to rely exclusively on their tools and internal technology resources to keep their client's information— and their own — fully protected. Even if you have purchased the right appliances and feel safe today, you may not be tomorrow. Most importantly, your systems might be infected already and you may not even know it! A skilled consultant will not only be able to set your mind at ease, he will:

- Assess your security risk
- Detect and remove malware
- Destroy/quarantine dangerous viruses
- Advise on a technology protection plan that's right for your business
- Evaluate the effectiveness of your entire technology infrastructure and make recommendations

Computers and the Internet are now an integral part of the way we do business. With the free flow of global information comes an onslaught of risks and dangers that grow more sophisticated each day. In order to keep our systems, businesses and financial data safe from attack it is essential to take defensive action. Only with the right combination of security tools and regular assessments by a trained third party technology consultant can your practice hope to protect the firm's data as well as the data of its clients from the prying eyes of hacker spies.

Charles Bennett is the President of Triella, a technology consulting company specializing in providing technology audits, planning advice, project management and other CIO related services to small and medium sized firms. He can be reached at cbennett@triella.com or 416.269.4368. For additional articles, go to www.triella.com.

© 2005, by Triella. All rights reserved. Reproduction within permission is prohibited.

###