The Spyware Threat And How To Deal With It

by Matt Piercy - F-Secure’s manager, UK & Ireland - Monday, 22 November 2004.

Spyware aka advertising-supported software or adware – has been until recently a fairly benign snooper on your surfing habits. The data it gathers is then used to target you with tailored advertising, either in pop-up windows or emails.

The problem is that these software spies are starting to get nasty. Spyware is being written and propagated with the express purpose of recording personal data such as passwords and credit card numbers, or hijacking your browser and bookmarking porn or other undesirable sites, or grabbing your web dialler. Some spyware even features self-updating code so that conventional freeware removal tools have no effect.

What’s more, unlike viruses and worms, most people with spyware on their computers have asked for it, albeit unwittingly. Many websites may ask you to register or sign up to them to receive content, and by doing so you may agree that spyware can operate on your PC – but this critical point is often buried in lengthy Ts & Cs where most users won’t see it.

Spyware everywhere

And it isn’t a small-scale problem. Research in the US in Spring 2004 showed that 1 in 3 PCs scanned had spyware hidden on its hard drive. A total of 650,000 PCs were scanned, finding more than 18 million spyware tools.

Nor is spyware confined to home users. The average amount of spyware on business machines is similar to home users’ – largely because most companies don't have centralised, managed anti-spyware protection in place. Certain spyware – such as that used by P2P networks like Kazaa – is also bandwidth hungry as it communicates a lot of data between machines, which can be a problem on corporate networks.

It’s becoming such a sizeable problem in the US that the Government voted unanimously in Spring 2004 to approve the first-ever anti-spyware bill. The Securely Protect Yourself Against Cyber Trespass (Spy Act), approved by the US House of Representatives, would levy fines up to $3 million for those who illegally collect personal information, change a browser's default home page or bookmarks, log keystrokes, or steal identities.

Evolution

So how has spyware been allowed to get this far without being restrained?

The key problem is that we have accepted spyware in a variety of forms for too long. A cookie – the website marketeer’s long time friend – is a form or spyware. Microsoft uses various forms of friendly spyware to help most of us in our everyday work, by tracking what documents and applications we’ve used recently and giving us quick, one-click access to them.

But in the same way that Internet worms evolved to take advantage of email, malware authors are now taking spyware away from its neutral roots into Internet crime – whether by hijacking browsers and diallers, keystroke logging or laying the groundwork for mass spamming. These authors are also using tricks from the virus world by finding and exploiting browser vulnerabilities to their advantage.

This means that spyware be installed even on a fully-patched Windows machine running the latest anti-virus software. A partial solution is to combine AV with a personal firewall – but even this isn’t a complete fix. Spyware can get installed through ActiveX which is enabled with MS Internet Explorer. Alternatively, it can exploit vulnerabilities that are patched in Internet Explorer – so-called zero day vulnerabilities because the loophole is exploited before the patch is available and widely deployed.

Disabling ActiveX is an option – but it makes surfing difficult because many websites actively rely on using ActiveX. It’s frustrating to have to click “Yes” every single time the web browser asks you about running ActiveX scripts and controls.

Managing the problem

So spyware has become both a security and a management issue for companies as it becomes destructive. But how do companies manage the problem? There’s currently a dearth of corporate anti-spyware tools which integrate with other security applications, such as anti-virus and desktop firewalling.

However, this is soon to change. Anti-virus vendors are starting to introduce spyware and adware pop-up blocking and removal to their core anti-virus and Internet Security solutions. These will be updated in exactly the same way as conventional virus signatures, and will give policy-based centralised management of this emerging issue – helping to nullify the threat from self-updating malicious spyware programs while giving IT staff the option to allow non-aggressive spyware.

By putting spyware on the security map, companies can ensure that the more malicious spyware elements do NOT come in from the cold.

Dealing with aggressive spyware

Use freeware tools to audit your PCs and identify what spyware is

- use freeware tools to audit your PCs and identify what spyware is resident.
- use the same tools to try and remove unwanted spyware: a combination of two tools often works where a single tool fails.
- look at latest-generation AV software which includes anti-spyware functionality, giving corporate, policy-driven spyware management of this emerging problem.