Internet News

Column Editor: Susan Miles;
e-mail: susan_miles_2002@hotmail.com

Ghosts in the machine

It's the season for ghosts, beasties and things that go bump in the night, or in my case, things that have taken over my IE settings! So, as much driven by unfortunate necessity as by a desire to prompt others to make sure they are well protected, here is an overview of the various nasties of computer/internet land with a few suggestions about how to protect yourself. I would expect corporate IS services to be on top of this sort of thing, so this is primarily aimed at the home user.

There are a range of terms which are frequently used to describe these pieces of software. There is some overlap between them, so that one particular piece of malicious software may fit into more than one category.

Definitions

Malware
This is a high level term and includes software such as Trojans that harms files on the disk, or attempts to place control of the machine in the hands of whoever distributed the software.

Spyware
This is another high level term, describing software installed with no disclosure that gathers information about the user of the machine and then sends this back to another server.

The following terms describe different categories of spyware.

Adware
Software installed, usually with limited disclosure, that mainly delivers ads. Some adware programs fit the definition of spyware if they also gather data about the user, either to sell to others or to make the advertising more relevant.

Stalking horses
Programs that enable adware networks to function on desktops, come bundled in many other downloaded programs. All will collect information.

Homepage Hijaker
A kind of advertising Trojan, these redo homepage settings without permission and spawn pop-up ads. Some edit your computer's registry to load themselves on restart to make it difficult to change things back.

Rogue Internet Diallers
These are pieces of dial-up software which, once downloaded, change the users ISP and dial-up internet connection to one using a premium-rate telephone line, often charging £1.50 a minute.

What can spyware get up to on my PC?

Unfortunately, it's more a case of what can't they do, rather than what they can do. Since much spyware are actual computer programs, they can be programmed to do anything that its creator wants it to do.

They can:

1. Perform a detailed check of your browser history
2. Install DLLs and other executable files
3. Send continuous data to the parent
4. Leave a backdoor open for hackers to intercept your personal data or enter your computer
5. Install other programs directly onto your computer without your knowledge
6. Send/receive cookies to other spyware programs, even if you have cookies disabled
7. Reset your auto signature, disable or bypass your uninstall features, monitor your keystrokes, scan files on your drive
8. Change homepages so that you can't change them back to your own preference [this is what has happened to me!].

This is not an exhaustive list but gives you some idea of their potential to wreak havoc on your computer.

Another problem with these types of software is that once installed they can be extremely hard to identify, cannot easily be deleted from your system using normal methods and often leave components behind to continue to monitor your behaviour and reinstall themselves.

How can I tell if I've been affected by any of these?

Typical symptoms that your computer has been infected include:

1. Unwanted pop-up adverts appearing (often of an objectionable nature)
2. New toolbars in your Internet Explorer that you didn't intentionally install
3. "Hi-jacked" home page
4. Slow running of the computer
5. Slow connections
6. Downloads failing

Even if you see none of these typical symptoms, you

maybe infected, because more and more spyware is emerging that is silently tracking your surfing behaviour to create a marketing profile of you.

How do I get rid of these nasties from my PC?

A whole market of software solutions has opened up to combat this latest and very serious threat to the security of your computer and personal data. There are very many commercial products available (see www.adwarereport.com/mt/archives/000004.html for a review); however you need to be aware that there are also a great many rogue pieces of software which will claim to have found malware on your machine, but instead of removing it, will actually install it! More details of this can be found in www.adwarereport.com/mt/archives/000007.html.

There are a number of non-commercial products available, the two most popular ones are:

1 Spybot – Search and Destroy (www.safer-networking.org/en/index.html)
2 Ad-Aware SE Personal (www.lavasoft.de)

Both these are used on our home computer, and we have found both products to be stable and to perform well under XP. To achieve the maximum benefit from them, you need to ensure that they have up-to-date definition lists, run both (just to be sure that you detect all you can) and use them with a real time monitor. Here again, there are many available, typically they are bundled with commercial spyware removal packages (including the full Ad-Aware product).

Non-commercial products include:
1 SpywareGuard
2 WinPatrol
both of which offer real time protection against further infection. They are available via http://www.spywareinfo.com/.

Anti-spyware/pro-privacy movement

Even a cursory examination of spyware and its friends is likely to raise concerns about the privacy of data and ones own computer. The pro-privacy and anti-spyware movements have developed in response to these concerns. I have discovered some comprehensive web pages by people involved in the pro-privacy movement, which might be worth a look if you're interested in delving into this whole subject further.

Bill Webb's 'Counterexploitation' website is at http://www.cexx.org/.

Browser hijacking
http://www.spywareinfo.com/articles/hijacked/
This article is from a website that also offers forums to help resolve infections by particularly persistent nasties. They have a comprehensive technical article outlining the steps to take to regain control of your browser.

Intranets and Content Management

Column Editor: Martin White
Intranet Focus Ltd;
e-mail: martin.white@intranetfocus.com
Getting it together

I am writing this just prior to flying to the USA to take part in Intranets 2004, which is organised by Information Today Inc. and run in parallel with KM World and CM (Content Management) World. It takes place in Santa Clara, one of the more unappealing parts of California in that most of the area around the conference centre is taken over by offices of the US network equipment company Cisco. You need a hire car just to go and have a cup of coffee away from the conference hotel/exhibition centre.

For the last couple of years one of the most popular early evening events has been an informal session of 'You show me yours and I'll show you mine'. We are talking intranets here! One of the big problems that intranet managers face is the difficulty in exchanging ideas about what works and what doesn't work. There are no intranet-specific conferences in the UK outside of some quite expensive seminars run by the Ark Group or by Marketing Week.

One of the issues that is associated with demonstrating intranets is that the content may give away confidential information about the company or organisation. Certainly this is an understandable issue, but certainly in the case of the showcases at the Intranets conferences the demonstrations show that you can manage the presentation to keep confidential information off the screen, and in any case there is a bond between the delegates that if they do spot something 'interesting' it stays inside the conference room.

There are many issues about intranets that perhaps do not require the full interactive demonstration. These might include ways of increasing intranet usage, the approach being taken to implement a content management system, and ensuring that staff