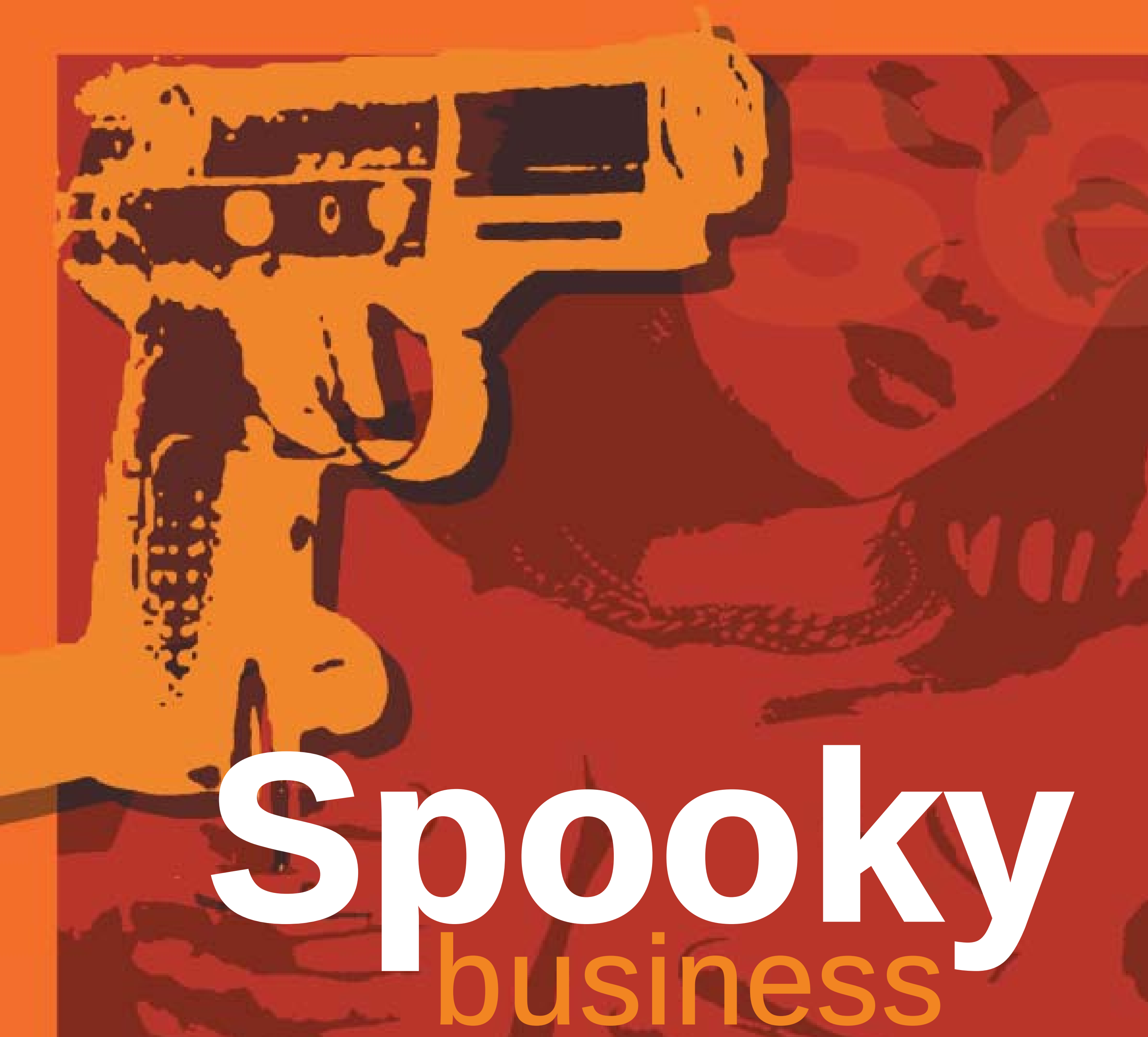


Spooky business

Spyware is set to become the scourge of the broadband era. Here in part one, Guy Dixon shows the extent to which third parties are monitoring your internet behaviour

This June saw welcome recommendations from the Information Commissioner calling on employers to notify staff should they decide to monitor their email or internet activity in any way. Failure to do so, they were warned, means they could fall foul of the Data Protection Act.

However no such guidelines exist for the home. While the issue of so-called domestic 'spyware' or 'snoopware' has received a lot of coverage in the US, it has drawn scant attention here in the UK.

The broadband era has ushered in an awareness about the threat of viruses and hack attacks – in other words, the dangers posed to your precious PC by overt forms of havoc. Yet we seem oblivious to the menace posed by individuals and companies that surreptitiously monitor every website we visit, every keystroke we make and every email we send.

ILLUSTRATION: SARAH AULD

cret

When the matter is raised it causes passionate debate. In a recent *PC Advisor* poll, some 61.5 percent thought it was wrong to snoop on the online behaviour of a partner or family member, deeming it an invasion of privacy.

But there is a clear demand for such products. Nearly one in 10 (9.1 percent) respondents indicated that they would use such surveillance to track their spouse, while getting on for a third (29.5 percent) said they would use it to keep tabs on their offspring.

Catch them red-handed

We're not talking about a quick trip to Internet Properties, where you can quickly check a user's History folder or cookie trail. We're talking off-the-shelf packages costing around £40 that will record a lot more than the occasional visit to an unsavoury website.

SpectorSoft's Spector is perhaps the best-known commercial 'snoopware' aimed at home users. It resides in your computer's memory and periodically captures snapshots of the desktop. You can either run it in Visible mode (complete with onscreen indicator) or in Stealth mode, where the user is completely oblivious to the application being in place at all.

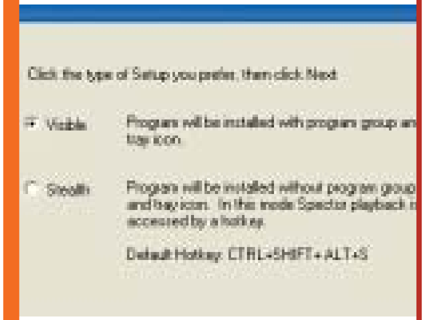
By typing a special key combination and an optional password – the default is Ctrl, Alt, Del, T but you can set whatever keys you like – Spector invokes a VCR-like display of actions the computer's user has taken, as well as log information and keystroke data.

Spector automatically takes hundreds of screenshots every hour, very much like a surveillance camera. It records everything from online activities such as chat conversations, instant messages, emails and internet surfing to which applications are opened and what is typed into them.

An options screen lets the owner of the program choose how often to take snapshots, what colour depth to record the grabs in, whether keystrokes should be captured and so on. Spector works by recording information in a specified folder inside the Windows directory. To keep curiosity at bay, the files it generates have uninformative and gibberish names such as '4f0bf6d8.tps'.

Spector: keeping an eye on things

1. Under Setup choose between Visible or Stealth mode



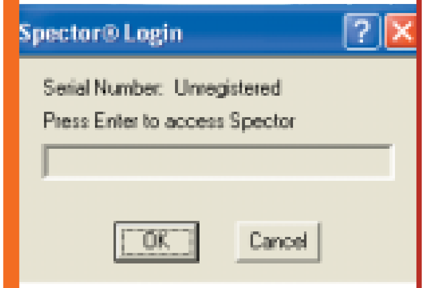
Click the type of Setup you prefer, then click Next

● Visible — Program will be installed with program group an tray icon.

○ Stealth — Program will be installed without program group and tray icon. In this mode Spector playback i accessed by a hotkey.

Default Hotkey: CTRL+SHIFT+ALT+S

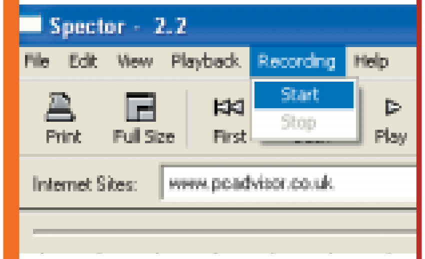
2. Enter the correct key combination and a login prompt appears



Serial Number: Unregistered

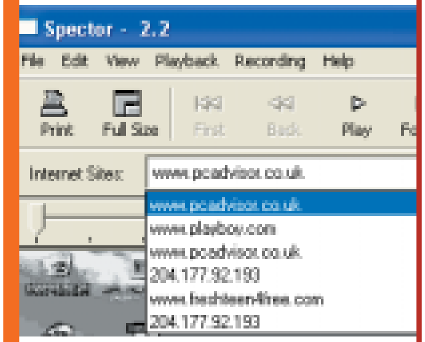
Press Enter to access Spector

3. Spector's VCR-style interface lets you record all PC actions. Select Recording, Start to begin monitoring



Internet Sites: www.pcadvisor.co.uk

4. Spector records all websites that the PC accesses, allowing you to monitor the user's surfing habits



Internet Sites: www.pcadvisor.co.uk

www.pcadvisor.co.uk
www.playboy.com
www.pcadvisor.co.uk
204.177.92.193
www.freshteen4free.com
204.177.92.193

Remote snooping

Data Spector gathers is accessed from the machine the program's installed on. That could be awkward if the person you're keeping tabs on uses the PC all day long. To solve this problem you can fork out an extra £60 for SpectorSoft's eBlaster which lets you snoop remotely from another PC.

The application sends messages containing Spector's findings to your designated email address. Reports include listings of each program executed right down to the user keystrokes. "Perfect for parents with kids away at school or paranoid fiancées," boasts the company's website.

As well as recording anything transmitted from the host machine, including popular chat software such as Microsoft Instant Messenger, eBlaster can automatically forward screenshots to your email address. It works over networks and dialup connections, providing the email account on the receiving end can handle attachments.

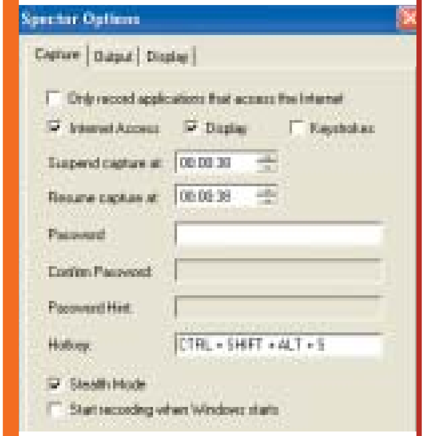
Windows XP's built-in firewall features can't detect eBlaster, although third-party products such as ZoneAlarm will. But a personal firewall is only a partial solution for someone being spied on as the snooper can always carry out an in-depth inspection whenever they gain physical access to the PC in question. Leaving few traces, your average user would have no idea their PC habits were being tracked.

Bring out your wares

Dubbed 'adulteryware' or 'pornware', packages such as Spector are used specifically by individuals on other individuals – usually concerned parents or paranoid fiancées. Perhaps more sinister are the other types of spyware that are likely to be routinely monitoring your behaviour. They fall into two categories: 'adware' and 'snoopware'.

Adware describes those irritating programs that fling pop-up ads on to your screen, install toolbars full of adverts or hijack searches and web surfing. Snoopware, on other hand, is far more underhand. These applications surreptitiously watch what you do, steal personal information and then despatch it to interested parties across the internet.

5. Under Options select the level of recorded detail you require – internet access, display, keystrokes or all three



Spector Options

Capture | Output | Display

□ Only record applications that access the Internet

☑ Internet Access ☑ Display □ Keystrokes

Suspend capture at: 00:00:30

Resume capture at: 00:00:30

Password:

Confirm Password:

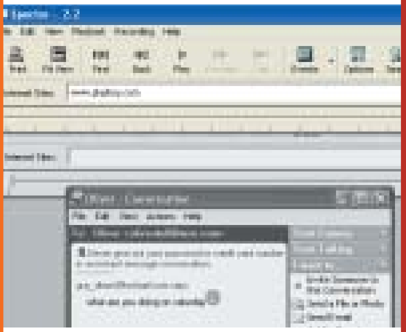
Password Hint:

Hotkey: CTRL + SHIFT + ALT + S

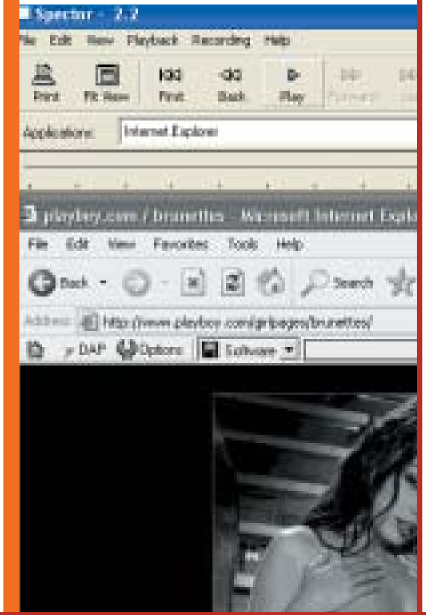
☑ Stealth Mode

□ Start recording when Windows starts

6. Spector records all applications including chat software such as MSN Instant Messenger



7. Play back all PC activity frame by frame


Spector - 2.2
File Edit View Playback Recording Help
Print Fit Here First Back Play Forward
File Edit View Favorites Tools Help
Back Search
DAP Options Software

Applications: Internet Explorer

playboy.com / brunettes - Microsoft Internet Explorer

Address: http://www.playboy.com/girlpages/brunettes/

Monitoring is largely carried out to establish demographic information which is then used to produce targeted marketing designed to fit your browsing habits. However some spyware goes even further than this, sniffing out files on your hard disk, logging whatever you type and actively paving the way for other software to be secretively installed.

Is antivirus software letting us down?

Antivirus programs combat the traditional threats of viruses, worms and Trojan horses but do little, if anything, about spyware installed by sneaky marketing folk.

One reason for the inadequate response from antivirus software developers is a wariness about defining spyware as malicious. In many cases these unsavoury applications are disclosed in the end-user licence agreements of the leading peer-to-peer software they ride in on. By accepting the agreement the user permits installation of the spyware. Details are often included in the small print that most people don't bother reading. In their desire to build up the music collection of their dreams, users click through multiple default agreements without fully comprehending the consequences of their actions.

Antivirus companies could easily guard against spyware in much the same way as they do against viruses by obtaining a sample of the malicious application, examining the underlying code and instructing the programs to look for the virus' unique signature.

In his book, *The Art of Deception,* hacker-turned-consultant Kevin Mitnick criticises the double standard that

Is spyware illegal?

Spyware in itself is not illegal. However privacy advocates are concerned that the user has no control over what data is being sent.

How does it work?

Advertising spyware hijacks the user's processor, RAM and bandwidth to connect to the internet. It then uploads whatever personal information it has gathered and proceeds to download 'targeted' advertisements using pop-up windows, based on its assessment of the user's tastes.

Why else might you want to be rid of spyware?

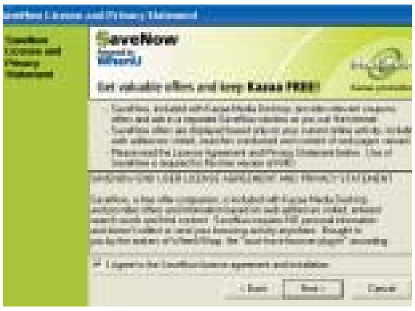
In many cases spyware applications are harmless marketing research tools. However if you allow one piece of spyware into your computer you may well be opening a future floodgate of the unwanted critters.

You could justify tracking down and destroying spyware purely in terms of inefficiency. Because they're clandestine applications, spyware effectively steals your hard disk space and memory, creating performance issues. The software programs are also often poorly written, which can cause computer crashes.

Who are the biggest distributors of spyware?

P2P (peer-to-peer) applications distribute the majority of spyware, particularly Kazaa – the world's most popular P2P network and officially the most downloaded piece of software ever.

File-sharing networks like Kazaa don't charge the end user, so the company looks for other means of attracting revenue. Installing multiple advertising spyware apps is one way of getting it.



SaveNow License and Privacy Statement

SaveNow

Get valuable offers and keep Kazaa FREE!

antivirus companies seemingly apply to viruses and to spyware.

"Antivirus software [treats spyware] as not malicious, even though the intent is to spy on people," Mitnick writes. That creates "the risk that each of us might be under illegal surveillance at any time".

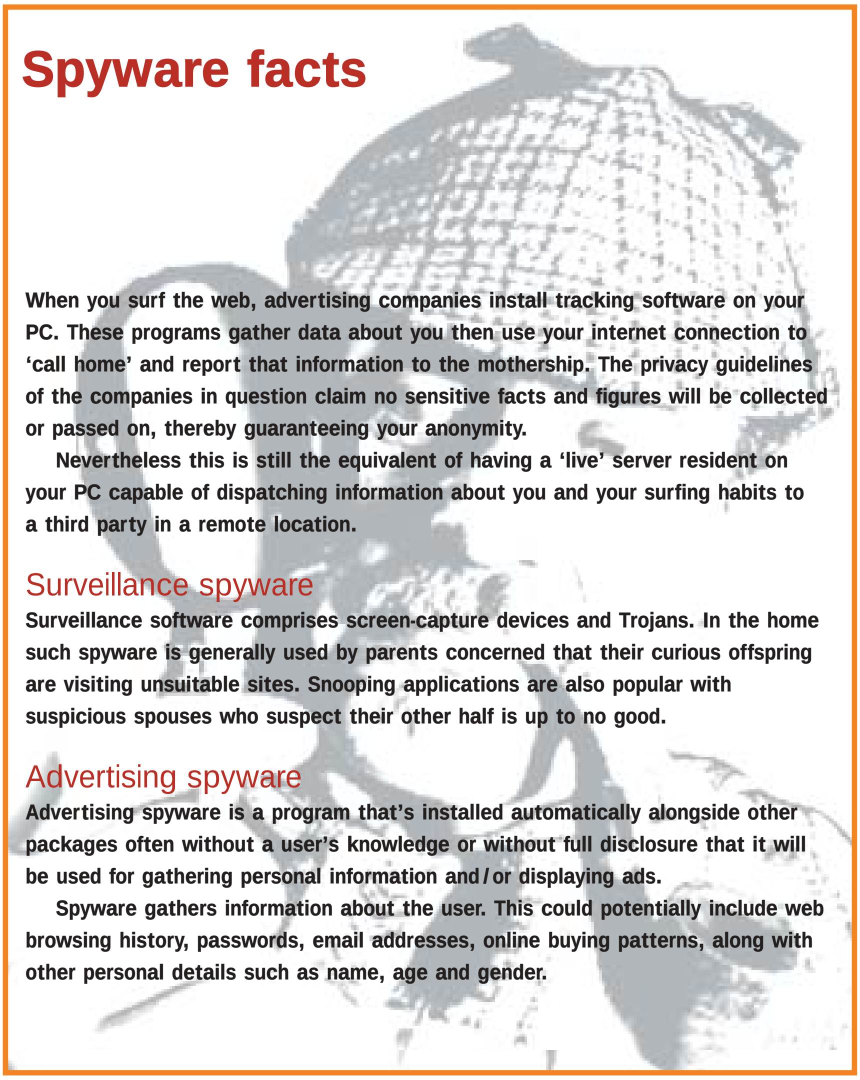
Turn detective

Until antivirus companies change their tune you will have to sniff out resident spyware in other ways. Most personal firewalls will alert you when a program attempts to access the internet, gagging spyware that emails personal information. And, for around £30, products such as SpyCop will specifically scan for all commercial snoopware applications.

In reality, however, the average PC user's only protection is an antivirus program. Isn't it time antivirus vendors at least offered customers the choice of guarding against the menace of spyware, thereby extending their armoury to include regularly updated means of countering such threats?

It's your right to know whether you're being spied on so be sure to read next month's Broadband advisor feature to find out how to fight back against snoopers. Even if you can't stop people keeping track of your habits, we'll show you how to tell whether you're under surveillance and how to respond accordingly. ■

Spyware facts



When you surf the web, advertising companies install tracking software on your PC. These programs gather data about you then use your internet connection to 'call home' and report that information to the mothership. The privacy guidelines of the companies in question claim no sensitive facts and figures will be collected or passed on, thereby guaranteeing your anonymity.

Nevertheless this is still the equivalent of having a 'live' server resident on your PC capable of dispatching information about you and your surfing habits to a third party in a remote location.

Surveillance spyware

Surveillance software comprises screen-capture devices and Trojans. In the home such spyware is generally used by parents concerned that their curious offspring are visiting unsuitable sites. Snooping applications are also popular with suspicious spouses who suspect their other half is up to no good.

Advertising spyware

Advertising spyware is a program that's installed automatically alongside other packages often without a user's knowledge or without full disclosure that it will be used for gathering personal information and/or displaying ads.

Spyware gathers information about the user. This could potentially include web browsing history, passwords, email addresses, online buying patterns, along with other personal details such as name, age and gender.

Top 10 spyware pests

The table below is drawn from a total of 300,663 pest reports from PestPatrol users for the month of June. This table reports on the most common pests in the All Spyware category (spyware cookies are excluded).

Pest	Count
VX2/a	68,491
SurfPlayer	66,729
DownloadPlus 1.0.6	9,392
Search-Explorer	8,609
WeatherCast	7,734
FileFreedom	5,767
FirstLook	5,157
ezCyberSearch	3,731
Mass Instant Messenger 1.7	3,255
OnFlow	3,248

Gathered from PestPatrol, last updated June 03