



## TECHNOLOGY INSIGHTS

These are our own opinions.

We have no commercial  
arrangements with vendors.

For more reviews, please  
contact TECHNOLEDGE.

T +61 2 9909 0246  
E [info@technoledge.com.au](mailto:info@technoledge.com.au)  
W [www.technoledge.com.au](http://www.technoledge.com.au)

## The Security Landscape A Guided Tour

### PART 2 - A SNAPSHOT OF THE CURRENT THREATS

**Viruses** are still in business. They were launched years ago by pimply college nerds in order to inflict random damage on the innocent. These nerds have grown up and some of them write spyware for businesses that sell your surfing habits to companies who want to tempt you with their offers. Others work for organised crime syndicates who want to gain access to your bank accounts or credit cards.

**Spyware** is big business. It's often transparent to the user, running quietly in the background. The ability to remain undetected is what makes it so dangerous.

Last year, *McAfee* launched a product called **Site Advisor** that pops up green, yellow and red lights next to items presented by search engines. A few months ago, the website posted a Spyware Quiz, which asked users to spot the safe site from five Web categories: screensavers, smileys (emoticons), games, musical lyrics, and file sharing (P2P). 97 % of participants failed the test. You can check your detection skills here: [http://www.siteadvisor.com/quizzes/spyware\\_0306.html](http://www.siteadvisor.com/quizzes/spyware_0306.html)

You can download **Site Advisor** from the same site, and there are several other products that warn you about dangerous websites (see [Driver Training](#)).

**Risky sites** have grown in leaps and bounds - in a year-long scan of over 4.5 million sites, a team at Google found code on 450,000 pages that could inject malware onto users' PCs via improperly-patched browsers. According to Google, the main attack vectors are web server security, user generated content, advertising and third-party software.

**Phishing** is bigger business. According to a US survey conducted by the *Gartner Group*, an estimated 109 million consumers saw phishing e-mails in 2006, compared to 79 million in 2005 and 57 million in 2004. 'They're getting better, much better, at their schemes,' *Gartner* analyst Avivah Litan said.

There are few figures on the number or cost of phishing attacks in Australia but, in the last three months of 2006 alone, consumers who registered complaints with the ACCC lost a total of \$2.3 million to internet scams and rip-offs. Many scams aren't reported, of course, since the victims are too embarrassed.

Financial institutions and online auction sites like eBay (and PayPal) are the most popular targets for phishers. If you want to check your ability to detect a phishing email, try this test: <http://www.sonicwall.com/phishing/>

### Beyond Malware

Phishing is crimeware and those caught at it face stiff jail sentences. That hasn't put the crooks off - they're simply getting smarter, coming up with more devious tricks and packaging them in new ways.

A **blended threat** is malware that combines different components, for example a virus that carries a worm or a Trojan with a keylogger on board. Using multiple techniques to attack PCs gives the crooks a better chance of cutting through standard PC defences.

**Spy-phishing** - a term coined by Trend Micro - combines phishing and spyware techniques for the purpose of long term espionage. The email that lures you to a fake website includes a backdoor Trojan that slips into your system and lies low to avoid detection. If you visit the targeted website, the spy wakes up and goes to work for its masters.

But even when the phishing site is closed down, the Trojan remains and can be co-opted to download additional spyware and do more clandestine work for its masters, just like a secret agent planted in a hostile country who's given new assignments by head office.

## Attack of the Zombies

Crimeware has become a crime wave in the form of **botnets**, PCs that have been hijacked through backdoors and turned into a shadow army of zombies. The 'bot herder' gains control over PCs by using exploits in Windows XP like *Remote Procedure Call*, *Internet Relay Chat*, *Background Intelligent Transfer Service* and buffer overflows.

The bot herder directs his army by remote control: at a single command from his computer, they will send out masses of spam to the email contacts on their PCs or launch broad attacks on specific targets that choke their supply lines. The owner of the PC is mostly unaware of anything more than a transient slow-down.

These botnets can grow to vast proportions, as the Dutch Police found not long ago when they closed down a botnet of 1.5 million PCs. A recent surge in e-mail spam hawking penny stocks and penis enlargement pills was tracked to Russian hackers running a net of 70,000 hijacked PCs, 'seeded' with the *Spam Thru Trojan*. This one carried a very special payload: a pirated copy of Kaspersky's security software that had been modified to ignore the malware files on the hijacked machines during scheduled scans.

## Beyond traditional defences

When antivirus software becomes a target for hijackers, it's time to find better mousetraps. Security experts tell us that multiple layers of defences provide the best protection. They don't mean running three different antivirus scanners or installing several firewalls – they mean installing products from different makers rather than putting all our security eggs in one vendor's basket.

Microsoft has long been accused of not doing enough to make its products secure, and this irked the giant so much that he's decided to muscle into the security business. Can elephants learn to dance on pinheads? It doesn't matter: if you use Microsoft servers in your business, you'll be encouraged to embrace **Forefront**, the new security suite Microsoft has assembled from various products it acquired in recent years.

If putting all your eggs in one basket is a bad idea, so is giving the crooks a big target to aim their weapons at. There's no bigger target than Microsoft, and Symantec is the biggest target among the AV vendors by far. A better strategy is to keep a low profile by using security products from smaller makers, a strategy we'll explore in a future article.

**[PART 1 – TREACHEROUS TERRAIN](#)**

**[PART 3 – SECURITY LAYERS, A ROUGH GUIDE](#)**