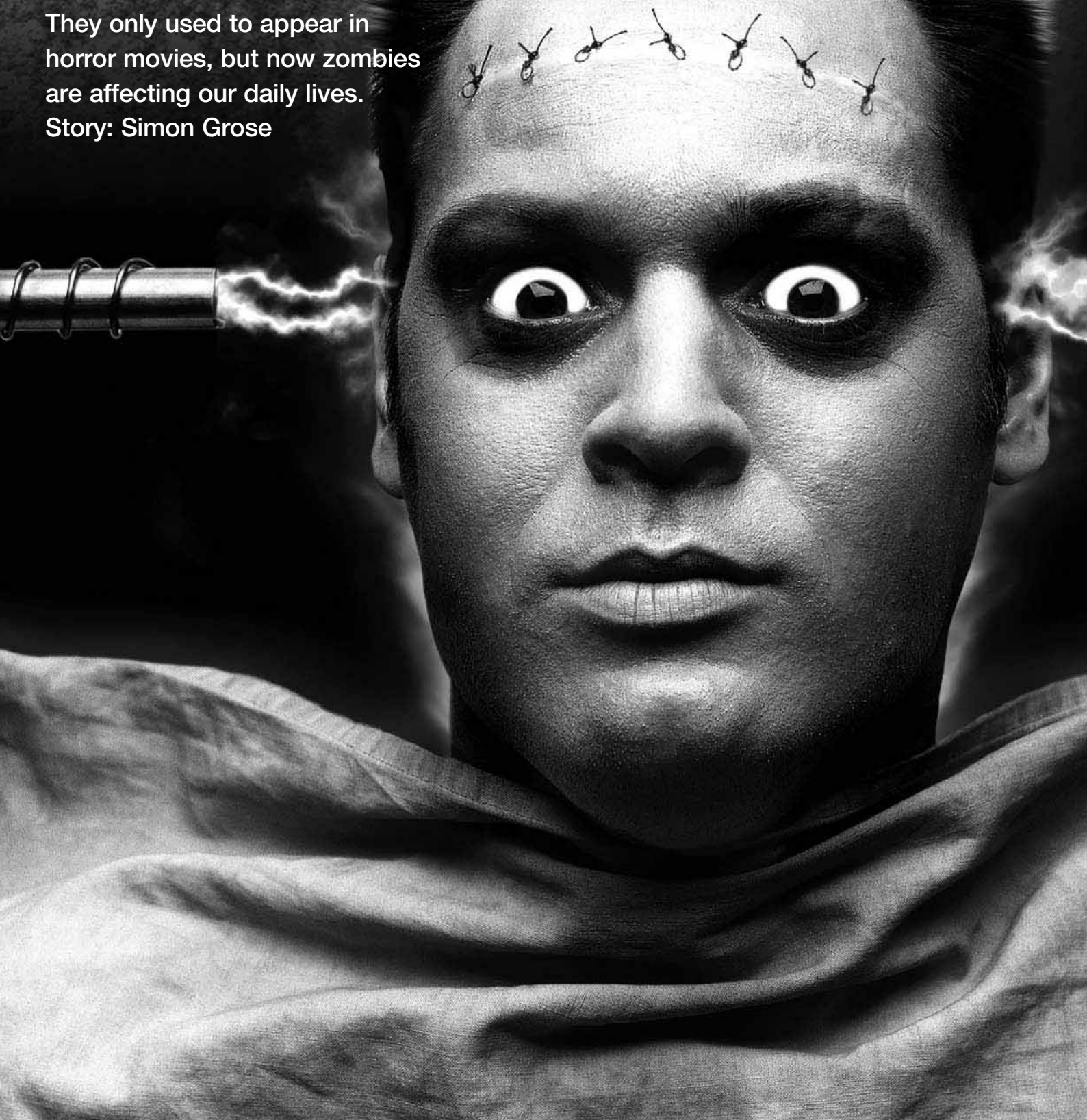


ATTACK OF THE ZOMBIE

They only used to appear in horror movies, but now zombies are affecting our daily lives.

Story: Simon Grose



ES

The world had its first significant encounter with zombies when film director George A Romero unleashed an army of them in his 1968 horror flick *The night of the living dead*. Back then, the chaos they caused was confined to the silver screen.

Now a new breed of zombies has arrived and is causing havoc in both our virtual and real worlds.

Millions of personal computers around the world have been compromised by hackers and have become dumb troops in a network of zombies known as a botnet (see: 'Deliberate chaos' on page 26).

They are the dark side of the virtual world, making the internet as much a threat as it is a boon for business, entertainment and personal communications.

"This technological revolution has delivered many exciting opportunities, but with the undoubted economic and social benefits has also come a new risk of cyber crime," according to the House of Representatives Communications Committee Chair, Belinda Neal (Member for Robertson, NSW), whose committee recently commenced a public inquiry into cyber crime.

"Illegal activity, such as identity theft and financial fraud, threaten individuals' right to privacy and the competitiveness of Australian businesses and the international companies that operate here," Ms Neal says.

"In this rapidly moving field it is timely to review Australia's progress in combating cyber crime and promoting e-security at home and abroad."

Computer users with an email address have become accustomed to spam or junk emails, but few are aware of the extent to which the internet has been colonised by criminals. In June this year spam accounted for 90.4 per cent of all email global traffic. Botnets were the source of 83.2 per cent of all spam emails, up from 57.6 per cent the previous month.

Reporting this data, MessageLabs, a subsidiary of global e-security provider Symantec, said the biggest known botnet, Cutwail, was estimated to have an army of at least 1.5 million zombies under its control and was responsible for up to 35 per cent of global spam during May.

Spam emails have accounted for high proportions of total email traffic for several years, but the intensity of cyber criminal activity is undoubtedly increasing.

Speaking in Sydney in April, Symantec's Research Vice President, Joe Pasqua, said more than a million new strains of malware were released into cyberspace during 2008, more than in the previous 20 years.

"We've crossed the point where there is now more malware in the world than goodware," Mr Pasqua said.

In 2000 the company identified an average of five new viruses per day, but in 2009 an average day sees 25,000 new virus signatures crawling around cyberspace and at least 1,500 malicious websites created.

"We tend to refer to it as an arms race," says Craig Scroggie, head of Symantec Australia.

"Every time we produce another defence mechanism they look for ways around them. As we get smarter and build better technology, so do the criminals because financial gain is the name of the game."

One example is a phishing scam which targeted at least 20,000 Australians in June as they were preparing to submit their 2008-09 tax returns. They received an email which appeared to come from the Australian Tax Office, inviting them to fill out an online tax form as part of a trial, for which they would receive a discount on their tax bill.

To provide a false sense of security, the email warned against lodging the form electronically, instead asking that it be printed out and posted to the ATO. But the malware embedded in the form was designed to harvest the individual's personal

"AS WE GET SMARTER AND BUILD BETTER TECHNOLOGY, SO DO THE CRIMINALS BECAUSE FINANCIAL GAIN IS THE NAME OF THE GAME."

LIVING DEAD:
Millions of
computers have
been compromised.
Photo: Photolibrary

Deliberate chaos

A humble desktop computer becomes a zombie when it is infiltrated by a Bot program, generally referred to as 'malware'.

Bot programs are created to establish a network of zombies—a botnet—which can spread the infection ever further. Computers without security software whose users are willing to click on attachments and links from unsolicited emails are most at risk of becoming zombies.

There is an underground market for botnet programs whose controllers ironically have to use passwords and other security measures to stop rivals gaining access to their botnets.

Once the malicious code is installed, a zombie computer can be activated by command and control servers which are typically geographically distributed to mask the location of the perpetrators.

When commanded to attack, they generate spam emails which spread the original infection or dupe recipients into revealing passwords, bank account details or other personal information which can be used for fraudulent purposes.

details, including tax file and Australian business numbers, as soon as the 'print' button was pressed.

This kind of phishing exercise is bound to become more common and more sophisticated, according to Dr Raymond Choo, a research analyst at the Australian Institute of Criminology where he focuses on high-tech crime and money laundering.

One of 23 Australian 2009 Fullbright Scholars, Dr Choo is in the US for the second half of 2009 working at Rutgers University and the Palo Alto Research Centre to further his study of cyber crime.

He expects 'spear phishing' to become more prevalent, as cyber criminals launch attacks on small groups of internet users who are identified as members of vulnerable sub-groups or as individuals of high net worth.

"Attacks are becoming more targeted, more sophisticated and more financially motivated," Dr Choo says.

"In the early phase of hacking and virus creation the motivation was to be noticed, now they want to lie low so that their malware is not recognised by the anti-virus companies, so they can maximise their profits. This is a trend that is going to continue."

Cyber criminals are also adopting methodology developed by cyber espionage agencies to mask their activities with virtual smokescreens and dummy targets.

In an Australian Institute of Criminology paper, *Future directions in technology-enabled crime: 2007-09*, in which



he was lead author, Dr Choo cautioned that attempting to attribute the actual source of cyber espionage "is not a straightforward process".

The paper cites a report from a cyber espionage investigation which suggested that networks of infected computers physically located in a particular jurisdiction "could have been deployed as staging posts, perhaps in an effort to deliberately mislead observers as to the true operator and purpose of the system".

Along with most experts in this field, Dr Choo believes there are two key ways to thwart cyber criminals: educating computer users to be wary of taking any online actions that may compromise their personal information and ensuring that their machines have updated security software.

He also argues there is room to improve the tools and systems that enable online activity to provide greater protection.

"If we could manage to get the industry to develop more secure hardware and software we could reduce many cyber vulnerabilities," Dr Choo says.

Professor Vijay Varadharajan, Chair of the Australian Computer Society's eSecurity Task Force, sees an opportunity for the government to more actively encourage these measures.

"We believe the government should consider developing agreements with vendors to ensure that computer systems and mobile devices are not sold without supplying adequate e-security and cyber safety information that covers current and known emerging threats," he says.

"The ACS would like to see vendors embrace secure development applications more fully on a voluntary basis and in accordance with internationally agreed standards."

Most providers do make efforts to improve their products in the ongoing arms race with cyber criminals, driven by



“If we could manage to get the industry to develop more secure hardware and software we could reduce many cyber vulnerabilities.”

the need to maintain their reputation in the market. But Symantec’s Craig Scroggie says their effectiveness can be compromised by the failure of users to employ the tools at their disposal.

“When Microsoft sends out their updates on the first Tuesday of every month, many organisations don’t patch their operating systems and applications immediately,” he says.

“A little bit more discipline will offer us a greater level of security than we are seeing today across many fronts.”

Legislative and regulatory initiatives to combat cyber crime will be a focus of the House committee’s inquiry. One option currently before the government comes from an Australian Law Reform Commission report, *Australian privacy law and practice*, issued in July 2008.

The ALRC recommended that a mandatory data breach disclosure notification regime be established, requiring organisations to notify the Privacy Commissioner and affected individuals when personal data has been acquired by an unauthorised person, and the organisation or the Privacy Commissioner believes this may pose a real risk of serious harm to those individuals. Failure to comply would attract a civil penalty.

THE DARK SIDE: *Attacks are sophisticated and financially motivated. Photos: Photolibrary and Jupiterimages*

The ALRC report followed the April 2008 release by the Australian Privacy Commissioner of a voluntary guide to data breach notification.

Craig Scroggie supports the move to a mandatory code for organisations covered by the Privacy Act, which applies to government agencies, organisations with turnover of \$3 million or more, and all health service providers.

He says a mandatory reporting regime would force organisations to manage their information more securely than many are capable of doing today.

“This will heighten sensitivity around ensuring that confidential information is protected, and if an individual’s data has been accessed either illegally or by misadventure it will heighten awareness of the issues surrounding the security and confidentiality of their information,” he says.

When the ALRC report was handed down, then Special Minister of State, Senator John Faulkner, indicated that implementing its recommendations was not a priority for the government and it would be unlikely to be considered or acted upon before the next election.

A range of proprietary and open source software applications are available to alert system administrators and users when data may be about to be included in an email or otherwise downloaded from a network in contravention of an organisation’s security policies. They typically alert users to the potential for a breach, ask if they intend to continue, suggest or require encrypting of the data, and report the action to IT security managers.

While these tools may be suitable to enable organisations to comply with a mandatory notification regime, one problem is the need to effectively define “real risk of serious harm” as a threshold for notification. Once instituted, any mandatory scheme would also have to be enforced, a task that would require new powers and much greater resources for the Office of the Privacy Commissioner.

And while security firms and law enforcement authorities continue to develop technological solutions to combat cyber crime and inadvertent release of personal data, implementing these solutions must enable legal online behaviour to occur without major delays or interruptions. If not, organisations and individuals will disable them or find ways to work around them.

“There is always a trade-off between security and useability, and the weakest link is human so user education is very important,” Raymond Choo says.

Craig Scroggie agrees, pointing out that while attacks on organisations become cleverer and more common, the most vulnerable online targets for cyber crime are the people who use the millions of PCs, laptops and other mobile internet-enabled devices around the world every day. Each one is a potential zombie. •

For more information on the inquiry into cyber crime, visit www.aph.gov.au/coms or email coms.reps@aph.gov.au or phone (02) 6277 4601.