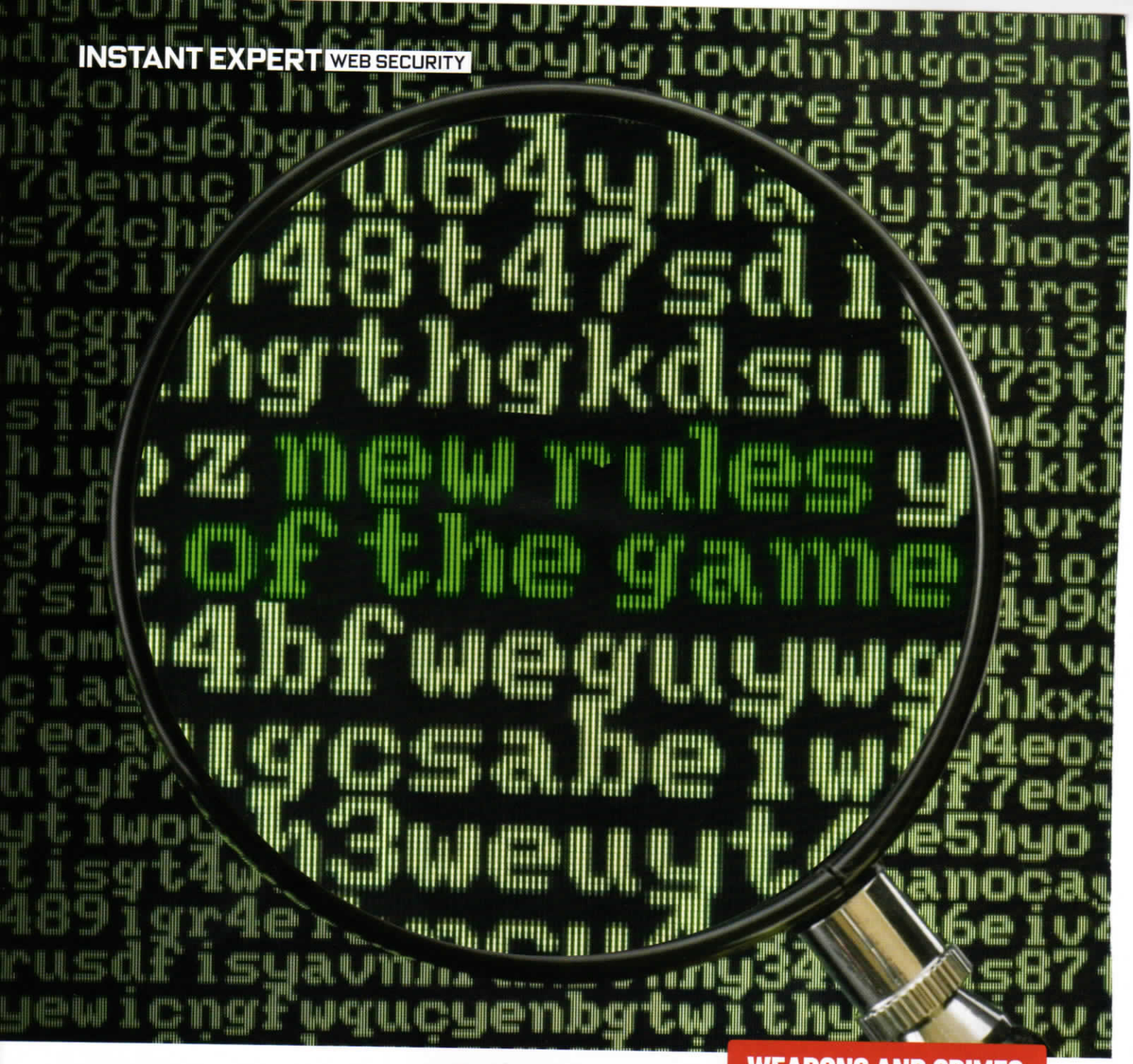


THE NEW THREAT LANDSCAPE OF ONLINE HACKERS AND CYBER-CRIMINALS.

BY YASMIN GHAHREMANI

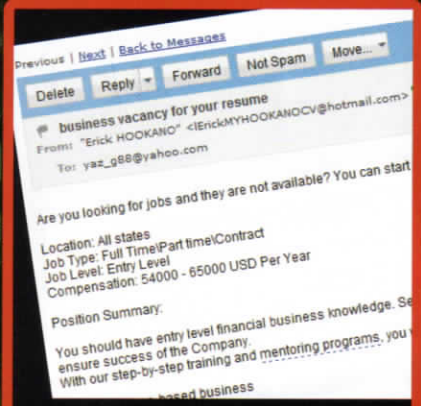
As Australia plans for a national broadband network, it's struggling with a problem that's become worth a trillion US dollars globally and is bigger than the international drug trade. Computer crime is on the rise, and it's no longer kids' play.

Today's cyber criminals are motivated by serious money and operate in stealth, infecting computers with far more polished attacks than a few years ago.

Australia is breeding its own computer criminals. It's in the top 10 countries for hosting spam sites and sends more than 135,000 malicious emails per month. But it's also being hit from abroad. IT specialists in Eastern Europe can make nearly ten times what they would in a legitimate job by working for organised crime gangs. "It's as sophisticated as looking at the technology sector in Silicon Valley," says Alana Maurushat, deputy director of the Cyberspace Law and Policy Centre at The University of New South Wales. Here are the essential facts.

WEAPONS AND CRIMES

BLACK-HAT HACKERS have a number of tools at their disposal, depending on the crime they want to commit. Identity theft – the fastest growing crime in the world – is one of the most common goals of an attack. In fact, the head of Crime Stoppers Australia, a frequent lecturer on identity theft, has had his credit card numbers stolen twice in the past year. Sometimes, however, a computer is attacked simply to make it part of a botnet – a network of infected computers, also known as bots or zombies, that can be enlisted to carry out other deeds.



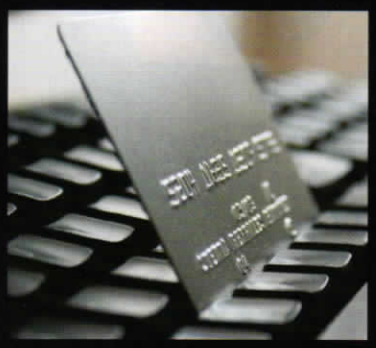
SPAM Believe it or not, spam works. Even if only one person in 1,000 clicks on it, if a criminal is tapping into someone else's computing power to send out millions of free messages, that's still a pretty good return rate. Spam is used to deliver ads, often for dubious products and services, but increasingly it's used to deliver links to malicious websites. In February, Symantec reported that 89.5 per cent of Australia's email traffic was spam, and of that, one of every 315 emails contained malicious links.

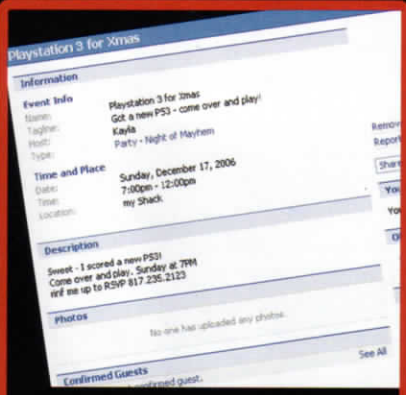
DDOS Distributed Denial of Service attacks are often associated with political motives, but economic warriors use them as well. Botnets inundate victims' servers with unwanted information until they are crippled. DDoS attacks can be used to take down competitors, or the mere threat of one can elicit ransom money. Australia's online gambling sites have been targets. "If they make $100,000 a day it makes more sense to them to pay $50,000 in extortion than to have the website go down for a day," says Kathryn Kerr, manager of analysis and assessments at AusCERT, which has received reports of the extortion threats.

FAKE SECURITY SOFTWARE

Beware of the growing number of bogus pop-ups warning that your anti-virus software has expired or your computer is under threat. They lead to realistic looking sites selling nothing but trouble. The fraudsters not only collect money for their worthless wares, they also warn customers to disable their current security software so they can download the fake application. They often steal credit card details and enlist the computer as a new bot to boot. Security software company McAfee reports a 400 per cent increase in these attacks in the past year.

PHISHING Phishing attacks use links to divert users to fake websites where they are asked for valuable personal data. Financial institutions are the most common types of sites spoofed. Sophisticated designs that mimic real bank websites down to the letter make current phishing sites harder to detect than a few years ago. To complicate matters, today's scammers may make withdrawals from your account that don't even show up when you log in online. The only way you can detect them is to get a paper statement.





SOCIAL NETWORKING SCAMS

One of the trendiest attacks for 2010 enlists not just you but your friends. Once you've been hit by a drive-by, key logging software is downloaded onto your computer. Every keystroke you make is recorded by the criminal. Log in to your favourite social networking site, and your user name and password are in the criminal's hands. Suddenly your 200 Facebook friends get a message from you telling them about a hilarious video, which actually contains an infected link. "They wouldn't open it if it was from someone saying, 'Get your free Viagra here'," says Greg Singh, principal consultant at security firm RSA. "But they'll open it because it's from one of their mates." Another new favourite for criminals: The TinyURL that's become ubiquitous in Twitter. A shortened, anonymous link is an easy way to route someone to a malicious website. Make sure you trust the sender and the message looks kosher before you click.

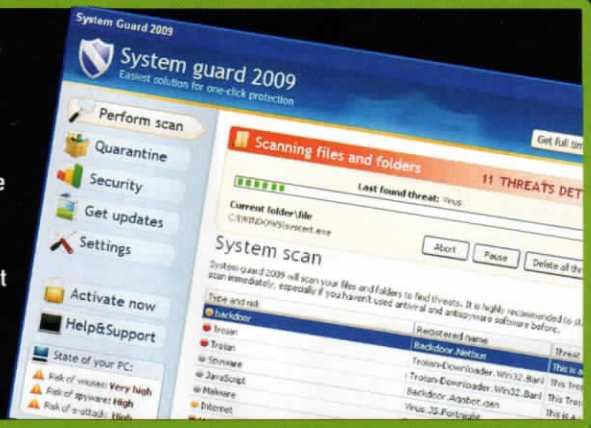
ONLINE SHOPPING SCAMS – The number of complaints about online scams received by the Australian Competition & Consumer Commission grew 70 per cent last year, and the complaints about online shopping doubled. "The perception of many people is that scammers are obvious and easy to pick out, like the old-fashioned Nigerian e-mails," says Peter Kell, deputy chair of the ACCC. "But scammers today are offering much more sophisticated and incredible offers to consumers." Australians have lost hundreds of thousands of dollars to unscrupulous vendors of everything from cars to pedigree pups.

DRIVE-BY INFECTIONS A drive-by infection is a piece of malware hidden on a website that infects a user who merely visits the site. What makes a drive-by so dangerous is that it can be lurking on a legitimate site. The Sydney Opera House website came under drive-by attack three years ago and infected a number of people's computers before the malware was detected. These days, hackers love to hide infections in real or fake Web pages delivering news about big events. Michael Jackson's death and the Haiti earthquake both served as lures for drive-bys. "The message of 'Don't double click attachments from unknown people', has gone pretty well," says David Hall, spokesman for Symantec's Asia-Pacific operations. "So now just searching the Web is the most likely way that you'll be exposed to an infection."

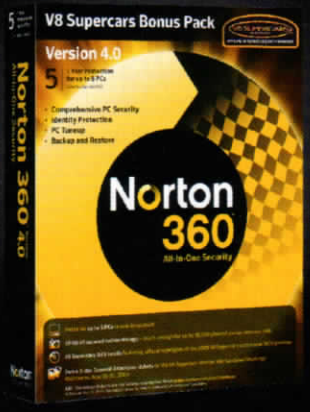
SAFE SURFING

The threats out there are real, but you don't have to unplug and revert to cash to stay safe. There are ways to protect yourself. AusCERT'S Stay Smart Online alert service (w/) provides ongoing news about the latest threats, and solutions in layman's terms. Here is a roundup of some basic ideas:

BEWARE OF APPLICATION UPDATES Like fraudulent security software, sometimes application updates have been known to include malware. Make sure the program is something you even have, then check the version number. If you're still not sure, go to the manufacturer's website and see if they really have released a new update.



BATTEN THE HATCHES Keeping your operating system, applications and security software updated go without saying. But that's only the beginning. "Anti-virus is not detecting anywhere near 100 per cent of the malware," says Kathryn Kerr, manager of analysis and assessments at AusCERT. In addition, "malware uses root kits to hide itself and takes other measures to disable anti-virus and other security features." She recommends regularly running free online scanners to check for malware, in addition to using locally installed up-to-date anti-virus software. The scanners can be run without disabling commercial security software. Besides scanners, freeware such as Internet Explorer's SmartScreen Filter help detect potential phishing sites and Google can let you know if one of its search results has hosted malware in the recent past. Commercial security software offers similar tools and many new improvements in this area, too.



CONSIDER LINUX FOR BANKING. Detective Inspector Bruce van der Graaf of the New South Wales Police Computer Crimes Unit recommends running a Linux boot disc before banking online or conducting other secure transactions. That process installs a clean operating system on the computer. But for users scared off by that idea, van der Graaf advises surfing the Web under a limited user account, which would restrict the access of any intruder; and using Windows Steady State, a tool that lets the computer be restored to a previously stored state every time it reboots. "The only way you're going to be 100 per cent sure you're not going to pick up a zero-day exploit is to boot from a clean machine – either from Linux or a known good installation of Microsoft Steady State," says van der Graaf.

PLAYERS

The underground cyber-crime world comprises a whole fraud ecosystem, where players assume specialised roles for maximum efficiency.

TOOL AND SERVICE PROVIDERS

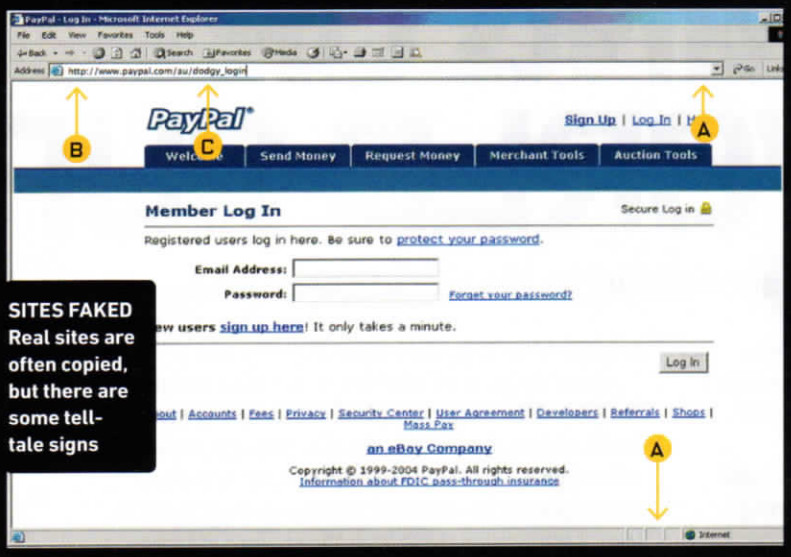
Much like their legitimate counterparts in the commercial realm, these IT pros create software programs and the services to maintain them. They may even rent software-as-a-service or IT infrastructure. The only difference is that their wares have malicious intent: Key logging spyware, fake antivirus applications and toolkits for creating botnets. All of these goods and services are traded on the black market.

ID HARVESTERS

These people extract identity information from victims. Sometimes they use the information themselves, but more often they sell it on the black market. 'Carders' offer credit card numbers for prices that vary, depending on how fresh the numbers are, from about $1 to $35 a piece. A Medicare record, which contains enough data to open a bank loan in the victim's name, fetches $50 to $60, according to Singh.

FRAUDSTER

The thief or scammer who will ultimately cash in on the main crime at hand.



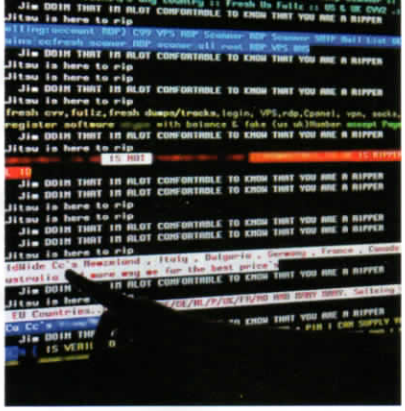
SITES FAKED Real sites are often copied, but there are some tell-tale signs

KNOW WHO YOU'RE GETTING PERSONAL WITH. This means checking the digital certificate of any site you give valuable information to. A digital certificate is part of the protection provided by Secure Socket Layer and is a way to check you are not inadvertently visiting a phishing site. SSL encryption also helps protect your communications from being read in transit while information is being exchanged between your computer and the Web site. If the website has a digital certificate, there will be a padlock icon **[A]** to the right of the Web address window in Internet Explorer or to the bottom right of the browser window in Firefox. The URL will also start with 'https', **[B]** instead of 'http'. To check the certificate, right click on the padlock. Make sure that the domain name **[C]** displayed belongs to the organisation you think you are connected to; check that the certificate has not expired and that it is verified by a third party, not by the certificate owner. If one of these conditions is not met, don't trust the website. It's also important to note that a padlock, 'https' and digital certificates do nothing to ensure that the website you are visiting is free of malware, or that your keystrokes are not already being logged by malware on your computer. It is simply a way to verify the identity of the remote website and means that your communication with the website in question is encrypted and safe from being read in transit while information is exchanged between you two.

MULE HERDERS

Mule herders recruit unsuspecting 'mules' to help criminals launder their ill-gotten gains. Some 200 mules are estimated to be operating in Australia at any time. They usually respond to job notices – sometimes even on legitimate job boards – promising a telecommuting position that requires no education and delivers a great salary. All the applicant needs is a computer and a bank account.

Once recruited, the mule begins receiving payments to his bank account. Unbeknown to him, they are from a stolen credit card. He is instructed to withdraw each payment, keep a small percentage for himself, and wire the rest to his employer. He continues that process until he gets caught, at which point the herder and the fraudster are untraceable. "The mules always get caught and they are very expendable," says Singh.



NETTING THE BUTTERFLY

The world watched in early March as Spanish police revealed 800,000 stolen credentials found in the possession of three arrested suspects allegedly behind the Mariposa botnet. Mariposa had grown in a disturbingly short time to a 13-million strong army of zombie computers, including 32,000 Australian machines. Its crippling was one of the rare international success stories among international cyber-crime fighters.

Mariposa first surfaced in September 2009 and grew from 600,000 PCs to several million in three months. Defence Intelligence CEO Chris Davis set up a working group in Spain, where the botnet's command and control centre was located, and devised a plan to take down Mariposa by shutting down the 25 domains that the criminals were using to control the botnet.

At the time, Mariposa encompassed at least 10 million computers by December 23. When shut down, the gang's supposed leader, nicknamed Netkairo, began a furious attempt to regain control. Panicked, he logged in from his home computer, outside the anonymity of the gang's virtual private network. That would prove to be his fatal mistake. He then bribed an employee at a domain host to reinstate one of the domain names, and then updated about a million computers with a variant of Mariposa.

Netkairo's game was arrested in early February. Clues found on his computer led to the two other arrests. Mariposa is, however, still spreading quickly. "We don't know if there is a second stage that will deliver more malware," says Davis.