ACMA goes **zombie** hunting

ACMA has developed and will host a program that finds 'zombie' computers on the Australian internet.

The program, the Australian Internet Security Initiative and launched in November by the Minister for Communications, Information Technology and the Arts, identifies infected computers with Australian internet addresses and is being trialled with five internet service providers (ISPs).

'There are millions of "zombies" around the world and they have become a major problem on the internet,' said Ms Maddock. 'Global software companies estimate that more than 60 per cent of all global spam is now relayed via zombies and I am delighted that ACMA is working closely with ISPs and the public to address this issue.'

Under the trial program, ACMA will supply the ISPs in the trial with a list of the infected internet addresses on their networks. Each ISP will then contact customers with infected computers to advise them on what they may need to do to fix the problem.

If the owner either cannot or will not fix the problem and their computer remains a threat to other internet users, the ISPs may take steps under their acceptable use policy to disconnect the computer until the problem is resolved.

Telstra BigPond, OptusNet, Westnet, Pacific Internet and West Australian Networks are the ISPs participating in the trial. The Australian Computer Emergency Response Team (AusCERT), the Department of Communications, Information Technology and the Arts and other online experts are also assisting in the trial.

The best way for a consumer or business to prevent their computer being infected is to use anti-virus software and a firewall, and keep security patches up-to-date. They may also wish to consider anti-spyware software and a spam filter.

ZOMBIES AND BOTNETS ZOMBIES AND BOTNETS ZOMBIES AND BOTNETS ZOMBIES AND B

zombie computer: a computer attached to the internet that has been compromised by a hacker, a computer virus or trojan software, and performs malicious tasks, under the direction of the hacker. Many owners of zombie computers are unaware that their systems have been compromised or that any hacker attack ever occurred.

botnet (jargon): a collection of zombie computers. A botnet's originator can control the group remotely and usually does so for malicious purposes., including:

- distributed denial of service attacks (DDoS), which pose a threat to critical information infrastructure
- spam relays, often containing illegal or pornographic material, now responsible for the majority of Australian-originated spam
- theft of personal information, identity theft and
- phishing attacks (Gartner estimates that phishing attacks grew 28 per cent in the 12 months to May 2005).

Although the hackers using botnets are based mainly in North America and Europe, the compromised computers may be based anywhere. Computers with broadband connections are particularly vulnerable.

ACMA identified 7,385 new zombies in Australia (this is not necessarily the total number of zombies in Australia) in August and 5,905 in September 2005, which represents 5–6 per cent of the zombied computers in the Asia–Pacific region. CipherTrust reported that in May 2005 it detected around 172,000 new zombies worldwide every day.

Botnets are formed and disbanded daily, so no numbers are available. They can be highly organised and analysts report that they can be bought or leased for specific purposes.

Botnets can consist of tens of thousands of compromised machines and pose serious threats. Even a relatively small botnet with only

100 bots has the potential to cause disruption.

Botnets have been used for various purposes including:

- transmitting bulk spam messages—Sophos (2005) stated that compromised computers are responsible for 40 per cent of global spam
- sniffing traffic—software that captures data, such as passwords
- keylogging—remotely monitoring someone's keystrokes to obtain personal information, such as logon names and passwords
- spreading new malware—designed to cause damage or obtain personal information.

Sophos reported on 10 October 2005 that authorities in the Netherlands have arrested three men suspected of running a zombie network of more than 100,000 computers, including computer hacking, installing spyware and using compromised computers without permission. Prosecutors claim that the men ran a zombie network of 100,000 infected computers around the world, one of the largest ever detected, and Dutch authorities are investigating claims that the gang attempted to blackmail a North American organisation. It is not unusual for criminal gangs to use zombie networks to extort money from online companies, forcing them to pay to prevent a DDoS attack against their websites.

If a computer's operating system appears slower than normal, or if the hard drive spins when the user is not accessing it, or if the internet connection becomes active when it should not be, then the computer may have been compromised.

The best-case scenario is that it will merely affect the way that individual computer system operates; for example, slowing computer response times to 'clicks', or the time taken to download web pages or information from the internet. This may be inconvenient and annoying for the computer's users.

In the worst case scenario, the computer could be unwittingly used to send personal information without the user's knowledge or consent to another person who uses the information to defraud the user or in combination with other 'zombies' to launch spam or denial of service attacks against web sites or organisations, for financial gain or corporate defamation.

Each participating ISP in the pilot has agreed to a protocol for the Internet Security Initiative during the trial period. Under this protocol, each ISP will advise ACMA on the action it would take in regard to customers whose details are passed to it by ACMA. All five ISPs have agreed to a protocol that customers will not be summarily disconnected from the internet. This does not preclude ISPs from quarantining a computer from the network if it is causing network disturbance. The protocol is consistent with ISPs' existing service agreements.

In May 2005, the US Federal Trade Commission and 35 government partners (including ACMA) from more than 29 countries announced 'Operation Spam Zombies', an international campaign to educate ISPs and other providers about hijacked or zombie computers that spammers use to flood inboxes.

Twenty members of the London Action Plan, an international network combating spam, and 16 additional government agencies who will participate in Operation Spam Zombies will send letters to more than 3,000 ISPs around the world urging them to employ protective measures to prevent their customers' computers from being hijacked by spammers. These measures include:

- blocking a common internet port used for email when possible
- applying rate-limiting controls for email relays;
- identifying computers that are sending atypical amounts of email and take steps to determine if the computer is acting as a spam zombie. When necessary, quarantine the affected computer until the source of the problem is removed;
- providing plain-language information for customers on how to keep their home computers secure; and
- providing or pointing their customers to easy-to-use tools to remove zombie code if their computers become infected.

For more information about ACMA's anti-spam activity, see the ACMA website at www.acma.gov.au (go to Internet > Spam).

IMPROVED ARRANGEMENTS FOR PRIORITY ASSISTANCE CUSTOMERS

ACMA has approved changes to Telstra's priority assistance arrangements. The changes streamline the application process for priority assistance customers, extend the renewal period from one to three years and mean customers will no longer have to renew their registration when they move house.

The approved changes build on existing arrangements and will deliver improved service levels for priority assistance customers.

Priority assistance is an enhanced level of telephone connection and fault repair service for people with a diagnosed life-threatening medical condition who are at risk of suffering a rapid, life-threatening deterioration in their condition.

The changes are contained in a variation to Telstra's Priority Assistance for Individuals Policy, an appendix to its Standard Marketing Plan, which is available on the Telstra website, www.telstra.com.

A variation to a Standard Marketing Plan is subject to approval by ACMA in accordance with section 12W of the *Telecommunications Act 1997*. ACMA has discretion as to whether it will require a provider to publish a draft variation to a Standard Marketing Plan for public comment.

ACMA does not consider public consultation is warranted in this instance, given the substantial public consultation that occurred in a review of the policy by the Australian Communications Authority in 2004.

in brief

ACMA ALLOCATES SUBSCRIPTION TV LICENCE

ACMA has allocated one subscription television broadcasting licence to Hotel Entertainment Network Pty Ltd.

Hotel Entertainment Network proposes to deliver a range of programs including news, weather and movies, as well as services of interest to members of the Australian Hotels Association and their patrons.

Unlike apparatus licences or other service delivery permits, these licences do not have geographical limitations. Therefore, a service licence is valid throughout Australia as long as the programming on that service is the same in all areas of reception. If the service differs in a location, a separate service licence is required.