TRENDS & ISSUES
in crime and criminal justice

Australian Government
Australian Institute of Criminology

No. 333 March 2007

Zombies and botnets

Kim-Kwang Raymond Choo

Bot programs allow attackers to remotely control vulnerable computers and form virtual networks of zombies – botnets. Botnets can be leveraged to orchestrate concerted attacks against other computing resources, for example, distributed denial of service (DDoS) attacks against targeted networks. The shift in motivation from curiosity and fame seeking to illicit financial gain has been marked by a growing sophistication in the evolution of bot malware. The ABS estimated that there were over 6.65 million active internet subscribers in Australia in September 2006. Most subscribers are households, with over 5.83 million household users compared with 826,000 business and government users. This paper examines the activities and consequences associated with botnets and provides examples of existing incidents so that subscribers can be better informed of the risks. Business, government and individual householders need to be aware of risk mitigation strategies and to ensure that these strategies are implemented and updated, as attacks on the internet are not likely to disappear any time soon.

Toni Makkai
Director

Bot programs are codes or programs that operate automatically as agents for a user or another program. The first bot program was probably Eggdrop, created by Jeff Fisher, which originated as a useful feature of internet relay chat (IRC) in the early 1990s. Early bot programs were designed to allow IRC operators to script automated responses to IRC activities. As IRC gained popularity among internet users, inappropriate behaviour started to become a problem. Misbehaving users were klined (ejected) from IRC channels. As payback, some ejected users developed ways to attack the IRC channel, which led to the IRC wars that caused the first DDoS attacks in the mid 1990s.

Bot programs (malware) are surreptitiously forwarded to victims by various means, such as via email attachments, via peer-to-peer (P2P) networks, and visits to an infected website. Bot malware typically takes advantage of system vulnerabilities and software bugs or hacker-installed backdoors that allow malicious code to be installed on computers without the owners' consent or knowledge. They then load themselves into such computers, often for nefarious purposes. Bots – individual computers infected with bot malware – are then turned into zombies. These can then be used as remote attack tools or to form part of a botnet under the control of the botnet controller as illustrated by Figure 1. Among the three botnet communication typologies identified by Cooke, Jahanian & McPherson (2005) – centralised, distributed P2P and random – the most commonly used are the centralised and distributed P2P.

Zombies are nodes in the sleeper cells of machines waiting to be activated by their command and control (C&C) servers. The C&C servers are often machines that have been compromised and arranged in a distributed structure to limit traceability. Some forms of authentication mechanism (e.g. password-based login from a predefined domain) are often deployed on C&C servers by botnet controllers to prevent unauthorised third party access. Once the botnet controllers are authenticated and logged in, they can issue attack commands to the servers via IRC channels or using P2P technologies.

ISSN 0817-8542

ISBN 978 1 921185 35 9

GPO Box 2944
Canberra ACT 2601
Australia
Tel: 02 6260 9272
Fax: 02 6260 9293

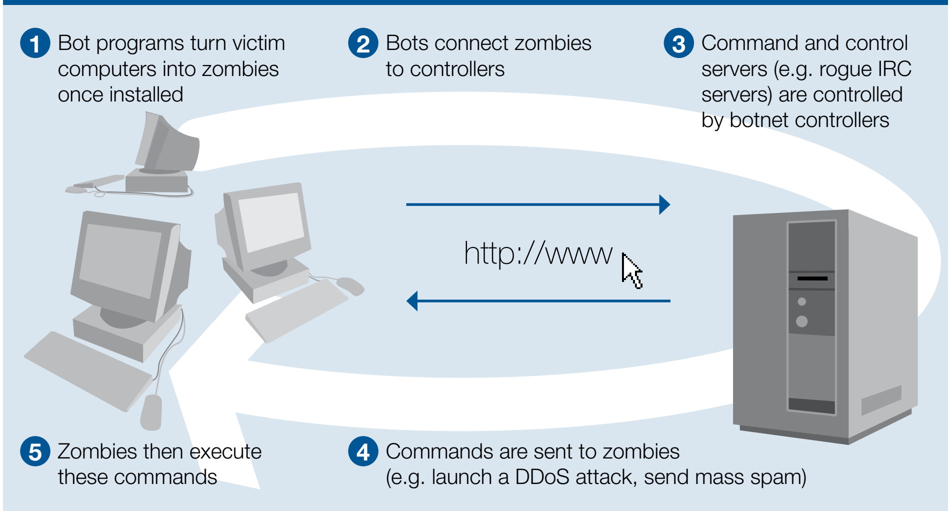
For a complete list and the full text of the papers in the *Trends & issues in crime and criminal justice* series, visit the AIC website at: http://www.aic.gov.au

Disclaimer:
This research paper does not necessarily reflect the policy position of the Australian Government.

Project no. 0074a

<AHTCC>

Figure 1: A typical botnet


1 Bot programs turn victim computers into zombies once installed
2 Bots connect zombies to controllers
3 Command and control servers (e.g. rogue IRC servers) are controlled by botnet controllers
http://www
5 Zombies then execute these commands
4 Commands are sent to zombies (e.g. launch a DDoS attack, send mass spam)

Building botnets

Building botnets requires minimal levels of expertise (Ianelli & Hackworth 2005). A brief two-step overview on how to build a botnet is outlined below.

Information gathering stage

There is a wide diversity of exploitations, including many of those used by worms, written into botnet code bases that use well known vulnerabilities to infect target systems (Barford & Yegneswaran forthcoming). Locating such exploits and other information to facilitate the creation of botnets, as outlined below, can be easily achieved using search engines.

Source codes – the full text of the actual code that will potentially allow an attacker more room for exploitation can be obtained using search engines, including the recently released Google code search functionality.

Step-by-step instructions on how to compromise systems – which includes obtaining packaged exploits, simple command-line and GUI-run exploit frameworks, and tools that can be abused for malicious purposes, e.g. to gain clandestine entry into computer networks and systems, and bot malware such as Agobot, Bionet Bot, Forbot, GTBot, Phatbot, SDBot, Slackbot, SubSeven Bot, Rbot, URBot, XtremBot, and UrXBot.

Vulnerable systems for exploitation in underground hacking sites – such sites could potentially contain detailed lists of IP ranges (netblocks) including those ripe with vulnerable systems, those that are heavily monitored and should be avoided, those that are unallocated or un-routable, and those that are allocated to certain types of organisations including educational institutions and government agencies (Ianelli & Hackworth 2005).

Exploitation and propagation stage

After locating the vulnerable systems and the tools to exploit them, attackers can proceed to connect to identified backdoors (e.g. backdoor left by Bagle variants on port 2745) or vulnerable services. By running the obtained or known exploit(s) against known vulnerable systems, attackers can gain clandestine entry and escalate previously acquired privileges (e.g. administrator-level privileges and root access) to facilitate installation of bot malware by uploading or commanding the target system to download a copy of the bot malware.

This bot malware can also propagate via various means such as P2P networks, open file sharing networks and backdoors left by worms (e.g. W32/SDBot) already installed on compromised machines.

Upon successful invasion, bot malware can use popular protocols such as file transfer protocols (FTP), hypertext transfer protocol (HTTP) and trivial file transfer protocol (TFTP) to infect the computers and spread until a viable (bot) force is assembled. In addition, bot malware can be updated automatically, which expands the list of exploits that can be leveraged to distribute it.

Motivations

Historically, curiosity and fame seeking have primarily been the motivations for underground research and hacking. Trends in recent years, however, suggest that online attackers have shifted their focus from curiosity to illicit financial gain. This is, perhaps, not surprising as recent advances in information and communication technologies (ICT) and the internet have revolutionised communication and the way in which commerce operates (e.g. electronic payment systems and online auction sites). While it is almost impossible to quantify the actual impact of ICT on world economics, a recent article by Milburn (2006) shows the value of integrating ICT into traditional business models – US$30 trillion of trade in goods and services is shifted across the globe through a computerised supply chain every year.

Several academic and industry studies have found that financially motivated high tech crime cases are on the rise. For example, the 2006 AusCERT (2006) survey and the DTI Information Security Breaches Survey 2006 (PWC 2006) indicated a notable increase in the view by businesses that electronic attacks have been motivated by illicit financial gain in Australia and around the world.

The FBI recently reported that financial loss due to cybercrime in 2004 is estimated to have been US$400 billion (McAfee 2005). The survey in the UK (PWC 2006) also indicated that information security breaches cost UK companies across several industry sectors £10 billion per annum. With these economic incentives, it is hardly surprising that bots are used as facilitators of high tech crimes. There is a notable increase in the number of reported cases of botnets being rented out or sold to spammers, hackers, and other criminals to facilitate other high tech crimes.

Emerging trends

There has been a sizeable increase in the level of sophistication of bot malware. For example, at the recent Defcon hacker conference 2006, the security community highlighted a new class of bot malware – Queen Bots. Queen Bots 'pack' (and 'repack') the executable files containing the malicious codes to further obfuscate the signatures of the malicious codes, with the aim of eluding detection by antivirus software. It was also noted that Queen Bots comprise half of the known bot programs operating today (IEEE 2006: 20). Although there are no known published statistics or reported incidents involving Queen Bots, it is likely that malware exploiting portable executable (PE) packers, originally designed to reduce the size of an executable file on disk through compression, will emerge.

Typically, membership of botnets ranges from hundreds to thousands or hundreds of thousands of zombies. Recently observed trends, however, suggest that botnet sizes have been decreasing, in order to elude detection since smaller botnets are often more difficult to detect (Cooke, Jahanian & McPherson 2005).

Vehicle for high tech crime

As Schaffer (2006) and many other security researchers have pointed out, such (bot) malware is just as dangerous as more familiar cyberthreats, e.g. viruses, worms, Trojan horses and network intrusions. Moreover, advances in modern technologies offer criminals more opportunities to commit economic crimes with larger payoffs and fewer risks. The identities of the bot criminals are preserved when they carry out concerted attacks since zombies (attack sources) are not owned by the attackers.

A recent report released by McAfee (2005) indicated that the number of potentially malicious threats emerging each month increased from roughly 300 to 2,000 between 2003 and 2005, largely due to the growing numbers of bot malware. Another independent report, released by Sophos (2006), highlighted that an unpatched computer with neither antivirus protection nor firewall installed would have a 50 percent chance of becoming a zombie within 30 minutes of being connected to the internet. These commandeered zombies can then be abused to facilitate the following high tech crimes.

Distributed denial of service attacks

Since the combined bandwidth of botnets often overwhelms the available bandwidth of the target servers, botnets can be leveraged to orchestrate DDoS attacks that could deplete the network bandwidth and other computational resources of the targeted sites. As recently as 6 February 2007, DDoS attacks reportedly carried out by botnets targeted several root servers hosting the domain name service (which translates domain names to numeric IP addresses) including one maintained by the United States Department of Defense (Sophos 2007).

Advantages of using botnets to launch DDoS attacks, frequently through public IRC channels, include magnified impact of the attack and not requiring the employment of any source IP address spoofing. This thwarts the use of the ingress filtering defensive mechanism used to detect and counteract spoofed source IP addresses.

Recent incidents involving the use of botnets to launch DDoS attacks are outlined in cases 1 to 3 of Box 1. Botnet controllers have also been known to offer targeted sites protection against DDoS attacks, although such offers often come without any guarantee.

Spam dissemination

As at April 2005, the spam statistical report released by Symantec (2005) indicated that 61 percent of global email is identified as spam. Categories of spam include health and medicine (e.g. Viagra), financial and stock, adult services, watch advertisements, and other advertisements.

Given the magnitude of spam and the potential financial gain in sending these massive amounts of spam, the computing power of zombies is harnessed to magnify the amount of spams. Increasingly, botnets are seen as the preferred method of spamming. For example, it is estimated that 70 percent of stock related spam is forwarded using botnets (Mathieson 2006) and the unavailability of a major botnet was suspected to have contributed to a significant (30%) drop in the number of spam emails detected in the first week of January 2007 (Broersma 2007). In using botnets to disseminate, the originating source of the real spammers can also be disguised.

Spamming is becoming more sophisticated. As recently as October 2006, a new 'spam-bot' malware, SpamThru, was uncovered (Stewart 2006) that has the following sophisticated features:

- installs its own antivirus scanner to eliminate competing malware installed on compromised machines
- downloads and leverages a template containing the spam to become its own spamming machine (instead of being a spam proxy)
- uses the advanced encryption scheme (AES), an encryption standard adopted by the United States government, to prevent unauthorised third parties from downloading the spam templates (without the corresponding decryption key)
- sends randomised GIF-based spam messages to avoid anti-spam measures that reject messages based on a static message.

Recent cases of using botnets to disseminate spam include case 4 outlined in Box 1.

Research on anti-spam measures is ongoing. Popular measures include evaluating senders based on their historical behaviours. For example, anti-spam solutions might examine whether a particular email (or IP) address has engaged in spamming. This measure, however, could result in the blacklisting of unwitting spammers – as the owners of these systems are often unaware that their systems have been used to send spam – as spam sources.

Facilitate phishing

Phishing attacks are also becoming more sophisticated and the number of such attacks is on the rise. A recent McAfee report (2005) indicated that an estimated 75 to 150 million phishing emails are circulated each day over the internet.

As recently as August 2006, a single botnet that controls more than 20,000 distinct IP addresses was reportedly used to send UK firms millions of phishing emails with subject lines referring to either NatWest or Bank of Scotland (DHS 2006). The email contained an inline image. Once the email recipients clicked on the image, they were directed to a website where they were instructed to input their personal information. The obtained information could then be used by the attackers to siphon cash from the victims' bank accounts.

Box 1: Examples of recent incidents involving the use of botnets

Case 1: DDoS case in New Jersey: A businessman and a 16-year-old hired hacker were arrested on 18 March 2006 for launching DDoS attacks against websites of the businessman's competitors in the online sports clothing market. The businessman recruited the hacker through an online instant messaging service, and gave him a list of ten competitor websites to attack. The DDoS attacks, repeated over five months, were carried out using a botnet controlled by the hacker. The hacker had infected 2,000 unprotected computers, turning them into zombies to carry out the concerted attacks. One business reportedly suffered more than 30 attacks, causing US$600,000 in losses. However, the DDoS attacks also affected the ISP companies that hosted the websites' servers, as well as at least 1,000 unrelated businesses as far away as Europe. The FBI estimated that the attacks cost over US$2.5 million. After an initial report to New Jersey authorities by one of the affected businesses, the FBI investigated, posing as a hacker in an online instant messaging service where they were contacted by the same businessman seeking further help hacking into competitors' websites. Prosecutors stated that they were seeking to have the juvenile hacker tried as an adult. | *Source: FBI 2005; McAfee 2005*

Case 2: Australian botnet-related case: In March 2006, the Australian High Tech Crime Centre (AHTCC) reported that a Melbourne man had been charged with botnet-related activities after a joint investigation by the AHTCC, the Australian Federal Police, and NSW and Victoria Police. Initial information was provided by the Belgian Federal Computer Crime Unit following a series of DDoS attacks on IRC servers in Australia, which also affected the United States, Singapore and Austria. The suspect, a 22-year-old male, faces charges under s 474.14 of the *Criminal Code Act 1995* (Cth), which creates an offence of using a telecommunications network (such as the internet) with intention to commit a serious offence. The serious offence involved may be any offence punishable by five years or more under Commonwealth, state, territory or foreign laws, and the maximum penalty under s 474.14 is as for the serious offence. A committal hearing in this prosecution was listed for December 2006. | *Source: AHTCC 2006*

Case 3: Russian hacker trio jailed for botnet-derived DDoS attacks: Three Russian nationals were arrested in a joint operation between Russian authorities and the then UK National Hi-Tech Crime Unit and sentenced to eight years imprisonment for extorting money from online gambling sites. Prosecutors stated that the Russian trio had conducted 54 botnet-derived DDoS attacks on gambling site servers in 30 countries over a six-month period in 2003, following up these attacks with demands for money. One target of the attacks was the UK-Australian betting site Canbet, which reportedly refused to pay an initial demand of $10,000 and was then hit with a DDoS attack that disabled its servers' operation, costing $200,000 per day until restored. | *Source: Dunn 2006a*

Case 4: Selling armies of infected computers to hackers and spammers: In January 2006, a 20-year-old Californian, Jeanson James Ancheta, pleaded guilty to computer fraud and spam offences connected to his dealings in botnets. Ancheta created new variants of the 'rxbot' robot family.11 and distributed these variants to establish several botnets. He then offered hired out the botnets to others for the purposes of sending spam and launching DDoS attacks, thus earning Ancheta thousands of dollars. It was also alleged that Ancheta used the botnets to generate income from the surreptitious installation of adware on the zombies. In May 2006, Ancheta was sentenced to 57 months in federal prison. | *Source: US Department of Justice 2006b*

Case 5: Using botnets to install adware: A 20-year-old Californian was indicted in February 2006 over the use of botnets to install adware. Christopher Maxwell pleaded guilty to releasing the program installing unauthorised adware in January 2005, which went on to cause major disruptions to computer systems including those of hospital networks and the US military. In the most serious incident, the intensive care section, operating room doors and paging system for the medical staff of a Seattle hospital were affected, and backup systems had to be used. It was reported that a compensation payment to the hospital of around US$250,000 was part of the plea arrangement. Maxwell and two juvenile co-conspirators were reported to have been paid $100,000 in advertising commissions in relation to the adware. In August 2006, Maxwell was sentenced to 37 months in prison and three years of supervised release for conspiracy to intentionally cause damage to a protected computer and commit computer fraud. | *Source: US Department of Justice 2006a; Dunn 2006b*

One popular countermeasure against phishing is to block data transmissions originating from specific IP addresses that are known to be associated with spammers and phishers. This, however, could result in the blacklisting of these unwitting 20,000 distinct IP addresses.

Host illegal data and disseminate malware

Bots that are specially designed for file sharing over IRC channels (e.g. Iroffer from http://iroffer.org/) could potentially be leveraged to host illegal data such as child pornography pictures and pirated software. Botnets can also be leveraged for secondary level infection, such as downloading malware and Trojans that can be used to allow attacker access to data (Ianelli & Hackworth 2005):

- *persistent data* available on the hard drive or stored in the registry – this includes personal and confidential information such as login credentials, email contacts, financial information and trade secrets
- *transient data* which includes screen shots, keystrokes, and network traffic observed on connected networks.

Such data can subsequently be used to facilitate other crimes such as identity theft. Recent examples involving the use of botnets to disseminate malware include case 5 outlined in Box 1.

In an incident in June 2006, three suspected members of the M00P virus-writing gang were arrested by the Metropolitan Police Computer Crime Unit, the Finnish National Bureau of Investigation and the Finnish Pori Police Department, in connection with a conspiracy to infect computers with malware to create a botnet. In an unrelated incident, three suspects were arrested in the Netherlands on suspicion of controlling a vast illegal computer network made up of more than 1.5 million zombies. It was alleged that the trio used the botnets to steal PayPal and eBay account information (Keizer 2005).

It has been acknowledged that botnets can speed up the spreading of worms. For example, the Symantec Security Response Team speculated that 2004's Witty worm that infected and crashed tens of thousands of servers, was probably launched by a botnet with a membership size of 2,400 (Lemos 2004).

Facilitate click fraud

Several search engines such as Google and Yahoo and online sites are supported either in part or mainly by a pay-per-click advertisement revenue model (based on the click-through rate of an advertisement). However, such a revenue mechanism, where an advertiser is charged, could potentially (and easily) be abused by the hosting sites. Click fraud has been identified as an emerging threat to e-commerce.

One of the measures taken to detect click fraud is to monitor click through patterns (based on the geographical locations of IP addresses). However, botnets usually control a large number of geographically dispersed IP addresses. Zombies located in different parts of the world infected with bot malware (e.g. Clickbot.A, coded to obtain financial profit from fraudulent clicks on online advertisements) can be abused to circumvent such measures.

This poses a threat to both the advertisers and the content providers. For example, if each of the 20,000 members of a botnet clicks on twenty different advertising sites per day, then the advertisers will suffer a substantial financial loss. Content providers (e.g. Google) could also face a ban or possibly a lawsuit for charging advertisers over fraudulent click referrals. In July 2006, Google agreed to pay up to US$90 million to settle a lawsuit alleging it had overcharged thousands of advertisers for such bogus sales referrals.

Another recent example involving the use of bots to facilitate click fraud is the exploitation of 34,000 zombie computers (infected with Clickbot.A) controlled remotely through several web servers to defraud pay-per-click advertising systems (McKewan 2006).

Legislative framework

Many of the wide-ranging activities and consequences resulting from botnet attacks constitute offences under Australia's legislative framework.

Criminal Code Act 1995 *(Cth)*

- **s 477.1**: unauthorised access, modification or impairment with intent to commit a serious offence
- **s 477.2**: unauthorised modification to cause impairment
- **s 477.3**: unauthorised impairment of electronic communication
- **s 478.1**: unauthorised access to, or modification of, restricted data
- **s 478.2**: unauthorised impairment of data held on a computer disk, etc
- **s 478.3**: possession or control of data with intent to commit a computer offence
- **s 478.4**: producing, supplying or obtaining data with intent to commit a computer offence
- **s 480.4**: dishonestly obtaining or dealing in personal financial information
- **s 480.5**: possession or control of thing with intent to dishonestly obtain or deal in personal financial information.

Penalties

A person who is guilty of an offence against the respective section is punishable by the following penalties:

- **s 477.1**: a penalty not exceeding the penalty applicable to the serious offence (an offence that is punishable by imprisonment for life or a period of five or more years)
- **s 477.2** and **s 477.3**: 10 years imprisonment
- **s 478.1** and **s 478.2**: two years imprisonment
- **s 478.3**, **s 478.4** and **s 480.5**: three years imprisonment
- **s 480.4**: five years imprisonment.

A sample botnet scenario

An attacker loads bot malware on several compromised computers including computers owned and operated by an Australian Government entity. Once the bot malware has been installed on these computers, the following can be performed:

1) Open a backdoor for the attacker to browse or modify files (e.g. win.ini and system.ini files) and to copy the malware to startup folders for different users on the infected computers. This violates s 478.1 of the *Criminal Code Act 1995* (Cth) since the attacker causes unauthorised modification of data held in a computer; the attacker knows such modification is unauthorised; the attacker is reckless as to whether the modification impairs or will impair the reliability, security or operation, of any such data; and the data that is modified is held in an Australian Government computer.
2) Install malware such as Arhiveus.A (MayAlert) to encrypt data on compromised computers for online ransom (i.e. cryptovirology). This violates s 477.1 of the Act since the attacker causes unauthorised modification of data held in a computer to facilitate the commission of a serious offence against a Commonwealth, state or territory law.
3) Install keyloggers that forward all captured information to the attacker. This violates s 478.1 of the Act. If intent to facilitate the commission of a serious offence against a Commonwealth, state or territory law is established, then s 477.1 of the Act is violated.
4) Redirect DNS requests for certain (banking) sites to designated phishing sites. At the phishing sites, the victims might then be persuaded to enter their login credentials which are captured by the attacker to facilitate fraud. This violates s 478.1 of the Act since there is intent to facilitate the commission of fraud.

Using botnets to disseminate spyware (including adware) may also result in a breach of the *Privacy Act 1988* (Cth), the *Telecommunications Act 1997* (Cth), or the *Telecommunications (Interception) Act 1979* (Cth) as personal financial information is harvested and collected without the victim's consent.

Conclusions

Bot malware is constantly evolving. Although the legislative framework in Australia provides a robust response to arresting botnet-related activities, a community effort is required to mitigate botnet-related risks. This includes developing new techniques to observe botnets and learn more about evolving bot malware (e.g. honeypot projects), user education (e.g. not to resort to illegal hacking-back remedies, timely application of operating system and application software updates, along with regular updates to antivirus signatures), and enhancing public–private partnerships to fully utilise the legislative framework.

Acknowledgments

The Australian High Tech Crime Centre (AHTCC) funded this research.

References

AusCERT 2006. *2006 Australian computer crime and security survey*. Brisbane: AusCERT

Australian High Tech Crime Centre (AHTCC) 2006. International internet investigation nets arrest. *Media release* 22 March

Barford P & Yegneswaran V (forthcoming). An inside look at botnets, in *Special Workshop on Malware Detection Proceedings*, Arlington, VA: Springer

Broersma M 2007. Spam shows sudden slide. *Computerworld.com* 10 January

Cooke E, Jahanian F & McPherson D 2005. The zombie roundup: understanding, detecting, and disrupting botnets, in *SRUTI '05 Workshop Proceedings*. Berkeley CA: USENIX Association: 35–44

Dunn JE 2006a. Heavy sentence handed to cyber-blackmailers, *Computerworld.com* 6 October

Dunn JE 2006b. Botnet chaos shut down hospital. *Techworld.com* 5 May

Federal Bureau of Investigation (FBI) 2005. The case of the hired hacker: entrepreneur and hacker arrested for online sabotage. *Media release* 18 April

Ianelli N & Hackworth A 2005. *Botnets as a vehicle for online crime*. Pittsburgh PA: CERT Coordination Center

IEEE 2006. News brief. *IEEE Computer* 39(10)

Keizer G 2005. Dutch botnet bigger than expected, *InformationWeek* October 21

Lemos R 2004. Alarm growing over bot software. *CNET news* 30 April

Mathieson SA 2006. Hot stocks to your inbox. *Infosecurity today* September/October: 10–13

McAfee 2005. *McAfee virtual criminology report*. Santa Clara CA: McAfee

McKewan A 2006. Botnets: zombies get smarter. *Network security* no. 6: 18–20

Milburn R 2006. Will IT automate the financial supply chain? *Computerworld* 21 September

PricewaterhouseCoopers (PWC) 2006. *DTI information security breaches survey 2006*. London: Department of Trade and Industry

Schaffer GP 2006. Worms and viruses and botnets, oh my! *IEEE security & privacy* 4(3): 52–58

Sophos 2007. Did your PC try to bring down the internet last night? asks Sophos. *Media release* 7 February

Sophos 2006. *Stopping zombies, botnets, and other email-borne threats*. Abingdon: Sophos

Stewart J 2006. SpamThru trojan analysis. *Secureworks.com* 18 October

Symantec 2005. *Symantec spam statistics*. Cupertino CA: Symantec

United States Department of Homeland Security (DHS) 2006. *Daily open source infrastructure report*. 4 August

United States Department of Justice 2006a. 'Botherder' dealt record prison sentence for selling and spreading malicious computer code. *Media release* 8 May

United States Department of Justice 2006b. California man sentenced for 'botnet' attack that impacted millions. *Media release* 25 August

Dr Kim-Kwang Raymond Choo is a research analyst with the Australian Institute of Criminology.

**General editor, *Trends & issues in crime and criminal justice* series:
Dr Toni Makkai, Director,
Australian Institute of Criminology,
GPO Box 2944 Canberra ACT 2601
Note: *Trends & issues in crime and criminal justice* papers are peer reviewed.**

The AIC is a statutory body with a Board of Management comprising Australian, state and territory government representatives, administered under the *Criminology Research Act 1971*.