2

Nature, Prevalence and Economic Impact of Cyber Crime

Introduction

2.1 This chapter addresses the nature, prevalence and economic impact of cyber crime.

2.2 The problem of cyber crime crosses many traditional technical, conceptual and institutional boundaries, and, due to its prevalence, has real and increasing social and economic impacts on all Australians. The chapter concludes that because of the inter-related nature of the different aspects of cyber crime, a more holistic and strategic approach must be taken to its prevention.

Nature of cyber crime

2.3 This section demonstrates that cyber crime is highly complex, self-reinforcing, technologically advanced, geographically widespread and indiscriminate by examining the history, tools, industrial nature, perpetrators and victims of cyber crime.

Cyber crime and the Internet

2.4 Mr Peter Watson, Microsoft Pty Ltd, told the Committee that the Internet, by its very design, is an inherently vulnerable network which has enabled cyber crime to flourish in a new virtual 'Wild West' environment.[1]

2.5 The Internet originated from a relatively basic network set up to share information between trusted people and organisations for military and academic purposes, with no view to the security of the computers attached to these networks, nor the information stored on these computers.[2]

2.6 Today, this open and insecure system has evolved into a world wide network, directly connecting in excess of one billion users, and is employed for much more than the simple sharing of information.

2.7 Cyber crime flourishes in the online environment for a variety of reasons:

- the fundamentally insecure nature of the Internet leaves computers vulnerable to exploitation by less-than-trustworthy Internet users;
- the huge number of computers connected to the Internet gives cyber criminals a wide array of targets;
- the Internet is an effective medium for running automated systems, thus leading to the automation of online criminal activity; and
- the unregulated nature of the Internet makes it inherently difficult to control the content and data traversing the network, thus impeding efforts to combat malicious exploitation of the Internet.[3]

Why do people commit cyber crime?

2.8 Cyber criminals may be motivated by curiosity, fame-seeking, personal reasons (such as stalking or emotional harassment), political reasons (such as protests), espionage or cyber warfare. However, during the inquiry financial gain was repeatedly identified as the prime motivator of cyber crime.[4]

[1] Mr Peter Watson, Microsoft Pty Ltd, *Transcript of Evidence*, 9 October 2009, p.18.

[2] CSIRO, *Submission 26*, p.4; Dr Paul Twomey, Internet Corporation for Assigned Names and Numbers (ICANN), *Transcript of Evidence,* 8 October 2009, p.2.

[3] See for example: Australian Computer Society, *Submission 38*, p.2. Dr Paul Twomey, ICANN, *Transcript of Evidence,* 8 October 2009, p.2; Australian Communications Consumer Action Network (ACCAN), *Submission 57*, p.53; Mr Stephen Wilson, Lockstep Technologies Pty Ltd, *Transcript of Evidence*, 9 October 2009, p.44; Symantec Asia Pacific Pty Ltd, *Submission 32*, p.19; Microsoft Australia, *Submission 35*, p.1; Internet Safety Institute, *Submission 37*, p.5.

[4] See for example: Dr Russell Smith, Australian Institute of Criminology (AIC), *Transcript of Evidence*, 19 August 2009, p.3; AIC, *Submission 41*, p.10; Mr Michael Sinkowitsch, Fujitsu

2.9 The Committee heard that cyber crime has become a highly lucrative business through cyber attacks which involve the theft of personal information, fraud, illegally accessing financial systems and online extortion. Additionally, an underground economy has developed through which cyber criminals may earn money by trading cyber crime related goods and services.[5]

How do people currently commit cyber crime?

2.10 Modern cyber crime is facilitated by a range of technologies and techniques including:

- hacking;
- malicious software (malware);
- botnets;
- spam;
- DNS based attacks;
- phishing;
- identity theft and identity fraud;
- scams;
- extortion;
- underground cyber crime forums; and
- money laundering techniques.

2.11 As with all aspects of cyber crime, cyber crime technologies and techniques are often interrelated and complementary. These technologies and techniques, and their purposes, are defined below.

Australia Ltd, *Transcript of Evidence*, p.49; Dr Paul Twomey, ICAAN, *Transcript of Evidence*, 8 October 2009, p.6; Organisation for Economic Cooperation and Development (OECD), *Malicious Software (Malware): A Security Threat to the Internet Economy*, OECD, June 2008, p.17.

[5] See for example: Dr Russell Smith, AIC, *Transcript of Evidence*, 19 August 2009, p.3; Mr Peter Coroneos, Internet Industry Association (IIA), *Transcript of Evidence*, 11 September 2009, p.13; Dr Paul Twomey, ICANN, *Transcript of Evidence*, 8 October 2009, p.6; Australian Federal Police (AFP), *Submission 25*, p.3; PayPal Incorporated, *Submission 60*, Symantec Asia Pacific Pty Ltd, *Submission 32*, p.3; Department of Broadband, Communications and the Digital Economy (DBCDE), *Submission 34*, p.6.

Hacking

2.12 'Hacking' is a term with multiple meanings. It can refer to testing and exploring computer systems, highly skilled computer programming or the practice of accessing and altering other people's computers. Hacking may be carried out with honest aims or with criminal intent.[6]

2.13 In relation to cyber crime, and for the purpose of this report, hacking refers to the practice of illegally accessing, controlling or damaging other people's computer systems. A hacker may use their own technical knowledge or may employ any of the cyber crime tools and techniques that are listed below.

Malicious software (Malware)

2.14 Malware is a general term for software designed to damage or subvert a computer or information system.[7] A range of different types of malware exists:

- viruses, worms and trojans are pieces of computer code or computer programs that automatically infiltrate computer systems, to degrade computer performance or to deliver other types of malware;[8]
- a backdoor permits a computer to be remotely controlled over a network;[9]
- rootkits are sets of programs that hide malware infections on a computer by concealing infected files and turning off anti-virus protection programs;[10] and
- keystroke loggers and spyware are programs that illegally capture data from a computer (spyware is related to a legitimate type of software called adware, described below).[11]

[6] See for example: G Urbas and KR Choo, *Resource materials on technology-enabled crime*, AIC, Canberra, 2008, p.83; AIC, *High tech crime brief: Hacking offences*, AIC, 2005, p.1.

[7] OECD, *Malicious Software (Malware): A Security Threat to the Internet Economy*, OECD, June 2008, p.10.

[8] See for example: OECD, *Malicious Software (Malware): A Security Threat to the Internet Economy*, OECD, June 2008, p.91; G Urbas and KR Choo, *Resource materials on technology-enabled crime*, AIC, Canberra, 2008, p.87; OECD, *Malicious Software (Malware): A Security Threat to the Internet Economy*, OECD, June 2008, p.91.

[9] OECD, *Malicious Software (Malware): A Security Threat to the Internet Economy*, OECD, June 2008, p.90.

[10] OECD, *Malicious Software (Malware): A Security Threat to the Internet Economy*, OECD, June 2008, p.90;

2.15 Malware may propagate through virtually any medium that contains data or transmits data between information systems including infected websites, email, instant messaging, removable data hardware (such as USB drives), file sharing networks and wireless networks.[12]

2.16 Previously, websites transmitting malware tended to be less reputable, and poorly maintained, many of which were designed purely to infect computers. However, cyber criminals are increasingly using highly-reputable and popular legitimate websites and social networking pages to infect computers. A cyber criminal will exploit a vulnerability of the system that is hosting the website or social networking page in order to hide malware in the system, unbeknown to the legitimate website operator. When a benign user visits this legitimate website or social networking page the malware will automatically and covertly install on the victim's computer.[13]

2.17 Malware may install itself on a computer via a self-propagating mechanism, or when a user clicks on a malicious link in an email, opens a malicious file or visits a website where malware is hosted.[14]

The relationship between adware and spyware

2.18 Adware is a legitimate type of software, similar to spyware, which is often automatically, and openly, installed on a computer as part of a larger software package.[15] Adware enables software providers to earn revenue by directing advertisements at the users of their software via 'pop-ups' or banner advertisements. Adware programs may also gather personal information which is then used by the adware company to tailor their advertisements to be more effective.[16]

2.19 The distinction between adware and spyware can turn on whether the adware company has adequately informed the end user of the function of

[11] See for example: OECD, *Malicious Software (Malware): A Security Threat to the Internet Economy*, OECD, June 2008, p.90-91; G Urbas and KR Choo, *Resource materials on technology-enabled crime*, AIC, Canberra, 2008, pp.79-87.

[12] OECD, *Malicious Software (Malware): A Security Threat to the Internet Economy*, OECD, June 2008, p.12;

[13] See for example: Australian Communications and Media Authority (ACMA), *Submission 56*, p.14; Symantec Corporation, *Submission 32*, p.2.

[14] OECD, *Malicious Software (Malware): A Security Threat to the Internet Economy*, OECD, June 2008, p.12;

[15] Symantec Asia Pacific Pty Ltd, *Submission 32*, p.20.

[16] AIC, *High Tech Crime Brief: More malware – adware, spyware, spam and spim*, AIC, Canberra, 2006, p.1.

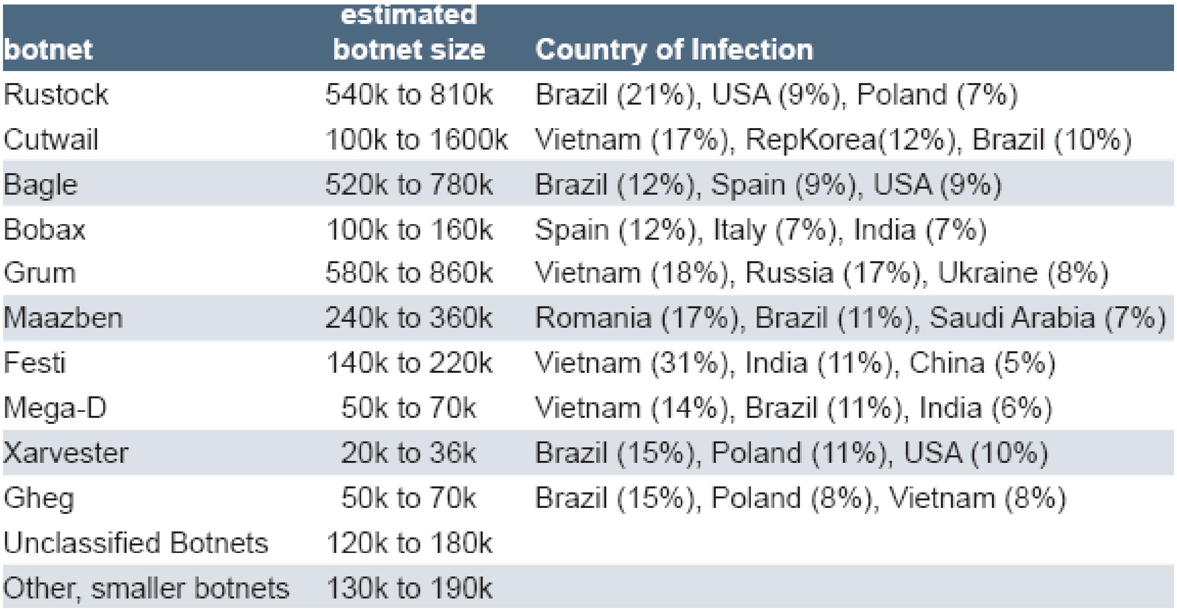
the software and the use of any personal information which is gathered.[17] Where the adware company gathers information outside of its permissions, or uses the information for purposes outside of its advertised terms, the software may cease to be adware, and become spyware.

Botnets

2.20 As previously mentioned, backdoors are a category of malware that enable a cyber criminal to remotely control an infected computer over a network. Such an infected computer is often called a robot or 'bot' computer. When several computers are infected with a backdoor and become bots, they can be simultaneously controlled from a single remote 'command and control' (C&C) mechanism. These remotely controlled networks of bot computers are known as 'botnets'.

2.21 Botnets can be comprised of a huge number of computers, with there being many documented cases of botnets comprised of more than 100,000 computers. Table 2.1 below shows the biggest botnets for 2009 as reported by MessageLabs, a subsidiary of the Symantec Corporation.

Table 2.1 Biggest botnets in 2009



botnet	estimated botnet size	Country of Infection
Rustock	540k to 810k	Brazil (21%), USA (9%), Poland (7%)
Cutwail	100k to 1600k	Vietnam (17%), RepKorea(12%), Brazil (10%)
Bagle	520k to 780k	Brazil (12%), Spain (9%), USA (9%)
Bobax	100k to 160k	Spain (12%), Italy (7%), India (7%)
Grum	580k to 860k	Vietnam (18%), Russia (17%), Ukraine (8%)
Maazben	240k to 360k	Romania (17%), Brazil (11%), Saudi Arabia (7%)
Festi	140k to 220k	Vietnam (31%), India (11%), China (5%)
Mega-D	50k to 70k	Vietnam (14%), Brazil (11%), India (6%)
Xarvester	20k to 36k	Brazil (15%), Poland (11%), USA (10%)
Gheg	50k to 70k	Brazil (15%), Poland (8%), Vietnam (8%)
Unclassified Botnets	120k to 180k	
Other, smaller botnets	130k to 190k	

Source MessageLabs, *Message Labs Intelligence: 2009 Annual Security Report*, MessageLabs, December 2009, p.8.

2.22 Botnets are considered to be one of the biggest enablers of cyber crime with the Cyberspace Law and Policy Centre, from the University of New

[17] K Howard, Mallesons Stephen Jacques, *Computers and Law*, March 2006, p.17.

South Wales, submitting that 'almost every major online crime may be traced to botnets'.[18]

2.23 Below is a description of the different functions of botnets followed by a description of methods by which botnets are becoming increasingly resilient.

Functions of botnets

2.24 A botnet can be instructed by its controller, known as a 'botmaster', to carry out a range of functions (as outlined in Figure 2.1 below) including:

- launching 'distributed denial of service' (DDoS) attacks (a method by which botnets flood a computer system with information thus damaging or shutting down the system); [19]
- hosting malicious websites (such as money laundering, malware or phishing websites) or obscene content (such as child pornography) to shield the originator from being identified; [20]
- scanning for, and exploiting, software vulnerabilities in other computers and websites; [21] and
- sending large numbers of unsolicited emails known as spam. [22]

[18] Cyberspace Law and Policy Centre (CLPC), *Submission 62*, p.3.

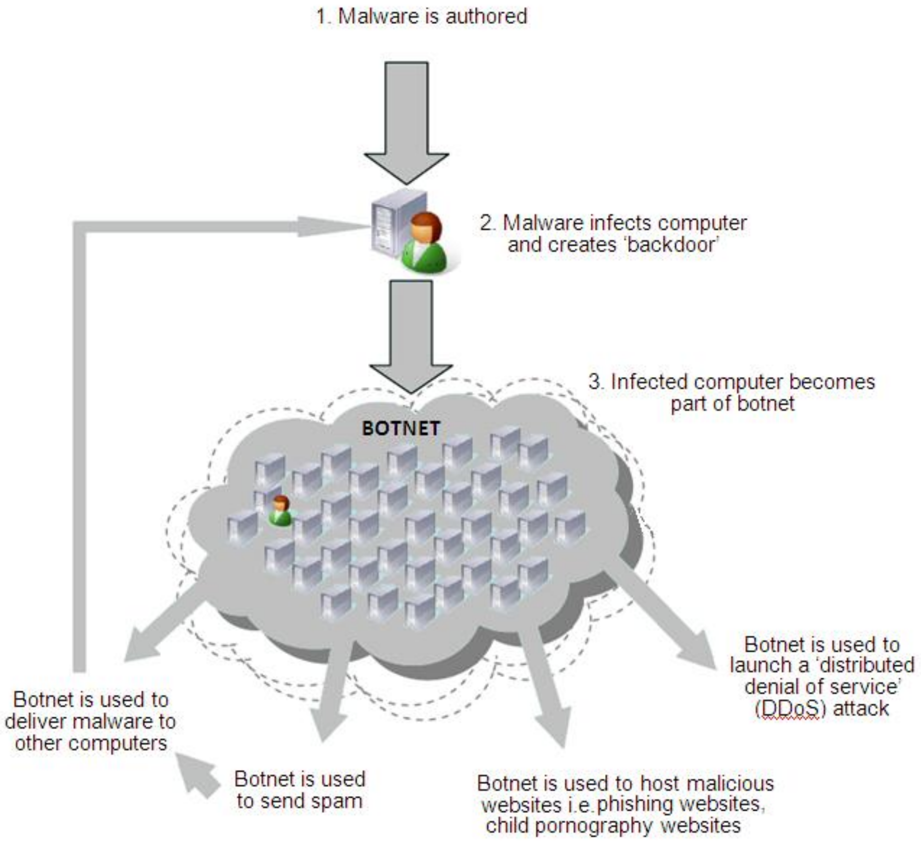
[19] OECD, *Malicious Software (Malware): A Security Threat to the Internet Economy*, OECD, June 2008, p.15. See also: G Urbas and KR Choo, *Resource materials on technology-enabled crime*, AIC, Canberra, 2008, pp.81; KR Choo, *Trends and issues in crime and criminal justice: Zombies and Botnets*, AIC, Canberra, 2007, p.4.

[20] See for example: RSA Security Inc, *Exhibit 2*, p.2; MT Banday, JA Quadri and NA Shah, 'Study of Botnets and their threats to Internet Security', *Sprouts: Working papers on information systems*, 2009, p.8, viewed 22 December 2009, <http://sprouts.aisnet.org>; OECD, *Malicious Software (Malware): A Security Threat to the Internet Economy*, OECD, June 2008, p.23.

[21] Symantec Asia Pacific Pty Ltd, *Submission 32*, p.6.

[22] Mr Graham Ingram, AusCERT, *Transcript of Evidence*, 11 September 2009, p.6.

Figure 2.1 Initiation, growth and function of a botnet


1. Malware is authored
2. Malware infects computer and creates 'backdoor'
3. Infected computer becomes part of botnet
BOTNET
Botnet is used to launch a 'distributed denial of service' (DDoS) attack
Botnet is used to deliver malware to other computers
Botnet is used to send spam
Botnet is used to host malicious websites i.e.phishing websites, child pornography websites

Source OECD Committee for Information, Computer and Communications Policy, *Malicious Software (Malware): A Security Threat to the Internet Economy*, OECD, June 2008, p. 23.

2.25 The relationship between spam and botnets is significant: spam can be used to spread malware, such as backdoors, to other computers which in turn may recruit more bot computers to a botnet (see Figure 2.1). This demonstrates the interconnectedness and self-reinforcing nature of cyber crime.[23]

Resilience of botnets

2.26 Botnets are becoming ever more resilient through: improved C&C techniques; an ability to remotely upgrade very quickly; and a practice called 'fast fluxing', which shields important parts of the botnet from being identified and shutdown.

2.27 As previously mentioned, botmasters control botnets via C&C mechanisms. The botmaster posts a command on the C&C mechanism

[23] IIA, *Submission 54*, p.3. See also: OECD, *Malicious Software (Malware): A Security Threat to the Internet Economy*, OECD, June 2008, p.37.

(often a hijacked bot computer itself), which is then automatically disseminated to the individual bot computers that comprise the botnet. Botnets can operate on a centralised model (where each bot computer individually contacts a single central C&C mechanism to receive commands) or a decentralised model (where commands can be posted on any part of the botnet and then automatically passed from computer to computer via a peer to peer network).[24]

2.28 The decentralised botnet model is extremely hard to stop or dismantle as there is no centralised C&C point which can be targeted. If a number of bot computers are identified and taken offline, the gaps in the network will close up and the botnet will continue to function.[25]

2.29 Botnets are also high resilient due to the ease with which botmasters can rapidly update the underlying malware which runs the botnet. This enables botnets to rapidly adjust to exploit newly discovered vulnerabilities, and to respond to new anti-botnet measures.[26]

2.30 Botnets are further strengthened by the process of fast fluxing, whereby important parts of a botnet can be shielded from being traced, identified and shutdown. During this process, data travelling to and from important parts of the botnet (such as bot computers that host malicious websites or C&C mechanisms) first passes through any one of a number of decoy or proxy computers. Fast fluxing refers to the practice of employing the large number of computers in a botnet to rapidly alternate which computers are used as proxies. Thus when an attempt is made to trace the host computer, the trace only leads back to one of these relatively insignificant and temporary proxy computers.[27]

[24] See for example: OECD, *Malicious Software (Malware): A Security Threat to the Internet Economy*, OECD, June 2008, p.24; AFP, *Submission 25*, p.9; JB Grizzard, VS Sharma, C Nunnery, BBH Kang and D Dagon, *Peer-to-Peer Botnets: Overview and Case Study*, in proceedings of USENIX Association First Workshop on Hot Topics in Understanding Botnets, 10 April 2007, Cambridge, USA, pp.5-6, viewed 24 December 2009, <http://www.usenix.org/event/hotbots07/tech/full_papers/grizzard/grizzard.pdf>.

[25] JB Grizzard, VS Sharma, C Nunnery, BBH Kang and D Dagon, *Peer-to-Peer Botnets: Overview and Case Study*, in proceedings of USENIX Association First Workshop on Hot Topics in Understanding Botnets, 10 April 2007, Cambridge, USA, p.1, viewed 24 December 2009, <http://www.usenix.org/event/hotbots07/tech/full_papers/grizzard/grizzard.pdf>.

[26] Symantec Asia Pacific Pty Ltd, *Submission 32*, p.6; CLPC, *Submission* 62, p.6.

[27] See for example: RSA Security Inc., *Exhibit 3*, p.2; Dr Paul Twomey, ICANN, *Transcript of Evidence*, 8 October 2009, p.8; Fortinet, *Submission 29*, p.9; Symantec Asia Pacific Pty Ltd, *Submission 32*, p.15.

Spam

2.31 Spam refers to unsolicited emails, or the electronic equivalent of 'junk mail'. Spam is often disseminated in large amounts by sending out generic emails to large lists of email addresses.[28]

2.32 Spam may be sent through normal email accounts provided by an ISP, free online email services such as Hotmail, hijacked email servers, offshore companies that specialise in sending bulk mail, or the large number of computers connected to a botnet.[29] Additionally, in order to avoid anti-spam programs that identify generic emails or offending spammer email addresses, spammers employ programs which subtly change each email or hide the actual spammer's email address.[30]

2.33 Spammers can acquire lists of email addresses by: using different pieces of address-harvesting software to locate, steal, decipher and compile email addresses; hacking into the information systems of organisations; creating fake websites which fool users into entering their email address on the website; or through buying lists of email addresses on the black market.[31]

2.34 Spam has a variety of uses including: the mass delivery of legitimate advertising;[32] the mass delivery of scams and phishing schemes;[33] and the delivery of malware and in turn the expansion of botnets.[34]

DNS based attacks

2.35 The Domain Name System (DNS) is one of the underpinning aspects of the Internet. The DNS converts user-friendly text commands (in the form of web addresses) into IP addresses (complex numbers which identify each individual computer connected to the Internet). Thus the DNS

[28] AIC, *High Tech Crime Brief: More malware – adware, spyware, spam and spim*, AIC, Canberra, 2006, p.1.

[29] See for example: P Wood, *A spammer in the works*, MessageLabs, Hong Kong, 2003, p.6; OECD, *Malicious Software (Malware): A Security Threat to the Internet Economy*, OECD, June 2008, p.27; MessageLabs, *The Dark Art of Spam*, MessageLabs, 2009, pp.3-4.

[30] P Wood, *A spammer in the works*, MessageLabs, Hong Kong, 2003, p.6.

[31] See for example: P Wood, *A spammer in the works*, MessageLabs, Hong Kong, 2003, p.6; OECD, *Malicious Software (Malware): A Security Threat to the Internet Economy*, OECD, June 2008, p.27; AIC, *High Tech Crime Brief: More malware – adware, spyware, spam and spim*, AIC, Canberra, 2006, p.1; Mr Anthony Burke, Australian Bankers Association NSW Inc., *Transcript of Evidence*, 8 October 2009, p.59.

[32] P Wood, *A spammer in the works*, MessageLabs, Hong Kong, 2003, p.1,5. See also: AIC, *High Tech Crime Brief: More malware – adware, spyware, spam and spim*, AIC, Canberra, 2006, p.1.

[33] ACCC, *Exhibit 16*, p.43.

[34] OECD, *Malicious Software (Malware): A Security Threat to the Internet Economy*, OECD, June 2008, p.27.

enables users to easily access computers that host web pages, without the need for complicated codes.[35]

2.36 Cyber criminals subvert the DNS in a number of ways:

- 'DNS spoofing' is a practice where cyber criminals hack into the DNS and replace a genuine IP address that leads to a legitimate website with a fake IP address that diverts users to a malicious website, such as a phishing website, or a website that infects computers with malware;[36]
- 'DNS hijacking' employs a trojan that changes the settings on a user's computer to access the DNS through a rogue DNS server instead of a legitimate ISP server, thus enabling users to be diverted to false websites;[37] and
- 'domain hijacking' is where a cyber criminal takes control of a domain name by stealing the identity of a domain name owner, then uses this domain name to host a malicious website.[38]

Phishing

2.37 Phishing describes an online attempt to assume the identity of, or mimic, a legitimate organisation for the purpose of convincing users to divulge personal information such as financial details, passwords, usernames and email addresses.[39]

2.38 The AIC provided the following example of a phishing website. Figure 2.2 shows the top section of a web page which appears to be from the legitimate 'Bank of the West' website.

[35] Educause, *7 things you should know about DNS*, Educause, January 2010, p.1, viewed 1 February 2010, <http://net.educause.edu/ir/library/pdf/EST1001.pdf>.

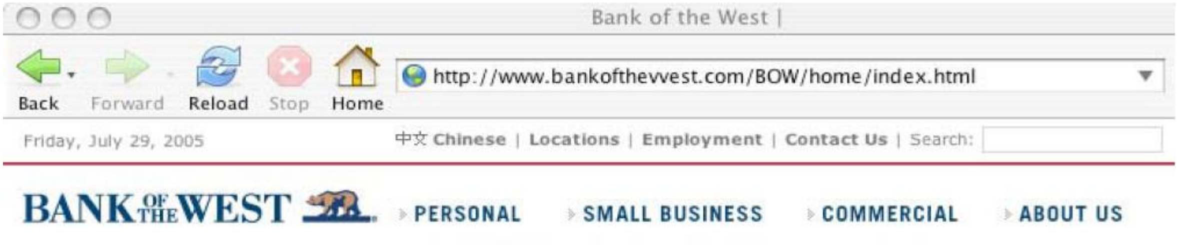
[36] Educause, *7 things you should know about DNS*, Educause, January 2010, p.1, viewed 1 February 2010, <http://net.educause.edu/ir/library/pdf/EST1001.pdf>.

[37] F Hacquebord and C Lu, *Rogue Domain Name System Servers,* blog post, TrendLabs Malware Blog, Trend Micro, 27 March 2007, viewed 26 February 2010, <http://blog.trendmicro.com/rogue-domain-name-system-servers-5breposted5d>.

[38] ICANN Security and Stability Advisory Committee, *Domain name hijacking: incidents, threats, risks, and remedial actions,* ICANN, 12 July 2005, p.8.

[39] See for example: G Urbas and KR Choo, *Resource materials on technology-enabled crime*, AIC, Canberra, 2008, p.85; Symantec Corporation, *Symantec Report on the Underground Economy July 07 – June 08*, Symantec Corporation, November, 2009, p.19.

Figure 2.2 Example of phishing website

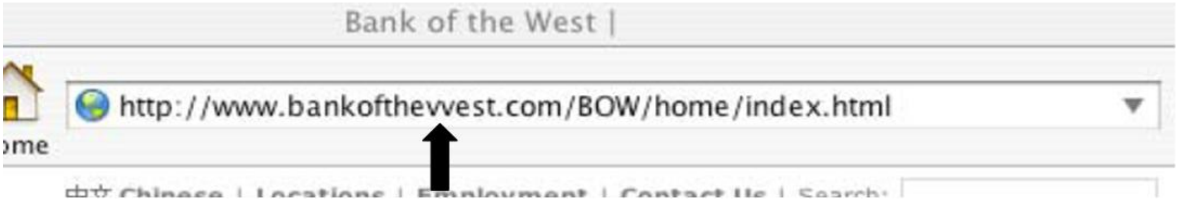


http://www.bankofthevvest.com/BOW/home/index.html

Source Australian Institute of Criminology, *Exhibit No. 5*, p. 8.

2.39 However, as demonstrated below in Figure 2.3, upon closer inspection of the address in the top bar of the browser, it can be seen that the W in 'Bank of the West' has been replaced with two V's to give the appearance of a W.

Figure 2.3 Close up of web address in phishing website



http://www.bankofthevvest.com/BOW/home/index.html

Source Australian Institute of Criminology, *Exhibit No. 5*, p. 8.

2.40 An unwitting user may be directed to this phishing website by clicking on the link in a fake spam email or through subversion of the DNS. The users may then fall for the confidence trick of the phishing website and may divulge personal details. In turn, the user may become a victim of identity theft or identity fraud.[40]

Identity theft and identity fraud

2.41 Through the use of keystroke loggers, spyware, and phishing websites cyber criminals may obtain a wide range of personal details. This is known as identity theft. These stolen details may then be used to commit 'identity fraud' (such as illegally accessing a victim's bank or credit card account, or taking out loans under a victim's name), sold online to other cyber criminals or used to fabricate fake official documents such as passports.[41]

[40] Dr Russel Smith, AIC, *Transcript of Evidence*, 19 August 2009, p.6.

[41] See for example: Symantec Corporation, *Symantec Report on the Underground Economy July 07 – June 08*, Symantec Corporation, November, 2009, pp.19, 24; Australian Bureau of Statistics, 2007 *Personal Fraud Survey*, ABS, Cat. No. 4528.0, 2007, p.8; Australian Government, *Dealing with identity theft: Protecting your identity*, Attorney General's Department (AGD), 2009, p. 4; AusCERT, *Computer Crime and Security Survey*, AusCERT, 2006, p.28.

2.42 Stolen information may also be used to commit further cyber crime activities. For example, a cyber criminal may use a stolen identity to open a new Internet account with an ISP from which to commit criminal acts.[42]

Scams

2.43 Online scams are another lucrative activity for cyber criminals. A plethora of scams exist on the Internet and new scams are continually emerging. Some of the scams brought to the Committee's attention were: romance scams, where victims hand over money to fraudulent participants on online dating websites (see the case study below for a victim's account of such a scam); advance-fee scams where the victim is promised large returns on an upfront payment; and fake lottery, ticketing or online shopping scams, where victims are fooled into paying for a nonexistent product.[43]

Case study: A victim's account of a romance scam

> Witness A, who is based in Australia, established an online relationship via a dating website with a man claiming to be a citizen of the USA. The man claimed to be travelling to Nigeria to work, after which he proposed to visit Witness A in Australia. Over the following months the man claimed to have run into a range of difficulties while in Nigeria and repeatedly asked for assistance in the form of money transfers and the provision of valuable goods. Witness A was suspicious of these requests, but felt emotionally compelled to assist their 'partner' to travel to Australia. Witness A lost AUD$20,000 before becoming aware that they were being victimised, and suffered significant emotional distress as a result of the scam.

Source Witness A, *Transcript of Evidence*, 17 March 2010, pp.2-4.

2.44 Perpetrators may use other cyber crime tools to fashion and disseminate online scams. For example, a cyber criminal may use seemingly inconsequential information gained from a spyware program, such as an address or friends' names, to make a personalised and highly convincing scam email. Additionally, a cyber criminal may seek to reach a wide number of victims by sending out a scam in a spam email.

[42] Symantec Corporation, *Symantec Report on the Underground Economy July 07 – June 08*, Symantec Corporation, November 2009, p.19.

[43] See for example: AIC, *Submission 41*, p.4; Mr Scott Gregson, Australian Competition and Consumer Commission (ACCC), *Transcript of Evidence*, 18 November 2009, p.1; ACCC, *Exhibit 16*, p.10.

Extortion

2.45 Cyber criminals carry out online extortion via DDoS attacks and specially designed malware.

2.46 Cyber criminals may threaten to carry out a DDoS attack on a business' website if they don't pay a fee. This is particularly the case with businesses that are wholly reliant on their website, such as online gambling companies. For example, in 2006 three Russian nationals were found guilty of, among other offences, carrying out a DDoS attack on an Australian gambling website when the company refused to pay $10,000 in extortion money. The DDoS attack shut down access to the gambling website and was said to have cost the gambling company $200,000 in lost revenue.[44]

2.47 Additionally, a virus, worm or trojan may be designed to automatically encrypt the data on an infected computer. The cyber criminal will then demand money from the victim in return for the 'key' with which to unencrypt the data.[45]

Underground cyber crime forums and websites

2.48 Cyber criminals utilise online forums and websites in order to communicate and trade. These websites or forums are often run purely for the purpose of facilitating cyber crime, and may be hosted on hijacked bot computers. This issue is discussed further in the section on the cyber crime industry below.[46]

Money laundering techniques

2.49 Financially motivated criminals use the online environment to launder illicit money received through other cyber crime activities. A variety of techniques exist for online money laundering including the use of money mules and 'virtual' currencies from online games.

2.50 Money mules are often benign Internet users, recruited via websites set up to lure users into applying for work-from-home jobs as a 'financial officer'. They receive funds into their bank account from cyber criminals, withdraw the money in cash and send the money back to the cyber

[44] KR Choo, *Trends and issues in crime and criminal justice: Zombies and Botnets*, AIC, Canberra, 2007, p.4.

[45] OECD, *Malicious Software (Malware): A Security Threat to the Internet Economy*, OECD, June 2008, p.16.

[46] Symantec Corporation, *Symantec Report on the Underground Economy July 07 – June 08*, Symantec Corporation, November 2009, p.9.

criminals via a wire transfer service. By withdrawing the money in cash, the sum of money becomes very hard to trace. In return for this service the mule is given a commission by the cyber criminal.[47]

2.51 The Northern Territory Government suggested that immediate wire transfer services such as Western Union were one of the main methods for mules to transfer illicit cash.[48]

2.52 Many online games have a virtual economy by which online players can exchange items within the game for virtual currencies. A gamer may pay real world dollars to receive a certain amount of the virtual currency for use in the game. A money launderer may purchase virtual currency using illicit cash, then exchange the virtual currency back into real world cash, thus reducing the traceability of the illicit funds.[49]

Interrelatedness of cyber crime techniques and tools

2.53 The different tools and techniques of cyber crime cannot be viewed in isolation. Below is a brief summary of some key relationships:

- malware can create botnets which in turn may scan other systems for vulnerabilities and infect other computers with malware;
- botnets may be used to send spam, which in turn delivers malware and extends the botnet;
- malware may steal personal information which may then be used to create and disseminate spam, phishing schemes and scam emails; and
- botnets (through fast fluxing) may perpetuate the hosting of malicious websites which facilitate further cyber crime such as phishing websites, mule recruitment websites or underground cyber crime forums.

The cyber crime industry

2.54 Australian governments, businesses and home-users are being targeted by a highly organised cyber crime industry. Below is a brief description of the emergence and operation of the cyber crime industry and an examination of its ramifications for cyber crime more generally.

[47] Australian Broadcasting Corporation (ABC), *Fear in the Fast Lane*, Four Corners program transcript, ABC, 17 August 2009, viewed 11 January 2010, <http://www.abc.net.au/4corners/content/2009/s2658405.htm>; Australian Bankers' Association, *Submission 7.1*, p.2. See also: Mr John Geurts, *Transcript of Evidence*, 8 October 2009, p.57; Mr Craig Scroggie, *Transcript of Evidence,* 9 October 2009, p.54-55.

[48] Northern Territory Government, *Submission 53*, p.1.

[49] AIC, *Submission 41*, p.8-9.

The emergence and operation of the cyber crime industry

2.55 The current cyber crime industry is driven by an underground cyber crime market place. Due to an increased number of people looking to commit cyber crime, and a resulting increased demand for cyber crime tools and services, an underground market has emerged where cyber criminals may purchase and supply cyber crime goods (such as pre-packaged malware and stolen information) and services (such as spamming or DDoS attack services). This market is often referred to as the underground cyber crime economy.[50]

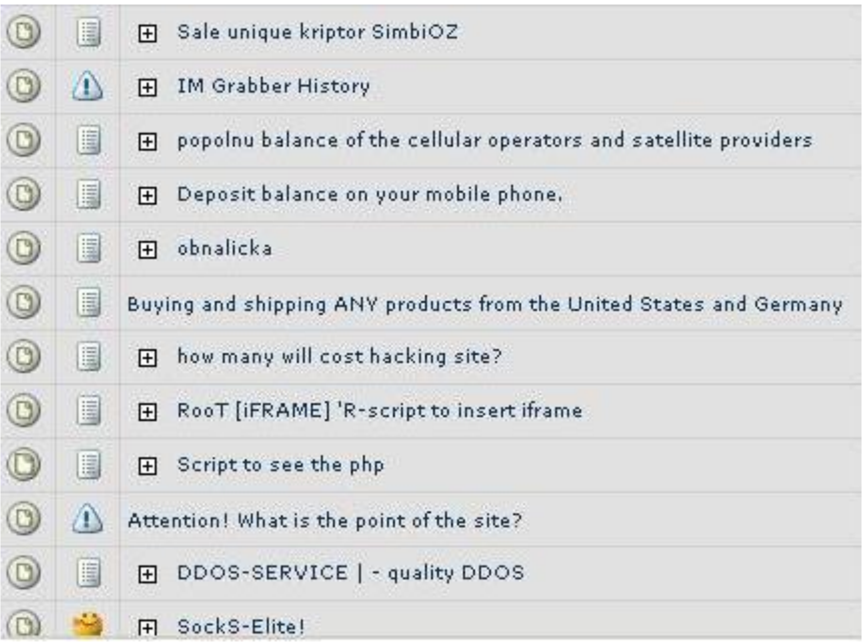
2.56 The trade that occurs in this underground market is often carried out on online cyber crime forums. In order to evade law enforcement, these forums are often hidden and require membership. Detective Superintendent Brian Hay from the Queensland Police Service described these forums as 'an Aladdin's cave of criminality'.[51]

2.57 Figure 2.4 below shows a screenshot from an online cyber crime forum. The row second from the bottom shows a cyber criminal advertising a DDoS attack service, while the sixth row from the bottom shows a potential cyber criminal inquiring as to the cost of having a website hacked.

[50] See for example: Internet Safety Institute, *Submission 37*, p. 7; OECD, *Malicious Software (Malware): A Security Threat to the Internet Economy*, OECD, June 2008, p.16; AFP, *Submission 25*, pp.4,6; Dr Russell Smith, AIC, *Transcript of Evidence*, 19 August 2009, p.8.

[51] See for example: Detective Superintendent Brian Hay, quoted in ABC, *Fear in the Fast Lane*, Four Corners program transcript, ABC, 17 August 2009, viewed 11 January 2010, <http://www.abc.net.au/4corners/content/2009/s2658405.htm>; Symantec Corporation, *Symantec Report on the Underground Economy July 07 – June 08*, Symantec Corporation, November 2009, pp.4-5; Dr Russell Smith, AIC, *Transcript of Evidence*, 19 August 2009, p.8; Mr Craig Scroggie, Symantec Corporation, *Transcript of Evidence*, 9 October 2009, p.55.

Figure 2.4 Screenshot of an online cyber crime trade forum



⊞ Sale unique kriptor SimbiOZ

⊞ IM Grabber History

⊞ popolnu balance of the cellular operators and satellite providers

⊞ Deposit balance on your mobile phone.

⊞ obnalicka

Buying and shipping ANY products from the United States and Germany

⊞ how many will cost hacking site?

⊞ RooT [iFRAME] 'R-script to insert iframe

⊞ Script to see the php

Attention! What is the point of the site?

⊞ DDOS-SERVICE | - quality DDOS

⊞ SockS-Elite!

Source Panda Security, *Cybercrime… for sale*, blog post, Panda Security Forum, 24 April 2007, viewed 13 January 2010, <http://support.pandasecurity.com/forum/viewtopic.php?f=16&t=608>.

2.58 The *Symantec Global Internet Security Threat Report: Trends for 2008* listed the most commonly traded cyber crime goods and services, and the prices of these goods and services, as observed by Symantec during 2008. Included were credit card information (trading at between US$0.06 to US$30 per card), full identities (trading at between US$0.70 to US$60) and scam design and delivery services (US$5 to US$20 for design, US$2.50 to US$100 per week for scam website hosting).[52]

2.59 Forums such as these constitute an integral part of the underground economy through enabling goods and services to be easily traded anywhere around the world.[53]

2.60 Ultimately, the emergence of this market place has resulted in the formation of a cyber crime industry where each cyber criminal may provide a discrete input in the process of targeting end users. For example, a spammer may charge a fee for disseminating an email that provides a

[52] Symantec Corporation, *Symantec Global Internet Security Report Trends for 2008,* Symantec Corporation, April 2009, p.10.

[53] See for example: Symantec Corporation, *Symantec Report on the Underground Economy July 07 – June 08*, Symantec Corporation, November 2009, pp.4-5; OECD, *Malicious Software (Malware): A Security Threat to the Internet Economy*, OECD, June 2008, p.16; AIC, *Submission 41*, p.7.

link to a phishing site, but may not be involved in running or profiting from the phishing website itself.[54]

The cyber crime industry and the evolution of cyber crime

2.61 The cyber crime industry has caused cyber crime more generally to evolve in a range of ways.

2.62 The large financial incentives provided by the underground cyber crime economy drive a development and testing process which leads to high quality malware that evades new anti-malware defences and avoids detection by Internet security companies thus increasing its profitability.[55]

2.63 Similarly, the market for malware has driven malware to become more user-friendly. Cyber criminals produce pre-packaged off-the-shelf style software packages (known as toolkits) which allow users to commit cyber crime acts (such as infiltrating a system with spyware or creating a botnet) with minimal technical knowledge.[56]

2.64 Figure 2.5 shows a screenshot from a popular toolkit called the 'Zeus Crimeware Toolkit' which enables entry-level cyber criminals to create their own botnets.[57]

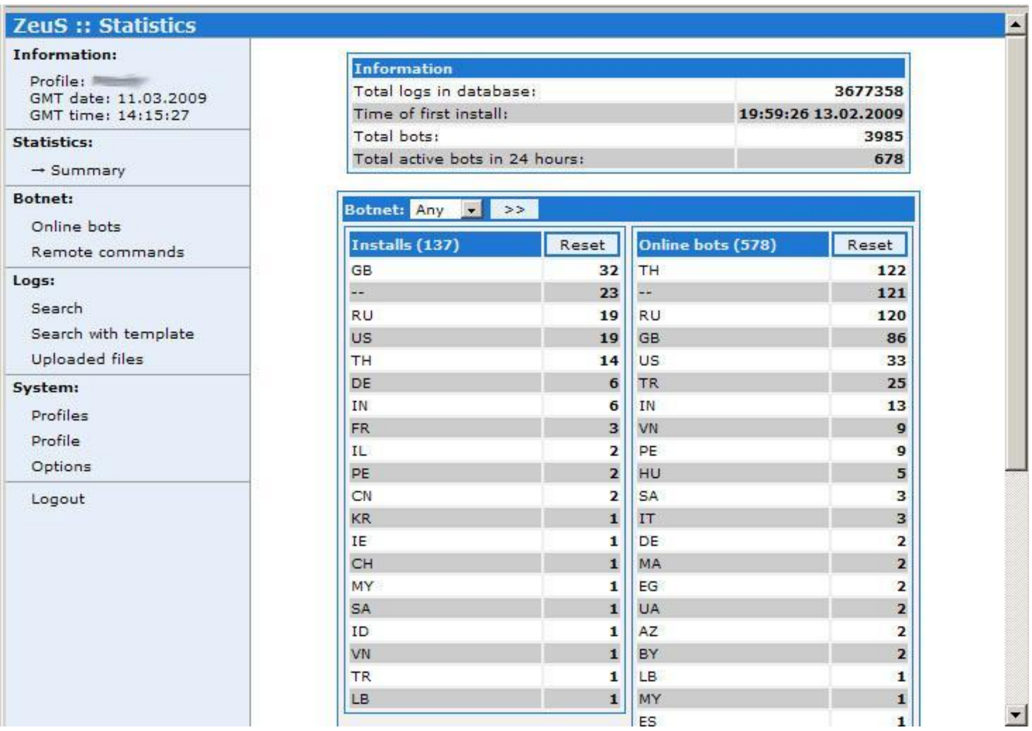
[54] See for example: Mr Craig Scroggie, Symantec Corporation, *Transcript of Evidence*, 9 October 2009, p.54; Dr Russell Smith, AIC, *Transcript of Evidence*, pp.6-9; AIC, *Submission 41*, p.9.

[55] See for example: Internet Safety Institute, *Submission 37*, p. 7; Mr David Zielezna, ACMA, *Transcript of Evidence*, 21 October 2009, p.5; Mr Peter Coroneos, IIA, *Transcript of Evidence*, 11 September 2009, p.14.

[56] Symantec Corporation, *Web Based Attacks February 2009*, Symantec Corporation, February 2009, p.10.

[57] P Coogan, Zeus, *King of the underground crimeware toolkits*, blog post, Symantec Security Blogs, Symantec Corporation, 25 August 2009, viewed 14 January 2009, <http://www.symantec.com/connect/blogs/zeus-king-underground-crimeware-toolkits>.

Figure 2.5 Screenshot of 'Zeus Crimeware Toolkit'



Profile:
GMT date: 11.03.2009
GMT time: 14:15:27

Information	
Total logs in database:	3677358
Time of first install:	19:59:26 13.02.2009
Total bots:	3985
Total active bots in 24 hours:	678

Installs (137)	
GB	32
--	23
RU	19
US	19
TH	14
DE	6
IN	6
FR	3
IL	2
PE	2
CN	2
KR	1
IE	1
CH	1
MY	1
SA	1
ID	1
VN	1
TR	1
LB	1

Online bots (578)	
TH	122
--	121
RU	120
GB	86
US	33
TR	25
IN	13
VN	9
PE	9
HU	5
SA	3
IT	3
DE	2
MA	2
EG	2
UA	2
AZ	2
BY	2
LB	1
MY	1
ES	1

Source P Coogan, *Zeus, King of the underground crimeware toolkits*, blog post, Symantec Security Blogs, Symantec Corporation, 25 August 2009, viewed 14 January 2009 ,<http://www.symantec.com/connect/blogs/zeus-king-underground-crimeware-toolkits>.

2.65 This toolkit enables unskilled cyber criminals to create their own tailored botnets through the use of an automated trojan to exploit computer vulnerabilities. As can be seen, the toolkit provides an up-to-date country-specific summary of the number of computers that are infected, the number of bot computers that are online and a 'remote commands' option through which the botnet can be directed. [58]

2.66 The lucrative cyber crime economy has also driven criminals to move from committing large indiscriminate cyber attacks to committing several smaller targeted and low level attacks in order to avoid detection by Internet security and law enforcement organisations.[59]

2.67 Finally, the underground cyber crime economy has led cyber criminals to increase the efficiency of the links between different areas of cyber crime

[58] P Coogan, Zeus, *King of the underground crimeware toolkits*, blog post, Symantec Security Blogs, Symantec Corporation, 25 August 2009, viewed 14 January 2009, <http://www.symantec.com/connect/blogs/zeus-king-underground-crimeware-toolkits>.

[59] See for example: OECD, *Malicious Software (Malware): A Security Threat to the Internet Economy*, OECD, June 2008, p.20; Mr Graham Ingram, AusCERT, *Transcript of Evidence*, 11 September 2009, p.3.

(such as the links between scam operators and money launderers) to the point where organised criminal networks have emerged.[60]

2.68 Below is a case study that provides an example of a cyber attack on German banks which incorporates all of the above mentioned aspects of the cyber crime industry.

Case study: German example of the operation of the cyber crime industry

> In August 2009, a group of coordinated cyber criminals first purchased a toolkit from an online cyber crime forum. This toolkit was then used to infect legitimate and fake websites with a trojan. When a user visited one of the infected websites the trojan would automatically install on the visiting computer. When this infected computer was used for online banking, the trojan would store the details. The trojan was then instructed to automatically log into the bank account and transfer money to a money mule's bank account for laundering. The trojan was automated to only transfer small amounts of money to avoid detection by banks' anti-fraud systems. This operation ran for two weeks and generated almost €1200 per day.

Source Finjan Malicious Code Research Centre, *Cybercrime intelligence report*, Issue 3, Finajn Malicious Code Research Centre, 2009.

Who commits cyber crime?

2.69 A variety of different people commit cyber crime including individual hackers, organised crime groups, corrupt company employees and foreign intelligence operatives.[61]

2.70 Witnesses suggested that, currently, perpetrators of cyber crime tend to be financially-motivated organised criminal networks with decentralised and flexible structures, and consisting of members from a variety of different countries. The majority of these attacks are said to originate from outside of Australia.[62]

2.71 Organised cyber criminal networks differ from traditional 'real world' organised crime groups in that there is not necessarily a hierarchical structure where all cyber attacks committed through the network are

[60] AFP, *Submission 25*, p.4.

[61] See for example: Mr Michael Sinkowitsch, Fujitsu Australia Ltd, *Transcript of Evidence*, 11 September 2009, p.47; Commander Neil Gaughan, AFP, *Transcript of Evidence*, 9 September 2009, p.11.

[62] See for example: Dr Russell Smith, AIC, *Transcript of Evidence*, p.9; AFP, *Submission 25*, p.3.

coordinated from the top. These criminal networks have a decentralised structure where members are anonymous and relatively independent. When a cyber criminal, or group of cyber criminals, wishes to commit a cyber attack, they may use the network to source the resources and skills for that particular operation.[63]

2.72 These cyber crime networks may consist of members from many different countries. The Committee heard that most cyber attacks appear to originate from America, China, Europe and Russia. It was also stated that organised criminal networks are appearing in South-East Asia. It was suggested that cyber criminals may find it easier to operate in countries were governmental institutions or the rule of law is not as strong, or where cyber crime makes a significant contribution to the growth of a developing economy.[64]

2.73 Cyber crime networks also target users from other countries in order to take advantage of traditional law enforcement boundaries that make it much harder for their crime to be investigated.[65]

Who are the victims of cyber crime?

2.74 All aspects of Australian society including Australian government, private businesses and home users, are victimised by cyber criminals.[66]

2.75 Australian governments, whether federal, state or territory, are potential targets of cyber attacks. Cyber attacks may target governments for a variety of reasons including to conduct protests or for cyber espionage. However Governments are also increasingly being targeted by financially motivated cyber criminals.[67] Government agencies are increasingly using the Internet to provide information to, and exchange information with, the public. This makes government organisations a target for financially-

[63] AFP, *Submission 25*, p.3.

[64] See for example: Mr Craig Scroggie, Symantec Corporation, *Transcript of Evidence*, 9 October 2009, p.61; Commander Neil Gaughan, AFP, *Transcript of Evidence*, 9 September 2009, p.7; Dr Russell Smith, AIC, *Transcript of Evidence*, 19 August 2009; Mr Richard Johnson, Westpac Banking Corporation, *Transcript of Evidence*, 8 October 2009, p.56.

[65] See for example: OECD, *Malicious Software (Malware): A Security Threat to the Internet Economy*, OECD, June 2008, p.20; Mr Graham Ingram, AusCERT, *Transcript of Evidence*, 11 September 2009, p.20.

[66] See for example: AusCERT, *Submission 30*, p.4; AGD, *Submission 44*, p.3.

[67] See for example: Australian Taxation Office (ATO), *Submission 59*, p.4; Australian Seniors Computers Clubs Association (ASSCA), *Submission 63*, p.5; Mr Michael Cranston, ATO, *Transcript of Evidence*, 16 September 2009, p.2; Lockstep, *Submission 36*, p.10; AusCERT, *Submission 30*, p.9.

motivated cyber attacks aimed at illegally obtaining funds or information, illustrated in the case study below.[68]

Case study: Fake Australian Taxation Office phishing website hosted in Ukraine

> The ATO reported that recently a number of Australian tax payers had been lured to a fake website hosted in Ukraine. The website, a mirror image of the ATO's legitimate website, asked visitors to enter a range of personal details in order to receive a tax refund of $9500. ATO submitted that this website was aimed at harvesting passwords and credit card numbers.

Source Australian Taxation Office, *Submission 58*, p.5.

2.76 Similarly, Australian businesses, whether small, medium or large organisations, are potential targets of cyber crime. Australian businesses may be the target of a variety of attacks including online fraud, theft of information and extortion.[69]

2.77 Home users are also vulnerable to cyber attacks due to low levels of online security. Cyber criminals seek information and money from home users through the use of scams, phishing schemes and malware. Due to their low level of security, home computers are highly vulnerable to being recruited to botnets.[70] Additionally, home users that fall victim to an online scam are more likely to be targeted by further scams. Cyber criminals note users who have responded to scams and place them on a 'sucker list' which may then be used to distribute further scams to these vulnerable home users.[71]

2.78 As the Internet is a resource shared among several different sectors of society, attacks on one section of Australian society may have flow on

[68] See for example: ATO, *Submission 59*, p.4; ASSCA, *Submission 63*, p.5; Mr Michael Cranston, ATO, *Transcript of Evidence*, 16 September 2009, p.2; Lockstep, *Submission 36*, p.10; AusCERT, *Submission 30*, p.9.

[69] See for example: Mr Christopher Hamilton, *Transcript of Evidence*, p.71; Mr Craig Scroggie, Symantec Corporation, *Transcript of Evidence*, 9 October 2009, p. 52; Symantec Corporation, *Submission 32*, p.9; KR Choo, *Trends and issues in crime and criminal justice: Zombies and Botnets*, AIC, Canberra, 2007, p.4; ABC, *Fear in the Fast Lane*, Four Corners program transcript, ABC, 17 August 2009, viewed 11 January 2010, <http://www.abc.net.au/4corners/content/2009/s2658405.htm>.

[70] AFP, *Submission 25*, p.5; Dr Russell Smith, AIC, *Transcript of Evidence*, 19 August 2009, p.13; ACCC, *Submission 46*, p.4; Mrs Nancy Bosler, ASSCA, *Transcript of Evidence*, p.1; Dr Russell Smith, AIC, *Transcript of Evidence*, 19 August 2009, p.14.

[71] Dr Russell Smith, AIC, *Transcript of Evidence*, 19 August 2009, p.14.

effects for other areas of society.[72] For example, due to the vulnerability of home users, botnets are often comprised predominantly of home computers. These botnets can then be used to launch attacks against businesses and governments.[73]

Prevalence of Cyber Crime

2.79 Witnesses emphasised that while the majority of Internet activity is legitimate, cyber crime has touched a significant number of Australians and is growing.[74]

2.80 This section examines the current level of cyber crime both globally and in Australia, and the current trends of cyber crime.

2.81 There is a wide variety of often incomparable information on cyber crime, all of which inevitably suffers from some degree of inaccuracy. However, despite these variations and inaccuracies, all information supports the same conclusion: cyber crime is highly prevalent and is growing at an increasing rate.[75]

Current level of cyber crime threat

2.82 Tables 2.2 and 2.3 below summarise the statistics made available to the Committee, including global statistics and statistics that focus solely on Australia.

[72] Mr Anthony Burke, Australian Bankers Association NSW Inc, *Transcript of Evidence*, 8 October 2009, p.62.

[73] AFP, *Submission 25*, p.5.

[74] See for example: Commander Neil Gaughan, AFP, *Transcript of Evidence*, 9 September 2009, p.2; Dr Russell Smith, AIC, *Transcript of Evidence*, 19 August 2009, p.16.

[75] Mr Alistair MacGibbon, Internet Safety Institute, *Transcript of Evidence*, 11 September 2009, p.63; ACMA, *Submission 56*, p.4.

Table 2.2 Global statistics illustrating the high incidence of cyber crime

Global statistics

Hacking

- In 2008, Verizon observed the compromise of over 180 million business records due to hacking.

Malware

- Symantec has detected a total of approximately 2.6 million different malware programs, 60 per cent of which were detected in 2008.

Malware infections via legitimate websites

- A 2007 study of 4.5 million web pages by Google found that one out of every ten websites contains malware.

Botnets

- McAfee estimates that nearly 40 million computers were recruited to botnets in the first three quarters of 2009.
- The Internet Society of Australia submitted that estimates of the number of bot computers range from five percent of all computers connected to the Internet (over 20 million) to twenty five per cent of all computers connected to the Internet (over 250 million).

DDoS attacks

- Telstra submitted that the size of the largest DDoS attacks increased a hundredfold between 2001 and 2007, from 0.4 gigabits per second to 40 gigabits per second.

Cyber crime industry

- Verizon reports that 91 per cent of the data breaches it observed in 2008 were linked to organised criminal networks.

Phishing and spam

- In the year 2008, Symantec observed 349.6 billion spam messages across the Internet.
- Symantec claim that in 2008 approximately 90 per cent of spam was sent via botnets.
- The Anti-Phishing Working Group, an international consortium of organisations against phishing, identified over 210 thousand unique phishing websites in the first half of 2009.

Source Verizon Business, *2009 Data Breach Investigations Report, Verizon Busines*s, 2009, p.2; Australian Communication and Media Authority, *Submission 56*, pp.4,7; Symantec Corporation, *Symantec Global Internet Security Threat Report: Trends for 2008*, Symantec Corporation, April 2009, pp.10,16,90 ; McAfee Inc, *McAfee Threats Report Third Quarter 2009*, McAfee Inc, 2009, p.3; Internet Society of Australia, *Submission 45*, pp.3-4; Telstra, *Submission 43.1*, p.2; Anti-Phishing Working Group, *Phishing Activity Trends Report: 1st Half 2009*, APWG, 2009, p.3; BBC News, *Google searches web's darkside,* online news article, 11 may 2007, viewed 19 January 2009, <http://news.bbc.co.uk/2/hi/technology/6645895.stm>.

Table 2.3 Australian statistics illustrating the incidence of cyber crime

Australian statistics

Malware

- A 2008 AusCERT survey of 1,001 Australian adults reported that 23 per cent of respondents had confirmed malware infections on their home computers.
- A September 2009 ACCAN survey of 141 Australian home users indicated that one in five respondents had been a victim of cyber crime.

Botnets

- On average over the 2008-09 financial year, ACMA received 4,291 reports per day of Australian computers infected with botnet malware.
- ACMA submitted that the number of Australian computers recruited to botnets in June 2009 may have been considerably greater than 10,000 computers per day.

Scams

- The ACCC received 12,000 online scam complaints in the 2007-08 financial year.
- Eighty-six per cent of respondents to a 2009 online survey by the Australian Consumer Fraud Taskforce claimed to have been invited to participate in a scam, 73 per cent of whom were targeted via email.

Businesses targeted

- The Australian Institute of Criminology report that fourteen per cent of Australian businesses experienced one or more computer security incidents in the 2006-07 financial year.

Online credit card and bank card fraud

- The 2007 Personal Fraud Survey by the Australian Bureau of Statistics (ABS) inferred that, in the twelve months prior to the survey, 76,000 Australians were the victim of online credit card or bank card fraud.
- The Australian Payments Clearing Association report that in the 2007-08 financial year the Australian payments industry, including banks and credit unions, lost $63.5 million due to online credit card and bank card fraud.

Phishing and spam

- The 2007 Personal Fraud Survey by the ABS estimated that, in the twelve months prior to the survey, 30,400 Australians were the victim of online phishing scams.
- The Commonwealth Bank of Australia receives 3,000 spam and phishing related reports per day, with the highest reporting period being May last year when 30,000 reports were being received per day.

Source Australian Communication and Media Authority, *Submission 56*, pp.4,7; Australian Competition and Consumer Commission, *Submission 46*, p.3; Internet Society of Australia, Submission 45, pp.3-4; K Richards, *The Australian Business Assessment of Computer User Security: a national survey*, Australian Institute of Criminology, 2009, p.xi; Australian Bureau of Statistics, *2007 Personal Fraud Survey*, ABS, Cat. No. 4528.0, 2007, pp.14, 21; Australian Payments Clearing Association, *Submission 50*, p.5; Mr John Geurts, Commonwealth Bank of Australia, *Transcript of Evidence*, 8 October 2009, p.59; J Dearden, *Comparing the 2008 and 2009 ACFT online survey results*, powerpoint presentation at Australian Consumer Fraud Taskforce Forum 2009, 8 October 2009, p.8; AusCERT, *AusCERT Home Users Computer Security Survey 2008,* AusCERT, 2008, p.3.

2.83 These statistics, whilst varying and sometimes imprecise, provide a number of insights into the current level of cyber crime:

- globally, malware and botnets are widespread and facilitate significant DDoS attacks, data breaches and phishing schemes;
- globally, it is very common for trusted and legitimate websites to be inadvertently hosting and propagating malware;
- a significant number of Australian computers are infected with malware and are part of botnets; and
- a significant number of Australian businesses and home users are the target of online scams, phishing schemes and identity fraud.

2.84 It can be seen that cyber crime is highly prevalent and directly affects a significant number of Australians.[76]

2.85 In 2006 and 2008 the Department of Broadband, Communications and the Digital Economy (DBCDE) commissioned KPMG to carry out cyber security threat and vulnerability assessments for home users and small businesses.[77] These reports are not publicly available. However ACMA informed the Committee that there are potentially tens of thousands of compromised Australian computers.[78]

2.86 These concerns were reiterated to the Committee by Mr Mike Rothery, the First Assistant Secretary, National Security Resilience Policy Division, Attorney General's Department (AGD):

> We are concerned that there are many thousands of compromised machines out there … in many cases … being used as part of botnets to do other things—launch spam attacks, denial of service, phishing attacks and a whole range of things, … many tens of thousands. [79]

The outlook for cyber crime in Australia

2.87 Throughout the inquiry witnesses continually reinforced to the Committee that cyber crime is a rapidly evolving phenomenon. The Committee heard that the cyber crime industry, driven by the lucrative underground cyber

[76] Mr Peter Coroneos, IIA, *Transcript of Evidence*, 11 September 2009, p.15.

[77] DBCDE, *Submission 34.1*, p.7.

[78] ACMA, *Submission 56*, p.4.

[79] Mr Mike Rothery, AGD, *Transcript of Evidence*, 25 November 2009, p.10.

> crime economy, will continue to adapt in order to exploit new technologies and in order to respond to new anti-cyber crime measures.[80]

2.88 Mr Graham Ingram, General Manager of the Australian Computer Emergency Response Team (AusCERT), summarised the outlook for cyber crime in Australia:

> [Cyber crime in Australia] is getting out of control and we are losing. And I think that, with the pressures coming on us over the next few years, if nothing is done to change the current direction we will lose faster.[81]

2.89 The future of cyber crime in Australia can be predicted by observing a range of trends in Internet and technology use, malware and cyber attacks.

2.90 During the inquiry a range of trends in Internet and technology usage were viewed as increasing the prevalence of cyber crime. For example, witnesses argued that the increased uptake of high speed 'always on' broadband services will increase the threat of cyber crime in Australia (a 2009 ABS survey estimated that Australian household broadband connections grew 18 per cent to 5 million during 2008-09).[82] Similarly, the Committee heard that the uptake of new computer systems, software and hardware (such as cloud computing, social networking and wireless systems) will lead to new vulnerabilities.[83] An additional concern was that as technologies become more user-friendly, computer users will require less computer knowledge and will therefore be more vulnerable to cyber crime.[84]

[80] See for example: Commander Neil Gaughan, AFP, *Transcript of Evidence*, 9 September 2009 p.3; Mr Graham Ingham, AusCERT, *Transcript of Evidence*, 11 September 2009, p.11; Mr Peter Coroneos, IIA, *Transcript of Evidence*, 11 September 2009, p.14; Mr Richard Johnson, Westpac Banking Corporation, *Transcript of Evidence*, 8 October 2009, p.56; Mr Michael Sinkowitsch, Fujitsu Australia Ltd, *Transcript of Evidence*, 11 September 2009, p.47.

[81] Mr Graham Ingham, AusCERT, *Transcript of Evidence*, 11 September 2009, p.3.

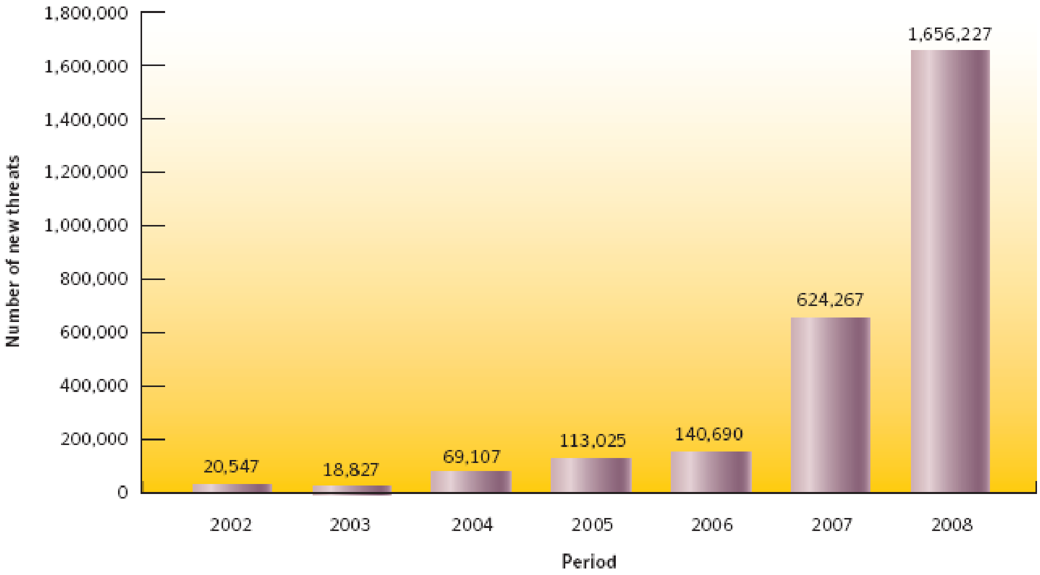
[82] See for example: Mr Graham Ingram, AusCERT, *Transcript of Evidence*, 11 September 2009, p.3; Mr Peter Coroneos, IIA, *Transcript of Evidence,* 11 September 2009, p.22; Internet Safety Institute, *Submission 37*, p.4; Mr Anthony Burke, Australian Bankers Association NWS Inc., *Transcript of Evidence*, 8 October 2009, p.55; Mr Terry Hilsberg, ROAR Film Pty Ltd, *Transcript of Evidence*, 8 October 2009, p.66; Mr John Galligan, Microsoft Pty Ltd, *Transcript of Evidence*, 9 October 2009, Mr Craig Scroggie, Symantec Corporation, *Transcript of Evidence*, 9 October 2009, p.15; ABS, *Household Use of Information Technology 2008-09*, ABS, Cat. No. 8146.0, 16 December 2009, p.37.

[83] Mr Graham Ingham, AusCERT, *Transcript of Evidence*, 11 September 2009, p.3; ATO, *Submission 59*, p.6; ROAR Film Pty Ltd, *Submission 64*, p.5; Dr Russell Smith, AIC, *Transcript of Evidence*, 19 August 2009, p.5; McAfee Australia, *Submission 10*, p.2.

[84] Microsoft Australia, *Submission 35*, p.4.

2.91 Trends in malware were also identified as an area of concern. For example, Symantec reported that malware is being produced at an ever increasing rate (refer to Figure 2.6), with detected malware levels jumping 60 per cent in 2008.[85] Additionally it was argued that cyber criminals are increasingly propagating malware via popular and trusted websites[86], and that this malware is increasingly surreptitious, specialised and targeted.[87] The Committee also heard that botnets continue to grow (refer to Figure 2.7) and are likely to become more versatile in exploiting new vulnerabilities and in responding to anti-botnet measures.[88]

Figure 2.6 Number of new malware programs detected globally per year, 2002 to 2008



Source Symantec Corporation, *Symantec Global Internet Security Threat Report: Trends for 2008*, Symantec Corporation, April 2009, p.10.

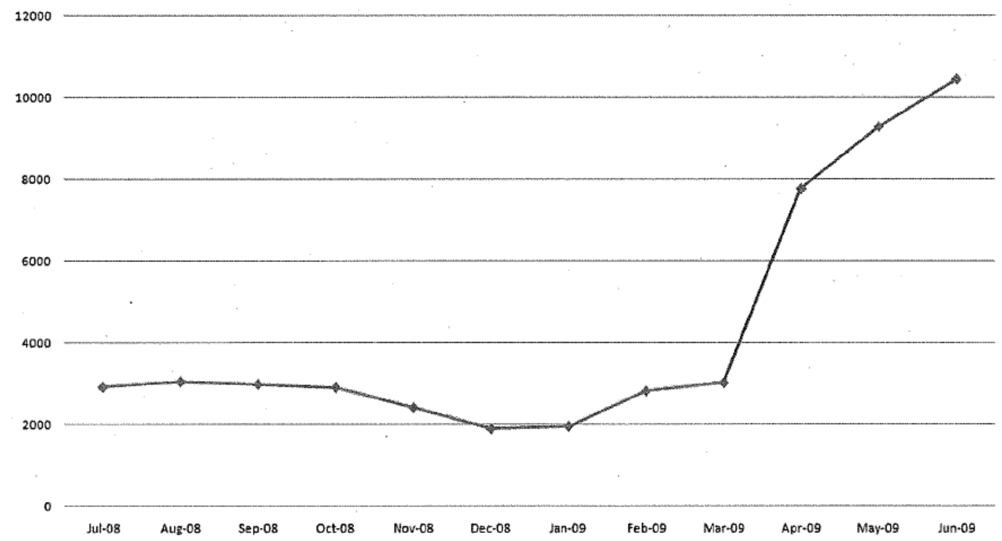
[85] Symantec Corporation, *Symantec Global Internet Security Threat Report: Trends for 2008*, Symantec Corporation, April 2009, p.10.

[86] See for example: Mr Graham Ingram, AusCERT, *Transcript of Evidence*, 11 September 2009, p.7; Mr Bruce Matthews, ACMA, *Transcript of Evidence*, p.5.

[87] Telstra, *Submission 43*, p.2.

[88] The ICANN, *Submission 40*, p.1.

Figure 2.7 Average number of IP addresses that are part of botnets reported to ISPs via ACMA's Australian Internet Security Initiative per day July 2008 to 2009



Note: AISI figures do not accurately identify how many Australian computers are compromised due to multiple computers that operate under the same IP address and due to computers that may be missed or not identified during the reporting process. ACMA submits however that the number of Australian computers compromised is likely to be considerably greater than shown in AISI reports.

Source Australian Communication and Media Authority, *Submission 56*, p.5.

2.92 Other acts of cyber crime were also said to be increasing. Submitters stated that organised cyber criminals are committing increasingly low profile attacks against identified vulnerable users including small businesses, home users and prior scam victims.[89] Also, it was argued that as the cyber crime industry supplies increasingly user-friendly malware and skilled hackers-for-hire, the skills needed to carry out complex cyber attacks will gradually decrease.[90] The Committee also heard that cyber criminals are increasingly targeting victims in other countries in order to reduce their risk by taking advantage of jurisdictional barriers to law enforcement investigations.[91]

2.93 Mr Alistair MacGibbon, Director, Internet Safety Institute, told the Committee that cyber criminals have, and continue to compile, large stockpiles of stolen information but are not efficient at converting this stolen information into money. Mr MacGibbon stated that his main fear is

[89] See for example: AIC, *Submission 41*, pp.2-3; AFP, *Submission 25,* p.3; Dr Russell Smith, AIC, *Transcript of Evidence*, 19 August 2009, p.13; Mr Craig Scroggie, Symantec Corporation, *Transcript of Evidence*, 9 October 2009, p.52; DBCDE, *Submission 34*, p.3.

[90] See for example: OECD, *Malicious Software (Malware): A Security Threat to the Internet Economy*, OECD, June 2008, p.30; ACS, *Submission 38*, p.6.

[91] OECD, *Malicious Software (Malware): A Security Threat to the Internet Economy*, OECD, June 2008, p.30.

that cyber criminals will improve their techniques for monetising this information thus leading to a new wave of cyber attacks.[92]

Economic impact of cyber crime

2.94 Cyber crime has many current and potential negative economic impacts on Australians. Contributors to the inquiry outlined a range of ways in which cyber crime threatens the Australian economy:

- widespread cyber crime may undermine confidence in aspects of the digital economy thus inhibiting the growth of the Australian economy;
- continued cyber attacks against particular businesses may damage their reputation and result in a loss of customers and revenue;
- the development of measures to combat and respond to cyber attacks imposes a significant cost on businesses;
- cyber attacks cause direct financial losses to consumers and businesses resulting from the theft of information and money, or extortion; and
- cyber attacks targeting Australia's critical infrastructure may lead to immediate and long term economic losses.

2.95 These impacts are described below.

Economic loss from diminished confidence in Australia's digital economy

2.96 Australia's economy is currently benefiting from the increased development and use of new information and communication technologies. This area of our economy is referred to as the 'digital economy'. DBCDE define the digital economy as:

> The global network of economic and social activities that are enabled by information and communications technologies, such as the Internet, mobile and sensor networks.[93]

2.97 The digital economy consists of devices such as computers and phones as well as the infrastructure that enables the sharing of information such as telephone lines and mobile phone towers. The digital economy enables all aspects of Australian society to carry out a range of activities with increased ease and efficiency such as accessing government information,

[92] Mr Alastair MacGibbon, Internet Safety Institute, *Transcript of Evidence*, 11 September 2009, p.69.

[93] DBCDE, *Australia's Digital Economy: Future Directions*, DBCDE, 2009, p.2.

conducting financial transactions or communicating in real time with geographically distant friends or family.[94]

2.98 Ultimately, the digital economy opens up new opportunities for the Australian economy as a whole to increase its efficiency and to grow.[95]

2.99 Many contributors to the inquiry warned of the significant negative economic impact which would be caused by cyber crime undermining confidence in Australia's digital economy.[96] Ms Loretta Johnson, General Manager, Policy and Government Relations, Australian Information Industry Association (AIIA), provided a summary of this concern:

> The productivity, efficiency and economic growth advantages that can be delivered by our rapidly developing digital infrastructure are recognised by governments and users alike. The secure and safe use of that infrastructure should be a focus for governments which are concerned with enhancing their nation's GDP for the benefit of their own citizens. If that focus is lost, users will lose confidence in the internet as a business and commercial tool, leading to a consequent decrease in the efficiencies and productivities that digital engagement can deliver.[97]

2.100 It is difficult to quantify the negative economic impact caused by a loss of confidence in online services.[98] However, Mr Paul Kurtz, Executive Director of the US-based Cyber Security Industry Alliance, has suggested that a loss of consumer confidence in the digital environment is a billion dollar problem.[99]

2.101 ACMA's 2009 publication *Australia in the Digital Economy: Trust and Confidence* concluded that, while Australians are aware and concerned about the risks of using the Internet, these concerns do not currently stop

[94] DBCDE, *Australia's Digital Economy: Future Directions*, DBCDE, 2009, pp.2-3.

[95] DBCDE, *Australia's Digital Economy: Future Directions*, DBCDE, 2009, p.1.

[96] See for example: AusCERT, *Submission 30*, p.11; IIA, *Submission 54*, p.4; Microsoft Australia, *Submission 35*, p.5; Symantec Corporation, *Submission 32*, p.8; Mr Graham Ingram, AusCERT, *Transcript of Evidence*, 11 September 2009, p.10; Lockstep Technologies Pty Ltd, *Submission 36*, p.10; OECD, *Malicious Software (Malware): A Security Threat to the Internet Economy*, OECD, June 2008, pp.41-42.

[97] Ms Loretta Johnson, Australian Information Industry Association, *Transcript of Evidence*, 11 September 2009, p.24.

[98] OECD, *Malicious Software (Malware): A Security Threat to the Internet Economy*, OECD, June 2008, p.7.

[99] Cyber Security Industry Alliance, 'Survey: Lack of confidence in cyber security has economic, political effects', *Insurance Journal*, Wells Publishing, June 2006, viewed 29 January 2009, <http://www.insurancejournal.com/news/national/2006/06/07/69215.htm>.

people from using the Internet.[100] However, the 2008-09 ABS *Household Use of Technology Survey* estimated that over one million Australians refrain from purchasing goods or services on line due to concerns over online security or privacy.[101] Similarly, the Australian Communications Consumers Action Network (ACCAN) informed the Committee that they have encountered a large number of consumers who are refusing to use the Internet because of fears they will lose money to cyber crime.[102]

Financial loss to business from damaged reputation

2.102 Where a business is the target of persistent or high-profile cyber attacks, their reputation among clients and share holders may suffer, thus resulting in lower share prices, fewer clients and lower revenues.[103] For example, in January 2009, US-based payment processor Heartland Payment Systems experienced significant divestment which halved its stock price following a malware-enabled data breach which potentially compromised tens of millions of credit and debit card transactions.[104]

Cost of anti-cyber crime measures and cyber crime complaints

2.103 Many private businesses that supply ICT goods and services, or conduct business over the Internet, must direct significant resources towards dealing with cyber crime.[105] A 2009 AIC survey estimated that the annual cost of computer security measures for Australian businesses is between $1.37 billion and AU$1.95 billion.[106]

Direct financial losses to Australian businesses and home users

2.104 Australian businesses and home users continually suffer direct financial losses from cyber crime. Cyber criminals use scams, fraud and extortion to illegally obtain money from these victims. The loss to home users and business is difficult to quantify; however, the AIC estimate Australian

[100] ACMA, *Australia in the Digital Economy: Trust and Confidence*, ACMA, March 2009, p.1.

[101] ABS, *Household Use of Information Technology 2008-09*, ABS, Cat. No. 8146.0, 16 December 2009, p.30.

[102] Mr Allan Asher, ACCAN, *Transcript of Evidence*, 8 October 2009, p.16.

[103] OECD, *Malicious Software (Malware): A Security Threat to the Internet Economy*, OECD, June 2008, pp.40-41.

[104] AM Freed, *Another Payment Card Processor Hacked*, Information Security Resources, Infosec Island Network, February 14 2009, viewed 29 January 2009, <http://information-security-resources.com/2009/02/14/another-payment-card-processor-hacked/>.

[105] OECD, *Malicious Software (Malware): A Security Threat to the Internet Economy*, OECD, June 2008, pp.40-41.

[106] K Richards, *The Australian Business Assessment of Computer User Security: a national survey*, AIC, 2009, p.iii.

businesses lost between $595 million and $649 million in the 2006-07 financial year.[107]

Economic loss from disruption to Australia's critical infrastructure

2.105 Australia's national information infrastructure supports a range of computerised control mechanisms that govern other aspects Australia's critical infrastructure. Contributors argued that there is real potential for cyber criminals to highjack, damage or inhibit these systems which in turn could cause longer-term disruptions to economic development.[108]

Committee View

2.106 Cyber crime crosses many technological, conceptual and institutional boundaries, and, through its high prevalence, has real and increasing impacts on many Australians. Australia's public policy response must take account of several key factors:

- organised criminal networks consist of members from, and commit attacks across, several different traditional law enforcement and regulatory jurisdictions thus challenging traditional law enforcement and regulatory methods and procedures;
- cyber crime is rapidly evolving and responsive to anti-cyber crime measures, thus any legislative, regulatory, technological, intelligence and educational initiatives must be kept under constant review;
- the interrelated nature of different aspects of cyber crime makes it important to take a strategic and holistic approach to intervention; and
- the complex nature of cyber crime makes the reporting, gathering and analysis of data and intelligence an important element of the national and international effort to combat cyber crime.

2.107 While it is probably impossible to eradicate all cyber crime (just as it is in the offline environment) it is possible to ensure that Australia maintains an understanding of the threats and builds capacity to prevent cyber attacks. It is clear to the Committee that the many different aspects of

[107] See for example: OECD, *Malicious Software (Malware): A Security Threat to the Internet Economy*, OECD, June 2008, p.38; K Richards, *The Australian Business Assessment of Computer User Security: a national survey*, AIC, 2009, p.xi

[108] See for example: AIC, *Submission 41*, p.16; Australian Information Industry Association, *Submission 22*, p.9; OECD, *Malicious Software (Malware): A Security Threat to the Internet Economy*, OECD, June 2008, pp.42-43.

cyber crime are interrelated and Australia’s response cannot deal with these various aspects of cyber crime in complete isolation.

2.108 The following chapters canvass some of the options for expanding the current national strategy and building a broader, and more integrated response that takes account of the needs of consumers.