SUBMISSION NO. 56

Australian Government

acma

Australian
Communications
and Media Authority

ACMA submission to the House of Representatives Inquiry into Cyber Crime

AUGUST 2009

communicating | facilitating | regulating

Canberra
Purple Building
Benjamin Offices
Chan Street
Belconnen ACT

PO Box 78
Belconnen ACT 2616

T +61 2 6219 5555
F +61 2 6219 5353

Melbourne
Level 44
Melbourne Central Tower
360 Elizabeth Street
Melbourne VIC

PO Box 13112
Law Courts
Melbourne VIC 8010

T +61 3 9963 6800
F +61 3 9963 6899

Sydney
Level 15 Tower 1
Darling Park
201 Sussex Street
Sydney NSW

PO Box Q500
Queen Victoria Building
NSW 1230

T +61 2 9334 7700
1800 226 667
F +61 2 9334 7799

© Commonwealth of Australia 2009

This work is copyright. Apart from any use as permitted under the Copyright Act 1968, no part may be reproduced by any process without prior written permission from the Commonwealth. Requests and inquiries concerning reproduction and rights should be addressed to the Manager, Communications and Publishing, Australian Communications and Media Authority, PO Box 13112 Law Courts, Melbourne Vic 8010.

Published by the Australian Communications and Media Authority

Contents

ACMA Submission to the House of Representatives Inquiry into Cyber Crime

The Australian Communications and Media Authority (ACMA) welcomes the opportunity to provide a submission to the House of Representatives Inquiry into Cyber Crime (the Cyber Crime Inquiry). While many Australian government agencies have an important role to play in enhancing and maintaining the e-security of the online operating environment, the ACMA considers itself a key player in addressing emerging e-security issues.

The focus of the ACMA submission is primarily on the prevalence of 'compromised' computers on the Australian internet, with some general commentary on the potential implications of the number of these infections. As the ACMA's anti-botnet initiative—the Australian Internet Security Initiative (AISI)—provides the context for the ACMA's involvement in and knowledge of bot activities in Australia, some background on the AISI is provided below.

The AISI

The ACMA developed the AISI to help address the problem of compromised computers (sometimes referred to as 'zombies', 'bots' or 'drones')—computers that have become compromised through the surreptitious installation of malicious software (malware) that enables them be controlled remotely for illegal and harmful activities, without the knowledge of the computer owner. A trial of the AISI commenced in November 2005, and it has been progressively expanded since that time.

Through the AISI, the ACMA collects data from various sources identifying IP addresses[1] that have been detected as exhibiting 'bot' behaviour on the Australian internet. Using this data, the ACMA provides daily reports to participating internet service providers (ISPs) identifying IP addresses on their networks that have been reported as compromised (infected with malware) in the previous 24-hour period. The currency of the data is an important part of the initiative, as it is based on evidence of a recent infection that is highly likely to be still occurring when a customer is contacted.

The AISI reports include information on the IP address, timestamp and type of compromise identified. The IP address and timestamp enable ISPs to identify the customer associated with the compromise at a given point in time. Additional information is provided for some compromise types, such as the url associated with the 'malware serving host' compromise type.

When they receive AISI reports, ISPs are expected to contact their customers to advise them that their computer(s) appears to be compromised, and to provide them with information to assist them in addressing the problem. Many ISPs currently participating in the AISI have informed the ACMA that when contacted, their customers are often unaware their computer has been compromised and are grateful that their ISP has informed them of the problem.

Sixty-eight ISPs are currently participating in the AISI (the list of current ISP participants is provided at Attachment A). It is estimated that over 90 per cent of Australian residential customers of internet services are covered by these ISPs.

The AISI grew out of the ACMA's anti-spam activities associated with its enforcement and administration of the *Spam Act 2003*. As spam is a primary vector leading to compromises on computers, the ACMA saw the need to address spam at its source. The ACMA has vigorously enforced the Spam Act and is recognised as a world leader in combating spam. The work has involved a combination of approaches. These include close international cooperation, technical approaches including the SpamMATTERS spam reporting tool, encouragement of industry self-regulatory initiatives such as the Internet Industry Association's *Spam Code of Practice* and the promotion of anti-spam education and awareness activities. These approaches also have application in combating cyber crime and are elaborated further in this submission. Further general information on the AISI is available at http://www.acma.gov.au/WEB/STANDARD/pc=PC_310317 .

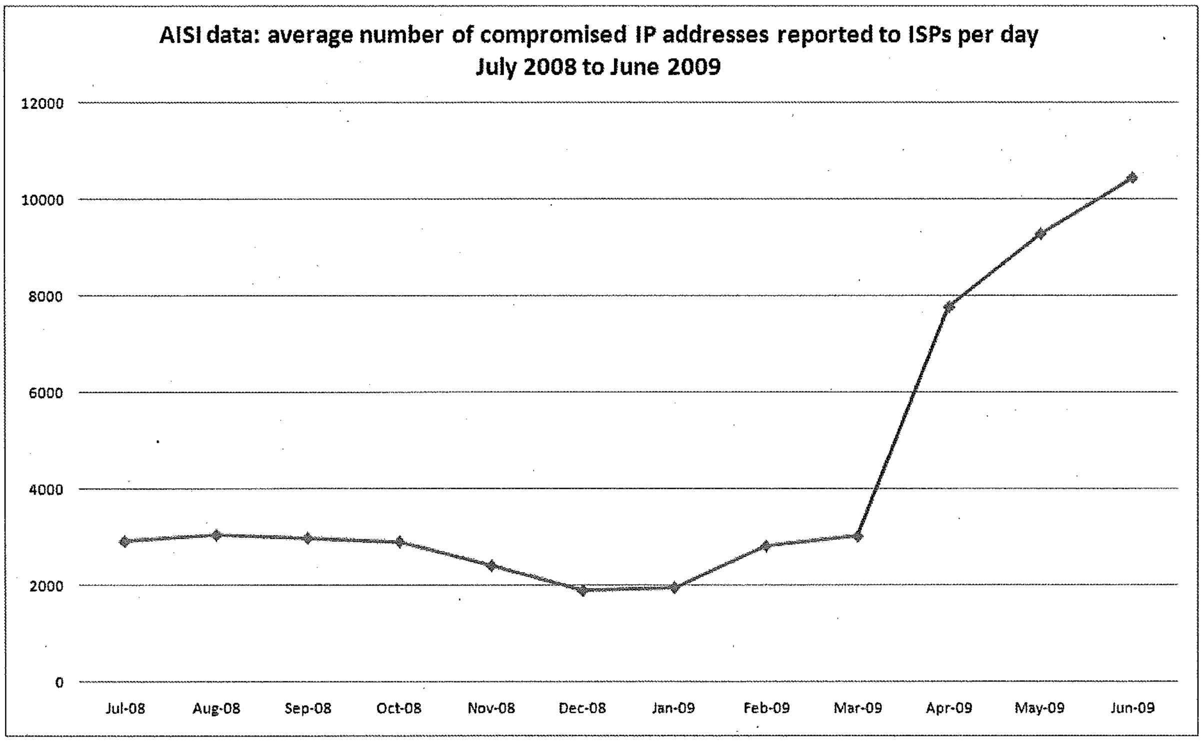
[1] **Note about the correlation between IP addresses and computers connected to the internet.** In many cases there will only be one computer associated with a given IP address, most typically in the case of a residential customer of an ISP with a single computer connected to the internet. However, most businesses (and increasingly residential internet users) will have multiple computers connected to the internet through a single IP address. This may occur through use of a proxy server or more commonly through routers performing Network Address Translation (NAT). Consequently, the number of internet users connecting to the internet through an IP address can vary from one to many thousands. For example, over 600 ACMA users connect to the internet through one IP address. However, a single computer may also utilise more than one IP address in a 24-hour period—for example, where an ISP provides a customer with a dynamic IP address and that customer disconnects and reconnects their internet connection with an ISP within the 24-hour period, that customer may receive a new IP address when they reconnect. A more detailed discussion of this issue is provided later in this paper.

The number of compromised computers in Australia

An important focus of the Cyber Crime Inquiry is on the nature and prevalence of e-security risks to Australian consumers and the impact—including the potential impact—of malware on cyber crime. While the ACMA does not have any independent data on levels of cyber crime in Australia, it does have data through its AISI activities that indicates the potential population of Australian computers[2] that could either perpetrate cyber crime or be subject to cyber crime through being compromised by 'bot' malware.

As identified in Chart 1, the number of individual compromised IP addresses reported daily by ACMA to ISPs in June 2009 was over 10,000 per day, indicating that potentially in the order of 10,000 Australian computers per day were infected with 'bot' malware. The data in this chart, however, needs to be interpreted with caution. As elaborated below, there are factors that indicate the number of compromised computers associated with these daily reports could be greater or lower than this figure. As also discussed below, the AISI data does not identify all active compromised computers on the internet during a given 24-hour period.

Chart 1.



The ACMA is unable to accurately identify how many Australian computers may be compromised at a given point in time, as it is not known how many computers are missed or not identified by the various sources of compromise data that feed into the AISI. It is also not known how many computers are connecting to the internet through a given IP address, and where multiple computers connect to the internet through an IP address, how many of these individual computers are compromised. As discussed below, however, there are indications that the number of compromised computers in Australia may be considerably greater than the number of IP addresses identified in the ACMA's AISI reports.

[2] That is, using compromised IP address data as a proxy for identifying the number of infected computers.

While there has been a steady increase in the number of compromises reported daily through the AISI since its inception and a marked increase in compromises since March 2009, this does not necessarily mean that the rate of compromises on the Australian internet on a per user basis is increasing. This is because the AISI compromise data is volatile, with the constituent data elements of the AISI constantly changing and evolving, as described below.

The key factors that have influenced the increase in the number of daily AISI compromises reported include:

> a steady increase in the number of ISPs participating in the AISI, leading to a greater coverage of Australian IP address ranges and hence Australian internet users—by way of comparison, on 1 July 2008, 37 ISPs were participating in the AISI, compared with 64 at 30 June 2009;

> the continuing expansion of IP address ranges by ISPs to provide for customer growth, resulting in an increasing coverage of Australian IP address ranges by the AISI and consequently a greater population of potential compromises. Over the last 12-months the ACMA has also actively sought from ISPs more comprehensive IP address range information than previously provided, leading to a significant expansion of IP address range coverage of the Australian internet by the AISI; and

> an increase in the number of sources of compromise data feeding into the AISI, combined with some individual sources significantly improving their compromise data gathering capabilities. This has led to the AISI progressively identifying more malware types and infected computers on the Australian internet.

There are other factors, however, that indicate that the number of infected computers on the Australian internet is considerably greater than the 10,000+ compromises currently being reported through the AISI on a daily basis. These factors include the following:

> *The constantly changing compromise 'landscape' on the internet.*
New compromise types are continually emerging, with the most significant compromise emerging in the last 12-month period being the 'Conficker' worm, which is discussed in more detail below. The sources providing data to the AISI will often need to develop new detection methods to identify these new compromises, and the ACMA is constantly developing new data handlers to process new and changed data feeds[3]. This volatility inevitably means that there are compromises that are either not identified in the data reported to the ACMA or there are delays in the reporting of compromise data for processing and other reasons.

> *The compromise data received by the ACMA is a subset of the total compromise data identified that relates to Australian IP address ranges.*
Some sources providing compromise data for the AISI make their data available directly to ISPs, and where this data is provided directly to an ISP it may not be provided to the ACMA. The ACMA estimates that in 2008-09 this 'direct ISP reporting' has resulted in the total number of compromises reported to ISPs being approximately 10 to 20 per cent fewer than would have been the case if this data had been reported to the ACMA. It is important to note, however, that if the ISP is utilising this compromise data in the same manner as it does the AISI reports, then the benefit to its customers is the same as if the data had been provided by the ACMA.

Some ISPs utilise independent sources of compromise data separate from those that feed into the AISI and some have also developed their own internal mechanisms to identify compromised IP addresses. It is not known how many additional compromised IP addresses are identified through these mechanisms, but it is likely to be a significant number. (Some

[3] Each source feeding into the AISI requires a discrete data handler in order to standardise the data contained in the daily reports provided to ISPs.

ISPs correlate the AISI compromise reports with their own compromise data sets to help prioritise their responses to compromises occurring on their networks.)

> The ACMA does not report compromise data to ISPs unless it has a very high level of confidence that the data represents a genuine compromise.
  The ACMA receives a substantial amount of indicative 'compromise' data that it does not report to ISPs, as it is either in the process of verifying the accuracy of this data or has previously assessed the data as potentially containing 'false positives'. As ISPs and their customers expend considerable resources responding to the daily AISI reports, it is important that their resources are focused on infections that have a very low likelihood of a false positive. Much of this discarded data, however, would contain genuine compromises.

> The AISI data only represents compromises that have been reported to the ACMA in the past 24-hours.
  As stated previously, an important feature of the AISI is the currency of the data, as it seeks to report recent infections that have a highly likelihood of being identified when a customer is contacted by their ISP and advised their computer is compromised. As a consequence, when the customer (or their agent) tests their computer for a compromise they will have a greater likelihood of identifying the compromise, as in many cases compromises occurring over a longer period may already have been eradicated by anti-malware. As a consequence, computers that are infected but have not been identified as active in the preceding 24-hour period are excluded from the AISI data. As many bots are not active within a given 24-hour period, they will not be included in this data.

> The intermittent supply of data from sources providing compromise data for the AISI.
  For a variety of reasons—including the development of new compromise detection methods and programming and hardware upgrades—the supply of data from many of the sources feeding data into the AISI is intermittent. As the ACMA is seeking to ensure that compromise data relating to a particular IP address is current, data that is reported beyond a 24-hour period is discarded. The ACMA is constantly seeking new sources of compromise data to moderate the volatility of the data and improve its diversity.

The preceding discussion illustrates the difficulty in making precise statements on the level of compromised computers on the Australian internet. The compromise environment is continually evolving and rapidly changing and is likely to remain so for the foreseeable future. What the analysis does indicate, however, is that the number of AISI compromise reports provided daily to ISPs probably represents the lower bound of compromised computers on the Australian internet.

Compromise levels relative to Australian residential internet connections

Comparing the number of residential internet connections in Australia with the potential number of compromised computers provides some context for the extent of the bot problem in Australia. However, as indicated in the following analysis, reaching firm conclusions from this data is very complex, as depending on the approach adopted the bot problem can be considered relatively inconsequential or a major concern.

Based on a survey of all Australian ISPs, the Australian Bureau of Statistics in its (ABS) *Internet Activity Survey*, *December 2008* recorded the total number of internet connections in Australia, as of December 2008 (business and residential), at 7.996 million. Residential internet connections constituted 6.675 million of these connections.

In broad terms the daily AISI compromise reports therefore, using the June 2009 average daily figure of 10,448 compromise reports per day, represent only a very small proportion—0.157 per cent—of the total residential internet connections in Australia. This analysis, however, as argued in the previous section, is likely to represent only a lower bound for the extent of the bot problem in Australia. The upper bound of the problem is not known, although the following section provides some indications of the potential scope of the problem in Australia, based on extrapolation of data contained in international studies of bot numbers.

The ABS report also recorded that 5.591 million (84 per cent) of residential internet connections in December 2008 were broadband services.

The increasing number of residential broadband services in Australia—and the increasingly greater data rates achieved by these services—is relevant to the consideration of the bot problem, as broadband services are more likely to be compromised by bot malware than dial-up internet services, and much more likely to compromise other internet users. This is because broadband services are often connected to the internet for extended periods, causing them to have greater exposure to compromises than dial-up services. They are also more attractive as hosts of malware, as they are more likely to have a constant presence on the internet than dial-up services and therefore be available to compromise other computers. Perhaps most significantly, broadband internet services are capable of disseminating malware at greater data rates than dial-up services.

While the compromise levels identified through the AISI represent only a small proportion of computers connected to the Australian internet at any given point in time, perhaps a more insightful way of analysing this data is to consider the number of Australian computers that collectively have been compromised through bot malware over an extended period of time. That is, computers that may have been compromised leading to personal identity information residing on those computers potentially being harvested for criminal activities.

On average, there were 4,291 AISI compromise reports per day over the 2008-09 year. On an annual basis, this represents 1.57 million discrete AISI reports. The ACMA has no means of identifying how many of these reports relate to the same computer or customer over the course of the year, as most residential internet customers in Australia are assigned dynamic IP addresses by their ISP. Therefore, the same computer or customer may be identified in separate AISI reports, although the IP address identifying their compromise will be different in each report. Anecdotal information from ISPs participating in the AISI indicates that some customers are continually identified in the AISI reports, which has resulted in the adoption of escalated procedures by many ISPs for these 'repeat offenders', including termination of their internet accounts in the most extreme cases.[4]

Although there are difficulties in determining how many individual Australian computers have been compromised extrapolating from the AISI data—and the consequential theft of personal identity information arising from these compromises—the AISI data indicates the population is potentially substantial. It is also important when examining this question to consider that one computer may contain the personal identity information of multiple users. Nielson Netview data for the month of May 2009 indicates that 11.2 million people used the internet from home during that month. Comparing this data with the previously quoted ABS figure of 6.675 residential connections in December 2008 indicates approximately 1.7 internet users per connection[5], significantly increasing the population of Australian internet users potentially exposed to identity theft associated with the 1.57 million discrete AISI reports in 2008-09.

While the AISI data does not enable the ACMA to definitively conclude that there are more infected computers on the Australian internet on a per capita basis in June 2009 than there were in June 2008, it is more likely than not that this is the case. However, the ACMA can conclude that the 10,000+ compromises reported per day in June 2009 represent a significant population of computer users exposed to potential financial fraud. This is because the malware identified in the vast majority of cases is capable of stealing the personal identity information of the infected Australian computer user, as illustrated by discussion of the Torpig botnet in the following sections.

Taken on balance, the AISI compromise data indicates the significant potential exposure of Australian internet users to personal identity theft arising from bot related malware. Accordingly, the ACMA considers this potential exposure should form part of the policy position adopted in responding to existing and emerging cyber crime threats.

The significant increase in the number of AISI compromises reported since March 2009 has also required a substantial increase in ACMA resources directed at addressing these compromises, an observation which is also expected to apply to ISPs participating in the AISI and responding to the daily reports. The ACMA's interaction with ISPs and their customers—the latter being usually via the ISP—has increase markedly since March 2009. These most generally involve the ACMA providing further information on individual compromise reports in response to enquiries for this information. In most (but not all) cases this further information can be obtained to assist the customer in more precisely identifying the nature of the compromise infecting their computer.

[4] Refer to the section below 'Botnet numbers and the significance of botnet size' for a more detailed discussion of this issue.

[5] Using the assumption that each home user had only one internet connection.

Botnet numbers and the significance of botnet size

As indicated in the preceding section, assessing the number of bots residing on the internet at a given point in time is complex and prone to widely varying estimates. Many of the estimates are provided by anti-malware vendors, utilising disparate assessment methodologies. There have also been studies undertaken by independent organisations, such as the Georgia Tech Information Security Centre (GTISC) in the United States.

The GTISC estimated that in 2008 '10 per cent of online computers were part of botnets', and predicted that in 2009 this number would increase to 15 per cent.[6] The United Kingdom's (UK) House of Lords, in its 2007 report *Personal Internet Security* cited an estimate of five per cent of all computers. This estimate was provided by the Center for Information Technology Research in the Interest of Society (CITRIS) at the University of California, Berkeley.[7] (If this estimate was accurate for Australia it would translate into 400,000 computers forming part of botnets.)

An April 2007[8] study from the Computer Science Department of Johns Hopkins University, examined the merits of different approaches to measuring the size of botnets, and posed the question whether the size of a botnet was the most important factor in measuring their detrimental impact on internet security. This study suggested that a more important metric may be how many bots within the botnet can be controlled by the botnet master at any given point in time, with this number in many cases being a small proportion of the size of the botnet.

A recent study (April 2009) from the Department of Computer Science at the University of California, Santa Barbara—*Your Botnet is My Botnet: Analysis of a Botnet Takeover*—suggests that many estimates of botnet sizes may be inflated and contains a detailed analysis of the operations of the Torpig botnet. What is particularly interesting about this study is that it is drawn from actual data observed when the researchers took control of the Torpig botnet for a period of ten days.

A key finding from this study was that there were significantly fewer compromised computers identified than indicated by the number of discrete IP addresses contacting the botnet command and control server. Although 1.2 million IP addresses contacted this server over the ten-day period of the study, only 180,000 compromised computers were observed. This meant that many computers contacting this server were cycling rapidly through different IP addresses (one computer cycled through 694 IP addresses in ten days)[9].

This finding may indicate that the AISI reports represent a significantly smaller population of compromised Australian computers than the I.57 million IP addresses reported in 2008-09, although further analysis will be required to examine the validity of translating these findings into the Australian environment. An important consideration will be to compare how often IP addresses in Australia are assigned to the same computer, with practices in this area likely to vary considerably between different ISPs.[10] The ACMA will conduct research into this area over coming months.

[6] *Emerging Cyber Threats Report for 2009 Georgia Tech Information Security Center*, October 15, 2008. http://www.gtiscsecuritysummit.com/pdf/CyberThreatsReport2009.pdf

[7] House of Lords Science and Technology Committee, Personal Internet Security, 10 August 2007, para. 2.21

[8] My Botnet is Bigger than Yours (Maybe, Better than Yours): why size estimates remain challenging, April 2007, http://www.cs.jhu.edu/~moheeb/webpage_files/HotBots2007.pdf

[9] *Your Botnet is My Botnet: Analysis of a Botnet Takeover*, Department of Computer Science, University of California, Santa Barbara, p.7

[10] The following quote from the paper (p.7) notes how IP address allocation varies from one country to the next. 'Interestingly, the IP address count significantly overestimates the infection count in some countries, because the

It is apparent from the range of studies undertaken on botnets that there are many types of botnets employing different methods of propagation and control, resulting in wide variations in the impact of a botnet on internet security. Therefore, while the overall number of botnets on the internet is an important statistic, the consequences arising from botnet compromises is perhaps the most important focus of studies on botnet activities. The recent *Your Botnet is My Botnet: Analysis of a Botnet Takeover* study provides some interesting insights into this issue, as discussed in the following section.

ISPs in those regions recycle IP addresses more often in comparison to others ... For instance, a naïve estimate per country would consider Italy and Germany to have the largest number of infections. However, the ISPs in those countries assign IP addresses much more frequently than their U.S. counterparts. In fact, Germany had less than half the number of infected hosts, yet double the number of IP address connections.' Table 2 in the paper provides a detailed comparison of IP address allocation for 10 countries (Australia is not listed).

What are botnets used for? Examination of usage of the Torpig botnet

As botnets harness the collective computing power of the computers contained in the botnet, they are capable of causing significant harm on the internet, and have being doing so for some time. The most obvious area of botnet activities relate to the dissemination of spam, with botnets generally recognised as being responsible for the dissemination of at least 90 per cent of spam. Some estimates put this figure at 99 per cent.[11]

At the network level, ISPs filter out high levels of email spam. For example, one large Australian ISP routinely filters out more than 90 per cent of inbound email traffic to its webmail service as spam. A significant industry is involved in creating and maintaining anti-spam software and despite these efforts email users still receive spam in varying amounts. Aside from the criminal elements of spam, there are considerable costs to the Australian economy in combating this spam, which is almost universally generated from botnets.

Botnets have also been used for distributed denial of service (DDOS) attacks. While DDOS attacks can take various forms, they generally involve multiple computers generating a high volume of traffic to a website in order to prevent or limit access to that website. A recent example of a DDOS attack is that on US and Korean government websites in early July 2009, when 'at least 35 government and commercial Web sites in the two countries' were attacked.[12] According to Nguyen Minh Duc, a Vietnamese Senior Security Researcher, 166,908 zombies from 74 countries were used for these attacks.[13]

Given the critical commercial importance of many websites—for example, gambling websites—the threat of undertaking a DDOS attack on such websites has been used to extort money out of the website owners. In 2003, three Russian men launched 54 DDoS attacks on online gambling sites in 30 countries, and followed the attacks with demands for money. It is reported up to US$4 million dollars was extorted. One of the attacks was on the UK-Australian online gaming and wagering company, Canbet, during the Breeders' Cup horse race. The attackers demanded US$10,000, which the company refused to pay. The attackers then launched a DDoS attack which completely disabled the company's servers and allegedly cost Canbet US$200,000 a day until restored.[14]

The consequences to internet users whose computers have been compromised with malware are particularly significant, as botnets not only wreak havoc on other internet users, but harvest personal information from compromised computers. That this harvesting actually occurs is amply demonstrated by the empirical analysis contained in the *Your Botnet is My Botnet: Analysis of a Botnet Takeover* study.

As this study contains some of the most comprehensive information available on the operations of a botnet, the findings of the study are examined in some detail in this section. The malware that enables computers to be enlisted to the Torpig botnet is the Mebroot rootkit, which takes control of a computer by replacing the system's Master Boot Record.

[11] The anti-malware vendor Sophos, for example, often quotes this statistic: 'Zombie computers can be used by criminal hackers to launch distributed denial-of-service attacks, spread spam messages or to steal confidential information. SophosLabs estimates that more than 99 percent of all spam today originates from zombie computers.' February 2008 http://www.sophos.com/pressoffice/news/articles/2008/02/botnet-busted.html

[12] U.S., South Korea Targeted in Swarm Of Internet Attacks, The Washington Post, 9 July 2009 http://www.washingtonpost.com/wp-dyn/content/article/2009/07/08/AR2009070800066.html

[13] http://blog.bkis.com/?p=718

[14] Heavy sentence handed to cyber-blackmailers, Computerworld Security, 5 October 2006. http://www.computerworld.com/s/article/9003894/Heavy_sentence_handed_to_cyber_blackmailers

(Some statistics from the AISI on the number of reports of Mebroot are provided at the end of this section.)

The *Your Botnet is My Botnet* study provides some disturbing examples of the information harvested by the Torpig botnet during the ten-day takeover period:

> In ten days, Torpig obtained the credentials of 8,310 accounts at 410 different institutions. The top targeted institutions were PayPal (1,770 accounts), Posteltaliane (765), Capital One (314), E*Trade (304), and Chase (217).[15]

Over the 10-day period, 1,660 unique credit and debit card numbers were captured by Torpig, including one computer that belonged to a call centre operator who had 30 credit card numbers extracted. Accurately assessing the quantum of losses from this form of botnet-related crime is extremely difficult, as illustrated in the following analysis from the *Your Botnet is My Botnet* study.

> Quantifying the value of the financial information stolen by Torpig is an uncertain process because of the characteristics of the underground markets where it may end up being traded. A report by Symantec ... indicated (loose) ranges of prices for common goods and, in particular, priced credit cards between $0.10–$25 and bank accounts from $10–$1,000. If these figures are accurate, in ten days of activity, the Torpig controllers may have profited anywhere between $83k and $8.3M.[16]

The personal identity information stolen by Torpig during the 10-day period was substantial.

> Torpig bots stole 297,962 unique credentials (i.e. username and password pairs), sent by 52,540 different Torpig-infected machines over the ten days we controlled the botnet.[17]

The data captured in the study enabled the researchers to assess the extent of reuse of the same password and login credentials by users of the infected computers, with 28 per cent of these users using the same credentials for different websites. Assuming this behaviour is generally replicated in Australia, it highlights the need for continuing education of users on the importance of correct password management for online transactions, to help minimise exposure to online fraud.

A similarly disturbing finding was made by the researchers concerning the strength of passwords deployed by those whose credentials were stolen. Of the 173,686 unique passwords captured during the 10-day period, using a commonly available password cracking tool, the researchers observed that:

> in less than 75 minutes, more than 40% of the passwords were recovered. 30,000 additional passwords were recovered in the next 24 hours by brute force...[18]

Again, this finding underscores the need for internet users to use strong passwords, which was a central theme of the Government's June 2009 National E-Security Awareness Week.

Included in the data captured by Torpig was a substantial body of private information, including email messages, records of websites visited, communications in personal forums and blogs and so on. The capture of this data by Torpig represents a considerable invasion of privacy, and is a less commonly observed consequence of botnet infections, with considerable potential for malicious exploitation by botnet controllers. After analyzing this data, the '*Your Botnet is My Botnet*' researchers observed:

[15] *Your Botnet is My Botnet: Analysis of a Botnet Takeover*, Department of Computer Science, University of California, Santa Barbara, p.8

[16] *Your Botnet is My Botnet: Analysis of a Botnet Takeover*, p.9

[17] *Your Botnet is My Botnet: Analysis of a Botnet Takeover*, p.9

[18] *Your Botnet is My Botnet: Analysis of a Botnet Takeover*, Department of Computer Science, University of California, Santa Barbara, p.10

> The result is what one could call the zeitgeist of the Torpig botnet. The victims of Torpig prepare for exams and worry about grades (5% of the messages), look for professional advice from doctors and lawyers (1%), play video games (2%), seek jobs and submit resumes (14%), are sport fans (6%), discuss money (7%), trade goods online (4%), exchange insults (0.1%), and look for sex or partners online (4%).

A primary use of the Torpig botnet was to perpetrate sophisticated phishing attacks on the users of compromised computers. When a user visited a website pre-programmed into the malware—such as a specified page on a banking website—a webform was inserted into the web browser that appeared to belong to the website being visited, enabling the sensitive personal information to be harvested. The researchers noted that:

> These phishing attacks are very difficult to detect, even for attentive users. In fact, the injected content carefully reproduces the style and look-and-feel of the target web site. Furthermore, the injection mechanism defies all phishing indicators included in modern browsers. For example, the SSL configuration appears correct and so does the URL displayed in the address bar.[19]

The importance of providing comprehensive and sustained education to internet users about how to appropriately maintain their computer and protect their personal information online is underscored by the user behaviour recorded by the '*Your Botnet is My Botnet*' study. A key conclusion from the study was that:

> the victims of botnets are users with poorly maintained machines that choose easily guessable passwords to protect access to sensitive sites. This is evidence that the malware problem is fundamentally a cultural problem. Even though people are educated and understand well concepts such as the physical security and the necessary maintenance of a car, they do not understand the consequences of irresponsible behavior when using a computer. [20]

The Mebroot category is one of the compromise categories contained in the daily reports provided to ISPs through the AISI. Approximately 30,000 IP addresses with Mebroot compromises were reported to ISPs through the AISI from 5 March 2009 to 20 July 2009. As noted in the analysis above, it is not known how many individual Australian computers were compromised through this form of malware. The '*Your Botnet is My Botnet*' study emphasises, however, that botnets are not simply a theoretical concern to internet users, but represent a serious threat to personal identity information, individual privacy and other internet users.

[19] *Your Botnet is My Botnet: Analysis of a Botnet Takeover*, p.3

[20] *Your Botnet is My Botnet: Analysis of a Botnet Takeover*, p.11

How do computers connected to the internet become compromised?

In recent years there has been a steady increase in 'Drive By Download' compromises on the internet. These compromises are facilitated by a hacker breaking into a web server and altering a webpage so that it automatically includes browser exploitation code when a user visits it. A wide variety of websites are vulnerable to exploitation, ranging from websites utilising legacy web forms to recently installed blogs and content management systems.

A common attack vector for users visiting websites is banner advertising, which is often supplied by third parties. Websites owners and operators need to be vigilant in ensuring that their own and third-party banner advertising is free from malware.[21]

One of the most high profile examples of a compromised website was that of the Miami's Dolphin Stadium, the venue of the 2007 Superbowl[22]. The website was experiencing high traffic in the lead up to the Superbowl. Hackers inserted malicious code into the header of the front page so that visitors to the site were secretly connected to a remote third party. Unpatched computers visiting the site were vulnerable to the installation of a Trojan which put the computer completely under the hacker's control and could be used to steal confidential information or to launch DDoS attacks.[23]

The majority of compromised websites are 'legitimate' websites, as opposed to websites that have been established with the objective of luring internet users for the purpose of compromising the computer of the website visitor.[24] (The latter form of website is commonly represented in the urls contained in spam emails.)

It is comparatively rare now for computers to be infected by emails containing malicious attachments, as the attachments are generally identified by anti-malware software. However, spammers are constantly on the alert for innovative means to infect internet users and respond quickly to emerging events, as evidenced by the response to the sudden death of Michael Jackson. 'Within 24 hours of [his death], spammers sent out malicious emails using a fake video of the singer's death as a social engineering lure.'[25] The popularity of the Twitter website has also seen a recent increase in emails containing Twitter invitations with malicious attachments.[26]

The role of legitimate websites in the dissemination of malware points to a need for greater vigilance by website owners and operators in maintaining the security of their website, particularly those websites containing web forms for data entry. An education program for

[21] A recent high profile website experiencing this problem was that of digitalspy.co.uk, as detailed in the following statement from this website: 'We can confirm that over the weekend it appears that Digital Spy was attacked by one or more ads containing some form of malware... We think that the attack happened through a practice known as chain buying, where inventory bought on our site is then re-sold to another provider, and possibly then others, making it progressively harder to verify the integrity of creative.' Reported at :
http://www.theregister.co.uk/2009/06/02/digital_spy_malware/ 2 June, 2009
It appears another variant of this problem resurfaced in mid-July 2009, as identified by website visitors from the United States and Australia. http://www.theregister.co.uk/2009/07/20/digital_spy_malware/

[22] http://securitylabs.websense.com/content/Alerts/1346.aspx

[23] Viruslist.com: Drive-by Downloads. The Web Under Siege; 15 April 2009
http://www.viruslist.com/en/analysis?pubid=204792056

[24] For example, see the *Websense Security Labs, State of Internet Security, Q3 – Q4, 2008* report, which states '77 percent of Web sites with malicious code are legitimate sites that have been compromised'.

[25] In the Mail, Monthly Websense Email Security Threat Brief, June 2009

[26] Symantec State of Spam, A Monthly Report, July 2009

website owners would help raise the awareness of this problem and provide information on how to rectify the compromise.

The internet industry is beginning to respond to the problem of compromised websites. For example, Google identifies compromised websites with a 'This site may harm your computer' warning message when it returns website results for Google search queries.[27] It also emails webmasters of compromised sites advising them that their website is compromised. Some web-browsers, such as Firefox and Opera, also warn users about websites that appear to be infected with malware.

Given the role of compromised websites as the primary vector for cyber crime, developing a comprehensive and timely response to this problem needs to be a key and urgent focus of all areas of internet governance and by key internet industry stakeholders.

[27] Refer http://www.google.com/support/websearch/bin/answer.py?hl=en&answer=45449

Incidence of cyber crime related financial fraud and identity theft in Australia

The ACMA has no independent data on the extent of 'cyber' related financial fraud and theft of personal information in Australia. The Financial Services Industry is the most appropriate source of information on this form of financial fraud and fraud-related identity theft, although minimal information from this industry appears to be publicly available on trends in these areas.

The AISI data does however provide a broad indication of the potential population of infected computers in Australia from which such fraud and identity theft could be attempted, although the caveats previously expressed on how representative this data is need to be taken into consideration. Of course not all attempts at Australian cyber financial fraud occur from Australian IP addresses, just as Australian IP addresses will be involved in cyber financial fraud outside Australia. The ACMA is aware, however, that many Australian financial institutions have protocols in place that apply additional checks to internet based financial transactions occurring from non-Australian IP address ranges, which underscores the importance of maintaining a high level of integrity to the Australian IP address space.

Need to develop reliable sources of data on cyber crime and identity theft

The ACMA considers there is a need to develop reliable data sources that enable the development of a robust, proportional and appropriately targeted policy framework for combating cyber crime and e-security in Australia.

The Model Criminal Law Officers' Committee of the Standing Committee of Attorneys-General grappled with this problem in its March 2008 report *Identity Crime*, commenting that:

> Accurate measurement of the cost of identity crime is difficult and there are relatively few statistics available on its impact in Australia. The Australian Institute of Criminology reported that approximately one quarter of incidents involving fraud reported to the Australian Federal Police involve 'the assumption of false identities'. [2002 ref.] Identity Fraud in Australia, a 2003 report by the Securities Industry Research Centre of Asia–Pacific (SIRCA) for financial intelligence agency AUSTRAC, claimed that identity fraud cost Australian large business $1.1 billion in 2001–02.

A sample of some of the varying figures quoted on identity fraud in Australia is provided below:

- ACCC, March 2007 'On identity theft alone, losses to the Australian community are estimated to be in excess of $1 billion annually'[28]
- Baycorp Advantage, June 2005 '*Credit bureau Baycorp Advantage's chief executive Andrew Want said identity related fraud costs Australians more than $2.2 billion a year.*'[29]
- *The Australian Business Assessment of Computer User Security: a National Survey*[30], issued by the Australian Institute of Criminology (AIC) in June 2009 (the 'ABACUS' study), states that, based on its survey results:

  > The total financial loss as a result of computer security incidents against businesses in Australia during the 2006–07 financial year was estimated at between $595 and $649 million.

The ABACUS study notes the difficulty in correlating the level of computer security incidents reported by business with the actual level of identity theft experienced as a consequence of these incidents, positing that businesses are attractive targets for identity theft given the large volumes of customer data they will often hold.

> It is therefore important to consider the types of computer security incidents against businesses that may facilitate identity theft. The ABACUS study found high proportions of businesses experiencing computer security incidents such as viruses and other malicious code, theft or loss of hardware, unauthorised network access and phishing. These computer security incidents could facilitate the theft of personal data and therefore 'be the precursor to more serious crimes' (Wall 2007: 186). One recent report (cited in Choo 2008: 274) noted, for example, that 'most new malware is designed to steal financial data (e.g. credit card details, bank account details, passwords, PIN numbers) as a precursor to various frauds and other deceptions' (see also Georgia Tech Information Security Center 2008).

[28] Scams target you! Protect yourself. ACCC Media Release. 4 March 2007

[29] ID theft costs Australia $2b a year, Sydney Morning Herald, 3 June 2005

[30] *The Australian Business Assessment of Computer User Security: a National Survey*: Kelly Richards, Australian Institute of Criminology, June 2009 – Foreword, III.

> Although these types of computer security incidents were experienced by large proportions of ABACUS respondents, there is no way of knowing whether personal data were stolen and used to facilitate further offences.
>
> …….Of particular concern is the finding in the ABACUS study that only 11 percent of businesses reported using policies aimed at protecting electronic information such as customer account details.[31]

The importance of collecting accurate data on the losses associated with online crime and the problems in gathering this data, for both business and consumers, has been recognised in other jurisdictions. The August 2007 report *Personal Internet Security* from the UK's House of Lords Science and Technology Committee concluded it was 'impossible to deduce how much online identity theft costs the United Kingdom economy' from the various data available, including an estimate from the UK Financial Services Authority of an annual cost to the UK economy of £1.7 billion from identity fraud.[32]

Given the potentially large financial losses associated with cyber crime (of which identity fraud is generally considered to be the key component), and the potential for this crime to be perpetrated in both the consumer and business environment in Australia, it important that independent data is captured on the extent of these losses. It is also important that these losses are provided within a broader context of total losses (online and other losses) for fraud categories such as identity fraud, so as to inform appropriate policy responses and the direction of resources.

[31] *The Australian Business Assessment of Computer User Security: a National Survey*: Kelly Richards, Australian Institute of Criminology, June 2009; p. 86

[32] House of Lords Science and Technology Committee, Personal Internet Security, 10 August 2007, para. 2.27

International collaboration in combating Cyber Crime

The AISI model is unique to Australia and has generated considerable international interest. For example, the International Telecommunications Union (ITU) has developed a botnet mitigation toolkit 'inspired' by the AISI model[33].

A high level of international cooperation is essential in combating botnets, and by extension cyber crime. Botnets transcend international borders, with the botnet controllers capable of directing botnet activities from anywhere in the world. No country in isolation can solve the botnet problem in its own jurisdiction, as the same global connectivity that is the core of internet functionality is also the means by which malware spreads and botnets are created, maintained and expanded.

Multiple international approaches are required to combat botnets, with both formal and informal measures needing to be applied. The formal international action required is concerted efforts in international internet standards and governance fora to strengthen internet security. An example of relatively recent action taken that may help address one aspect of the problem is that of the Internet Corporation for Assigned Names and Numbers (ICANN) efforts in tightening domain registration rules to limit domain squatting.

The 'conficker' case study referred to below provides a good example of the relatively informal approach adopted by various individuals and organisations in multiple jurisdictions to address the problems caused by this malware. It is essential that Australia participates in these informal and formal groups in order to influence measures that can help address cyber crime, both in terms of longer term minimisation and the management of shorter- term cyber crime eruptions.

As noted earlier, the ACMA has been working with the ITU to share its experiences from the AISI in order to assist other jurisdictions in combating botnets. It is particularly important that this cooperation extends to developing countries, as these countries have greater potential to be harmed by botnets as they have fewer resources available to combat this problem. An article in *New Scientist* magazine from 15 December 2007 elaborates on the the e-security problems confronting developing countries as well as the need for greater international cooperation in this area:

> Suresh Ramasubramanian, a consultant at the ITU, is working with local authorities in Malaysia on a pilot project designed to work out how best to avert botnet attacks in developing countries. The ITU is taking its lead from Australia, the country it says is among the best prepared to fight cybercrime.
>
> Since 2005, the Australian Communications and Media Authority has run the Australian Internet Security Initiative (AISI), which since May has monitored the nation's internet activity. When it detects telltale signs of botnet behaviour, it reports the IP address of the suspect computer to the hosting ISP, which can then help users neutralise the bot software on their machines.
>
> This kind of international cooperation is vital if developing countries are going to shore up their defences against cyber-attacks, says Marco Gercke of the University of Cologne in Germany.[34]

[33] http://www.itu.int/ITU-D/cyb/cybersecurity/projects/botnet.html (8/7/09) This webpage also provides useful links to a number of botnet-related studies

[34] Beware, botnets have your PC in their sights, New Scientist Print Edition, 15 December 2007, p.23

Conficker case study

Botnets take many forms and guises, although they rarely seem to penetrate the general public consciousness unless they become particularly widespread or have some unique characteristic that captures the public's imagination. In 2009, the botnet (or more accurately a series of botnets) generated by the Conficker malware has probably received the greatest public attention. However, as discussed in the following analysis, this publicity appears to have not stimulated a sufficiently robust response by Australian internet users in eradicating this malware.

Conficker is a powerful computer worm that attacks Microsoft Windows operating systems by spreading through low-security networks, computers without current anti-virus software, and external devices such as USB sticks. While the individual malware installation techniques it employs are not new to industry experts, its combination of such advanced techniques renders it difficult to eradicate. The authors of the Conficker worm track security efforts and release new versions of the malware to overcome anti-malware defences. There are currently five known variants of the Conficker worm.

The Conficker worm (variant A) was first discovered in late November 2008, with variant B discovered on 29 December 2008. In response to the Conficker threat, Microsoft established the Conficker Working Group in February 2009, a body of technology industry experts who are collaborating to implement a united, global approach to combat the worm.

Computers infected with the Conficker worm connect to websites in order to receive instructions from the command centre. Among other things, Conficker harms the security services of the compromised computer and blocks access to many security-related websites.

The Conficker worm gained significant publicity leading up to 1 April 2009, when it was understood to have a pre-programmed set of instructions causing it to contact websites to update itself. At this time it was uncertain what the consequence of this update would be and what form the Conficker malware would then subsequently take (the characteristic of botnets to continually update and change form illustrates the difficulty in combating this cyber threat).

Conficker previously used up to 250 domain names per day to send botnet instructions, however from 1 April 2009 it activated a special algorithm to randomly generate 50,000 internet domains. The vast number of these sites makes it difficult for researchers to target and block access to them, although in this case the Conficker Working Group succeeded in having all 50,000 domains 'sinkholed' or 'blackholed', rendering this aspect of the malware impotent. This action took enormous effort and required widespread industry cooperation around the globe from domain name authorities and numerous domain registrars.

During 2009 the ACMA has been collaborating internationally to enhance the AISI data to assist in combating Conficker compromises in Australia. The ACMA has been working with members of the Conficker Working Group to fight these compromises through capturing data on the worm and reporting it to Australian ISPs through the AISI. Conficker compromises are largely responsible for the significant increase in the number of compromises reported in the daily AISI compromise reports from April to June 2009 (refer to Chart 1, above).

The Conficker worm is malware that is relatively easy to eradicate from a computer once identified. Instructions on how to remove the worm are available from the Stay Smart Online Alert Service at Stay Smart Online Alert Service > Server applications > Update on Microsoft Windows Worm - Conficker/Downadup - SSO-AD2009-009.[35] The ACMA issued a special email alert to ISPs participating in the AISI immediately prior to 1 April 2009, including a link to the Stay Smart Online Alert Service. Internet users are able to utilise free Microsoft's Malicious Software Removal Tool to remove this and other malware. The scale of the

[35] The url is: http://www.ssoalertservice.net.au/view/6d1531be07113a581ef14cda7b0d07c6

Conficker problem is exacerbated by the failure of many computer users to update their software. The Conficker Working Group estimates that '30 percent of Windows computers do not have the Microsoft Windows patch released in October 2008 to block this vulnerability'[36].

Unfortunately the Conficker worm has continued to expand in numbers after 1 April 2009 (based on AISI compromise data), although the rate of increase has significantly declined in June and July 2009. This indicates that more action needs to be taken by Australian internet users to protect their computers. It also raises the issue of how effectively ISPs are conveying information from the AISI compromise reports to their customers.

[36] http://www.confickerworkinggroup.org/wiki/. Date sourced: 28 July 2009.

Role of ISPs in combating bots and malware infections

The extent to which ISPs should mitigate the effects of bots on their networks is a vexed issue, as there is a limit to the resources that ISPs can be reasonably be expected to deploy to limit their impact. If the conclusions drawn by the authors of the previously cited *Your Botnet is My Botnet* study are correct—that the 'malware problem is fundamentally a cultural problem' requiring a greater level of education of internet users—then any technical solutions deployed by ISPs will only partially address the problem in any case.

The ACMA has observed through its collaboration with ISPs through the AISI that ISPs are prepared to voluntarily take actions to combat bots and botnets. The AISI is not a mandatory program and 68 ISPs currently participate in the program at a level they consider appropriate to their own resources, systems and processes for customer interaction.

In early 2009 the ACMA conducted a brief survey of a subset of AISI participants (those who had received a threshold level of AISI reports). The survey sought views from the ISPs of the effectiveness of the program and how it could be improved, more detailed information on how ISPs interact with their customers when they receive the daily AISI reports, and information on responses ISPs receive from their customers when they advise them that their computer is compromised. The responses indicated a diversity of actions taken by ISPs in addition to advising their customer that their compromised. Responses included:

- limiting the customer's data rate for accessing the internet to 64 kbit/s and blocking port 25 access, plus sending a warning email advising the customer they are likely to have a compromise and need to clean it up before full access can be restored (which includes a helpdesk phone number provided for assistance and information);
- temporarily suspending the accounts of re-offenders (some ISP responses indicated an account would be terminated upon the third strike or after a period of inaction by the customer);
- placing the customer's internet service in a 'walled garden' (thereby restricting or preventing access to the broader internet), with links to relevant software to enable a clean-up of the computer;
- temporarily suspending the customer's access to the offending ports and protocol activity; and
- regenerating account passwords (thereby preventing customers from accessing the internet) in order to prompt customers to call the ISP's helpdesk so they can be educated on the issue.

These responses represent a dedication of considerable resources by many ISPs to assist their customers in addressing compromises on their computers. ISPs also have a commercial motivation for addressing bot malware, as IP address ranges that have been identified as sources of spam are often placed on blacklists, preventing the delivery of email from these addresses. Customers who have been blocked often object strongly to this action, and are liable to contact an ISP's customer contact centre to have this situation remedied, tying up the ISP's front-of-house resources. Typically an IP address range is blocked rather than an IP address, so customers utilising an IP address residing in that range may be blocked even though they have no compromise on their computer(s).

Interestingly, a survey by Arbor Networks in 2008 of 66 'IP network operators from North America, South America, Europe and Asia'[37] indicated considerable support for ISP involvement in combating botnets.

> We also asked if respondents believe that ISPs should be responsible for detecting and monitoring botnets. Sixty-one percent said Yes, while 23 percent disagreed, and another 17 percent responded Yes, with some criteria.[38]

All survey respondents were directly involved in network security operations for their respective organisations, so the survey population can be considered to be generally knowledgeable on the topic, adding further weight to the positions adopted.

Given that ISPs have a unique relationship with consumers accessing the internet—they provide the conduit for this access—ISPs have an important role to play in the overall strategy to combat malware and cyber crime. They are also well placed to assist in providing advice and educational material to their customers on how best to combat cyber threats. There have recently been steps taken by the internet industry in Australia to develop a comprehensive and coordinated approach to improving e-security on the Australian internet, as discussed in the following section.

[37] Arbor Networks, Worldwide Infrastructure Security Report, Volume IV, October 2008, p.4
[38] Arbor Networks, Worldwide Infrastructure Security Report, Volume IV, October 2008, p.23

Development of the internet industry e-security code of practice

The development of a voluntary e-security Code of Practice was launched during National E-Security Awareness Week in June 2009. A key recommendation of the 2008 National E-Security Review, the development of an e-Security Code of Practice is part of the government's strategy to create a 'security culture' among internet users through increased engagement with the Australian internet industry.

The development of the e-security code is strongly supported by the ACMA, who advocated the development of such a code in its submission to the 2008 review. The process of developing the code will provide a useful forum for ISPs to share their experiences and practices in maintaining e-security on their networks. There is currently no equivalent e-security forum for ISPs, so in the process of developing the code it may be beneficial to consider whether the establishment of an ongoing forum would assist in maintaining and enhancing the security of the Australian internet.

It is intended, among other things, that the e-Security Code of Practice will provide guidelines for ISPs to deliver consistent messages to their customers when they receive AISI compromise reports or otherwise identify compromised computers on their networks. It is also expected the code will contain consistent approaches to customers who do not take remedial action when they are notified of a compromise.

The Internet Industry Association (IIA) will develop the code with input from the ACMA and the Department of Broadband, Communications and the Digital Economy. The IIA hosted an industry forum during National e-Security Awareness Week as an opportunity for industry to directly contribute to development of the code, and it was attended by approximately 50 internet industry representatives. The event was launched by Senator the Hon. Stephen Conroy , who stated in his address that: 'ISPs sit at the gateway to the internet and are often a trusted point of contact for consumers when it comes to getting the most out of their time online'.

The IIA hopes to finalise the code by December 2009.

Summation

This submission has focused primarily on the bot-related aspect of cyber crime in Australia, and particularly the potential number of compromised Australian computers, the implications of these compromises and some current bot-mitigation activities. The ACMA is uniquely placed to comment on these aspects from its AISI activities.

The importance of educating internet users so as to limit their exposure to cyber crime, while touched on briefly in this submission, has not been discussed in detail. The ACMA is engaged in broad-ranging cyber safety educational activities. For example, on 13 July 2009 the ACMA launched its new Cybsersmart website— www.cybersmart.gov.au —which contains extensive resources and guidance for children, parents, libraries and schools on how to stay safe online.

The Cybersmart website offers:

- information and advice for parents on online safety, emerging cybersafety issues and new technologies;
- tips and advice for young kids, kids and teens;
- games and activities, quizzes, videos and animations that reinforce cybersmart safety messages to children of all ages;
- a wide range of accessible and engaging resources for schools, including lesson plans, learning pathways, videos and classroom activities and resources, through the School's Gateway; and
- online registration for cybersafety presentations and programs, including Cybersmart Detectives.

A multi-faceted approach is required to address cyber crime in Australia, with perhaps the most effective long term solution being the raising of awareness of the need to be vigilant and e-security conscious in the constantly changing online environment.

Attachment A

ISPs participating in the AISI at 21 July 2009

AAPT	FoundationIT	Nowires Pty Ltd
Access Net Pty Ltd	GCOMM	Optus Internet
Adam Internet	Global Dial	Orion Satellite Systems
AINS	gotalk	Over The Wire Pty Ltd
Albury Local Internet Pty Ltd	GoWireless	Overflow
All Hours Communications	Grapevine	Pacific Internet (Australia)
AOL	HaleNET	PPS Internet/StudentNet
ATU Internet Group	Highway 1	Reynolds Technology
Aussiewide Internet	Hotkey	Riverland Internet
AUSTARnet	HugoNET	(The) Smelly Black Dog Company
Bekkers	Hutchison 3G Australia Pty Ltd	Soul Communications
Bendigo Community Telco	IDL Internet	Speedweb Internet
Castaway Travel	iiNet	Spin Internet
Central Data	Internode	Telstra Bigpond
Chariot	IntraPower	TPG Internet
Comcen	iPrimus	TSN Communications
Dodo Australia	iseek	Uecomm
Dreamtilt	ispONE	Unwired
EFTel	KDDI Australia	Virgin Broadband
Enterprise IP	Neighbourhood Cable	West Australian Networks
EscapeNet	Netspace	Westnet
Exetel Pty Ltd	NetYP	Wideband Networks
EZ ADSL	Nextep	