Australian Government

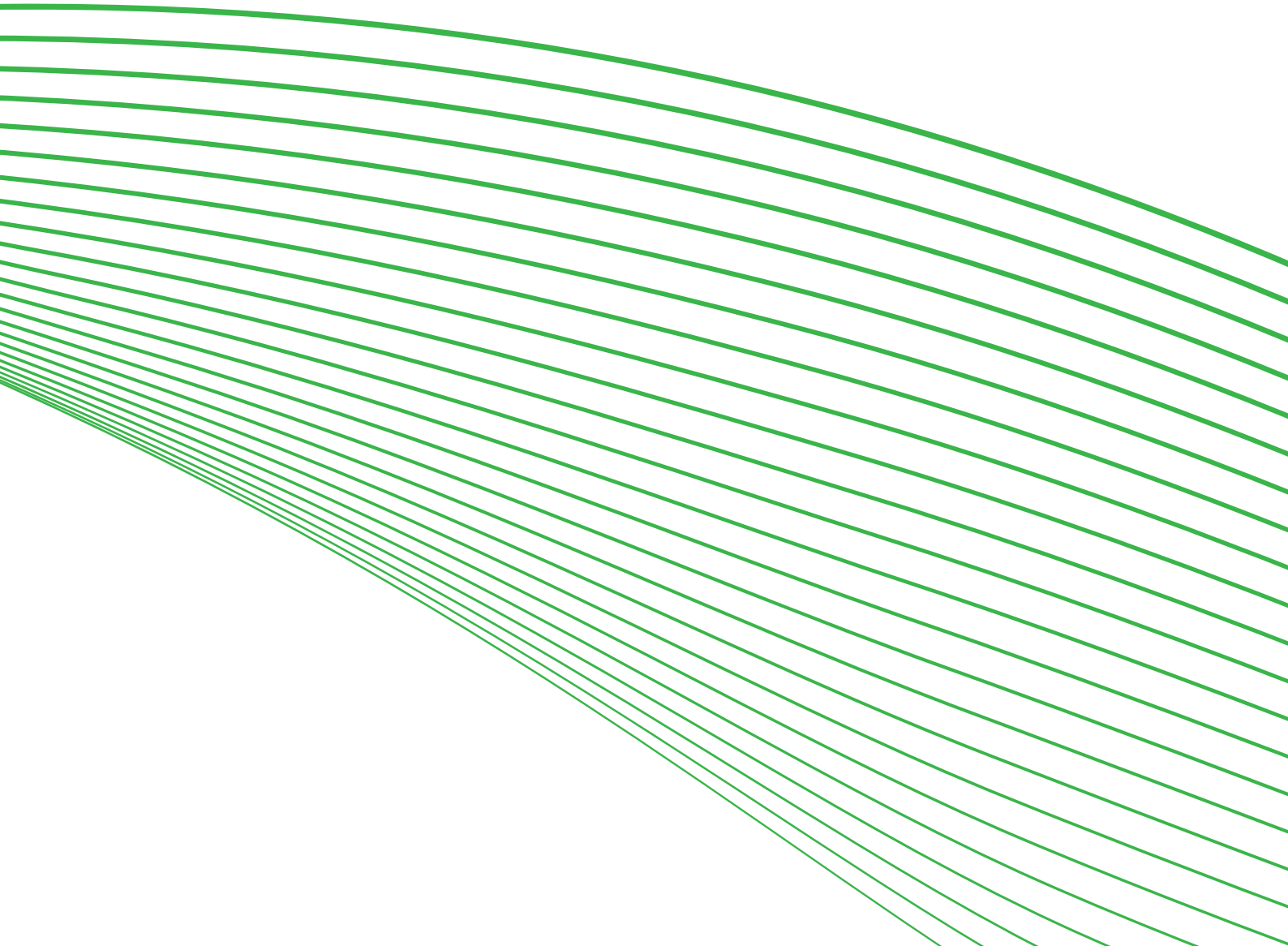
acma

Australian Communications and Media Authority

The Australian Internet Security Initiative—provider responses to security-compromised computers

Interviews with industry participants

SEPTEMBER 2012



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 5
The Bay Centre
65 Pirrama Road
Pyrmont NSW

PO Box Q500
Queen Victoria Building
NSW 1230

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

Published by the Australian Communications and Media Authority

Contents

Executive summary

The Australian Internet Security Initiative (AISI) is administered by the Australian Communications and Media Authority (the ACMA) to assist AISI participants address the problem of computers that are 'compromised' by malware (or malicious software). Malware infections enable computers to be controlled remotely for illegal or harmful purposes without the computer users' knowledge. While malware compromises may not be recognised by affected computer users, possible repercussions for internet users include the mass distribution of spam, hosting of phishing sites or identity theft.

When this research was undertaken there were 123 AISI participants who received 'daily' reports of compromises that were detected on internet protocol (IP) addresses on their networks. These reports help participants identify customers who may have a computer that is compromised by malware. Participants who receive these reports are encouraged to inform their customers about compromised computers and assist them to resolve the problem. AISI participants also receive weekly 'repeated sightings' reports that identify re-occurring compromises.

The research was conducted to understand the views of AISI participants about the operation of the AISI and how it might be improved. Twenty-four participants were interviewed by telephone between December 2011 and February 2012 by ACMA staff. Interviewees represent a range of AISI participants in different Australian states and include small, medium- and large-sized internet service providers, and universities.

Key findings

The findings are indicative of the ways that AISI participants respond to the information they receive about compromised computers. The small sample size of 24 does not provide representative measures of AISI participants, internet service providers or universities.

Various actions taken by AISI participants to address computer compromises

> The majority of the AISI participants (or providers) interviewed reported acting on AISI reports about compromised computers (21 of the 24 participants interviewed).

> AISI reports were generally regarded as accurate and useful by participants.

> Almost two-thirds of the providers interviewed who used AISI reports rely solely on these reports for information about malware infections.

> Almost all interviewed users of AISI reports had processes in place to address compromised computer problems with customers.

> The basic approach adopted by AISI participants to inform and assist customers to resolve malware problems involved notifying customers of the compromise, and providing information about the problem and how it might be resolved. This was usually achieved via an initial email and some providers did this by phone.

> About half of the AISI participants interviewed sent a standard email to notify customers about all of the compromises listed in the AISI reports. Some others cross-checked the information first or waited for multiple instances of a compromise to occur before contacting customers, and some acted only on the most persistent or significant malware problems due to other operational priorities.

> Most providers interviewed adopted strategies that encourage customers to respond to compromised computer notifications: two of these strategies relied on customers making follow-up phone contact with providers (in response to email

notifications or after their service had been restricted in some way); and another strategy was for providers to make follow-up phone calls to customers (often on the basis of AISI reports showing that the compromise had not been resolved).

> Some providers temporarily isolated their customers (in a walled-garden or captive portal) or cancelled services to prompt customers to make contact with providers and deal with compromises.

> Some providers gradually escalated their actions to encourage customers to respond to advice and resolve compromised computer problems.

> Varying degrees of assistance were provided to customers to help resolve computer compromises, and over half of the participants interviewed offered moderate to considerable assistance. This tended to involve additional advice and direct customer support as required.

Use of AISI reports by participants

> Almost two-thirds of the AISI participants interviewed who acted on AISI reports (13 out of 21 participants) relied primarily on these reports for information about compromises to customer's computers. Some medium- and large-sized providers used the AISI reports to complement or confirm other information sources.

> While a substantial majority of providers reported acting on AISI reports, three small-sized internet providers did not: two were developing their processes; and one was not aware it was receiving email reports due to organisational changes since it had registered with the AISI.

> Use of AISI reports varied considerably, with roughly a third of providers using both the daily and repeated sightings reports, a third mainly or only using the daily report, and a third mainly or only using the repeated sightings report.[1]

> Automated systems were widely used to process AISI reports, mainly by large- and medium-sized internet providers. Processing AISI reports (and information from other sources) usually involved providers sending a standard email to notify affected customers about a compromised computer problem.

Barriers to resolving compromised computer problems

> Allocating sufficient organisational resources by some large- and medium-sized internet providers was found to be the main barrier to more effectively dealing with computer compromises. Of those participants who acted on AISI reports, just under a third identified resourcing issues as limiting their capacity to make system improvements or provide better assistance to their customers to help them deal with these compromises.

> About a third of AISI participants interviewed (eight of the 21 who acted on AISI reports) reported that it was not easy or straightforward for them to match the IP addresses in AISI reports with specific customers or computers. This was mentioned by four medium-sized providers, two large providers and two universities. Difficulties occur where individual customers utilise dynamic (or changing) IP addresses, and where a single IP address is associated with many users such as in corporate organisations and universities. These difficulties indicate that some provider systems were not readily capable of matching IP addresses with customers or computers, although other participants reported being able to do this without difficulty.

Customer experiences from the perspective of AISI participants

> Residential customers and small- to medium-sized businesses experienced most computer compromises, and had a greater need for assistance from internet

[1] Providers who use only the repeated sightings reports and not the daily reports miss a large number of infections on their networks. This issue is discussed further in the main report.

providers. Large-sized business clients and universities had fewer compromises, perhaps as a result of having in-house IT support and computer systems that are better protected from malware and e-security threats.

- Although not quantifiable from this research, providers reported that compromised computer problems were usually resolved successfully by affected customers. These observations are based on direct feedback from those customers and by checking subsequent AISI reports for continuing problems.
- Many providers also reported that customers were generally unaware of compromises on their computers, but appreciated being informed.
- Some customers were suspicious about notifications from providers believing them to be scams or hoaxes, and consequently ignoring email notifications. Some customers also expressed concern about how ISPs obtained information about their computer and the legitimacy of that practice.

Suggested improvements to the AISI program

- About three-quarters of the participants interviewed indicated being mostly happy with the current AISI email reports, and had integrated the reports into their systems.
- About half identified improvements they would find useful. Improvements mainly referred to the provision of additional information that would:
  - assist with the identification of compromised computers
  - clarify the sources of information used in AISI reports and the methodologies used by these sources to identify compromises
  - identify the volume and history of activity associated with compromised IP addresses
  - identify infected websites hosted on their own networks
  - explain different types of compromises
  - advise providers about the actions they can take, such as quarantining internet services
  - provide intelligence about e-security risks
  - educate end users about the significance of computer compromises, the consequences of compromises and how customers can protect themselves.

It is significant to note that much of the additional information identified above is already provided regularly to AISI participants through the AISI program, and some information is not currently available from AISI data sources. More comprehensive information about computer compromises, including multiple sightings against IP addresses over a 24-hour period, will be provided through a proposed AISI portal that is currently under development. However, issues associated with computer identification can also be addressed by providers through other strategies such as improved network monitoring and analytical tools.

Some of the other suggested improvements, such as the general education of end users about cyber security and the identification of infected or compromised websites, are being addressed by other agencies.

- Some AISI participants were receptive to the idea of an online self-serve portal that was proposed to them during the interviews. Generally, these participants were interested in a portal if it provided useful information about computer compromises that they would otherwise not have.

Conclusions and recommendations

1. AISI reports are important sources of information about compromised customer computers for most AISI participants interviewed. Current reporting formats need to be maintained because they have been integrated into many providers' automated systems.
2. The main barrier to more effective use of AISI reports is the limited resources available to or allocated by some AISI participants to develop automated systems and improve customer assistance.

Sharing the research findings with AISI participants

3. A variety of approaches are used by AISI participants to address compromised computers with their customers. Understanding those actions might be especially useful to those participants who are not sure how to work with customers to resolve compromised computers within a voluntary scheme.
4. Sharing the research findings in this report could also be of broad interest to AISI participants to learn how others are using AISI reports and responding to malware problems.

User-friendly information for AISI participants

5. While information is regularly provided to AISI participants about the operation of the AISI—including the sources of reported AISI data about compromises and the expected actions of AISI report recipients—a number of those interviewed appeared not to be familiar with its content. Repackaging the material in a more attractive and user-friendly manner might help participants more easily access and use that information.

User-friendly information for small business and residential customers

6. Internet customers who learn about computer compromises from their internet providers might also find it useful to access well-presented and user-friendly information about relevant aspects of the AISI program. Information could focus on dealing with customer uncertainty, frustration and suspicion about the legitimacy of ISP notifications, and aim to improve customer understanding about the consequences of compromises and how they can best protect their computers.

AISI online portal for additional information

7. Interviewees were asked how useful they would find a self-serve online portal for additional information. A portal could provide more comprehensive information about computer compromises than that provided in the existing AISI email reports which may assist in the identification of compromised computers. It will also allow providers to undertake searches (for example, on IP addresses) and to more readily tailor compromised computer data to their specific needs. This portal is currently under development by the ACMA.
8. The portal could be a resource for AISI participants that links to other useful information sources. For example, the portal might link to information from CERT Australia[2] about how to report cyber security incidents, and educational material on cyber security for internet users from the Australian Government's website StaySmartOnline.
9. In a similar way, the portal could link to the internet industry's icode and its strategies to protect customers and networks from malware and e-security threats.

[2] CERT Australia is Australia's official national computer emergency response team (CERT). It is provides access to information to help protect Australians and Australian businesses against cyber based threats and vulnerabilities.

Enhanced engagement with AISI participants

10. Subject to resource availability, it may be useful for the ACMA to more regularly engage with AISI participants and more actively encourage feedback about the program. Such engagement may promote wider sharing of experiences between providers and reinforce an open line of communication.

Further research

11. Further research may be useful to estimate of the size of the compromised computer problem for internet users in Australia.
12. The ACMA is undertaking research to establish Australian's understanding of malware threats, their use of protections against harmful software and reasons for not using or updating anti-malware software. This research is expected to be published in late 2012.

Introduction

The Australian Internet Security Initiative (AISI) is administered by the Australian Communications and Media Authority (the ACMA) to assist internet and communications providers to address the problem of 'compromised' computers.

The primary activity of the AISI is obtaining data and reporting information that AISI participants can use to identify customers on their networks with computers compromised by malware (or malicious software). Its aim is for participating AISI participants to contribute to the reduction of spam and other e-security compromises. Participants are expected to advise customers that they may have a compromised computer, and to provide them with information to help them address the problem.

The research presented in this report examines how various AISI participants who receive those compromised computer reports act on that information to help protect the integrity of their customers' computers and their own communications networks.

The ACMA's strategic intent in conducting this research is to understand participants' perspectives on the operation of the AISI and how it might be improved.

Background

Participation in the AISI is voluntary, and open and free of charge to organisations that provide internet and associated communications services to a range of customers. The 123 participating AISI participants at the time of this research, which included 110 internet service providers and 13 universities, were then estimated to cover more than 90 per cent of Australian residential internet users. The AISI commenced operation six years ago, and more recently operates alongside the Internet Industry Association of Australia's (IIA) 'icode'.

The IIA 'icode' commenced in December 2010. It is voluntary and, among other things, aims to promote a security culture amongst the internet industry by reducing the number of compromised computers in Australia. The icode helps provide a consistent approach for Internet Service Providers (ISPs) to inform, educate and protect their customers from cybersafety risks. It encourages Australian ISPs to participate in the AISI and take steps to act on AISI reports. The icode is currently being reviewed and can be found at:
www.iia.net.au/userfiles/iiacybersecuritycode_implementation_dec2010.pdf

Acting on AISI reports involves informing customers they may have a compromised computer and assisting them to resolve the problem. Whether action is taken and the degree to which action taken is at the discretion of individual providers.

The Australian Government provides a website to assist internet users with cybersecurity and safety strategies at www.staysmartonline.gov.au. The ACMA provides a national cybersafety and cybersecurity education program—designed to meet the needs of children, young people, parents, teachers and library staff—with the associated website at www.cybersmart.gov.au.

Diversity of AISI participants

AISI participants represent a considerable range of internet and communications service providers. Most are ISPs, and along with other communications providers, offer a range of services that include website hosting, server hosting, cloud computing, online business networks, and subscription and on-demand television or video, as well as telephone, data, video and mobile communications. Their customers encompass residential, business, government, and university staff and student users.

Characteristics such as the type and size of service providers and the resources available to them have a powerful influence on how the AISI information is used by providers and their capacity to assist customers.

Information provided to AISI participants

The ACMA through the AISI program provides information and advice to AISI participants, along with data reports that identify compromised customer computers. The ACMA is also developing an internet portal that will provide additional data and information to participants.

Information provided about the AISI program

An information sheet *The ACMA's Australian Internet Security Initiative—Information for ISPs* is distributed regularly to AISI participants as an attachment to emails. It is updated as required, and emails are sent to participants when the ACMA has important new information to share.

The information sheet covers a range of advice about:

- the benefits of participating in the AISI program
- how the IIA's icode relates to the AISI
- the information that participants need to provide to the AISI
- the AISI 'daily' and 'repeated sightings' compromised computer reports, including how the reports might be used and examples of the data presented in the reports
- the information that participants might provide to customers about their compromised computer
- the top 50 different types of computer compromises reported by the AISI, with technical explanations
- some of the methods used by the ACMA to detect compromised computers
- where to find further information and who to contact about the AISI.

The ACMA welcomes requests for further information and feedback about the AISI program. Attachment A provides the latest AISI information sheet.

Additional links to information about the AISI program can be found at the following locations:

- AISI information page: www.acma.gov.au/aisi
- Presentation given at IIA icode forum, 14 June 2012: www.slideshare.net/acmaSlideShare
- Presentation given at Asia Pacific Computer Emergency Response Team (APCERT) Annual Conference, March 2012: http://event.idsirtii.or.id/wp-content/uploads/2011/10/The-Australian-Internet-Security-Initiative-Australian-bot-mitigation-Bruce-Matthews.pdf
- Presentation for the ACMA's International Training Program, 2011: www.acma.gov.au/webwr/_assets/main/lib100656/4.2australian_internet_security_initiative%28bruce_matthews%29.pdf

AISI reports

As part of the AISI, the ACMA emails two reports to internet providers who have registered to take part of the initiative and where compromises have been found on their networks:

1. Daily reports identify the number of infections detected for each AISI participant, a list of infected IP addresses and the corresponding name of the infection. These infections have generally been reported to the ACMA in the previous 24 hours

and are emailed to participants. Attachment B provides an example of the daily report.

2. Repeated sightings reports identify infected IP addresses that have been reported ten days or more out of the previous 14 day period, and which have been sighted once or more in the last three days. These reports are sent to AISI participants on a weekly basis. As with the daily reports, these reports detail the type of infection reported and information about the most recent time it was detected. They provide a strong indication of a persistent infection associated with certain IP addresses. Attachment C gives an example of the repeated sightings report.

Daily reports provide a more comprehensive list of compromised IP addresses than repeated sightings reports that present only a small subset of compromises. It is estimated that the repeated sightings reports list fewer than five per cent of the unique compromises covered in the daily reports. Therefore, participants who only use the repeated sightings reports would miss a large number of malware infections on their networks. This is especially the case where individual customers are allocated the use of different (or dynamic) IP addresses by providers and because multiple cases are only detected for a particular IP address over 10 or more days in a 14 day period.

The number of infected IP addresses that are reported daily by the ACMA to individual AISI participants range from zero to thousands. The total number of IP addresses that are currently reported per day for all AISI participants is approximately 19,000. Significant factors that influence the number of cases reported for individual providers include their market share, customer profile, network structure and systems, and management practices.

AISI reports are compiled from a broad range of data sources from the global cyber security community. Data collected are currently an amalgam of around 12 different sources, and some individual sources are also amalgams of different data sources (such as the Shadowserver feeds). The data collected are carefully checked by ACMA staff to promote accuracy, and large amounts of data are discarded where they are not considered reliable enough for reporting. Many of the data sources used by the AISI are not readily available to providers or ISPs.

While the AISI program is as comprehensive as it can be, it does not identify all forms of compromises affecting Australian internet users, and the amount of current compromises not reported through the AISI is unknown.

Proposed online portal

The AISI participants who participated in the research were asked in general terms whether an online self-serve portal might be a useful adjunct to the current AISI email reports. A portal could provide additional data about the compromises detected and be an alternative access point for AISI reports and other information. It is not practical to provide comprehensive additional data in the AISI reports.

The ACMA is currently developing a portal and a new version of the AISI software that will enable the capture and reporting of considerable additional data. For example, the current 19,000 reports per day are filtered from between one and two million daily malware-related ‘events’. Much of this additional data will be made available through the portal. Currently only the most recent event relating to a particular malware type for an IP address is reported by the AISI when there may be data available for hundreds of events for a given IP address over a 24-hour period.

Nature of the malware problem

Computers can be compromised through the surreptitious installation of malware (malicious software) that enables computers to be controlled remotely for illegal and harmful purposes without the user's knowledge. Compromised computers are often aggregated into large groups (known as botnets) that are used to assist the mass distribution of spam, the hosting of phishing sites and distributed denial of service (DDoS) attacks on websites.

Malware threats can have implications for both service providers and customers. From a consumer's perspective, the most effective approach to protecting against computer malware is to use anti-virus or anti-malware software, and ensure that it is kept up-to-date.

The nature of the malware problem is constantly changing as new threats arise. In May 2011, Microsoft reported that malware may occur at the rate of one in every 14 downloads from the internet.[3]

In 2010–11, the Australian Bureau of Statistics found that 90 per cent of the 15.3 million people aged 15 years and over who have access to a computer at home also indicated they had anti-virus and firewall software.[4] This indicates high use of such software at home but does not identify the extent to which the software is kept up-to-date.

The research

Research was undertaken with AISI participants to assist the ACMA to refine the AISI program by better understanding the measures used by participants to assist their customers to resolve computer compromises and any additional information or assistance that participants consider would enhance the program.

The findings may also be used to inform the review of the icode that is taking place during 2012.

Research issues

The views of a cross-section of AISI participants were sought to understand:

- how the AISI reports are used by participants
- what actions, if any, are taken by participants in response to the reports to notify and assist their customers
- how useful the reported information is to participants and their customers (from the perspective of participants)
- how the AISI program might be improved.

Details of the research methodology and sampling are provided in Attachment D.

[3] *Wall Street Journal* 'Malware is posing increasing danger', Technology, 23 May 2011.

[4] ABS, 8146.0 Household use of information technology, Australia, 2010–11.

Research findings

This chapter presents the results of 24 telephone interviews that were undertaken with a selection of AISI participants. The findings are indicative of the ways that internet providers respond to the information they receive about customer computers that have been compromised by malware.

Where relevant, observations about differences between the various types of internet providers are noted. As with the sample as a whole, these observations about sub-groups should not be regarded as representative measures.

Use of AISI reports by internet providers

The majority of AISI participants interviewed said they use and act on the information provided in AISI reports about compromised computers. Twenty-one of the total 24 were using the reports to notify and assist customers to resolve compromised computer problems.

Reasons for not using AISI reports

The three providers who were not using the reports were small-sized companies. Two of these small providers had been registered with the AISI program for one to two years and both said they had plans to act on the information. One of them in particular had reviewed the reported information, developed a comprehensive approach to address the compromises and was seeking management support to implement this approach. Management's main concern in this case was the development and resourcing costs involved that would divert resources away from their main focus on sales.

The third small provider was not aware that the AISI reports were being emailed to the organisation and consequently was not taking any action. Nor was it receiving any other information about compromised computers on its network. Knowledge about the AISI program had most likely been lost due to staffing changes since initial registration with the AISI in 2007. As a result of the interview email contact was re-established with this provider.

Use of AISI reports by internet providers varies considerably

Whether an internet provider uses both the daily and/or the repeated sightings AISI reports did not seem to follow a particular pattern. There were no associations apparent between internet provider type or number of cases reported, and use of daily or repeated sightings reports. Choices were made according to judgements about which information best suited their purpose and that could be accommodated within operational priorities.

Overall, there was roughly a three-way split between the providers who used both the daily and repeated sightings AISI reports, those who mainly or only used the daily report, and those who mainly or only used the repeated sightings report.[5]

Daily reports were considered to be timelier and allow providers to inform their customers of computer compromises on a daily basis. One medium-sized provider also expressed greater confidence in the comprehensiveness of the daily reports that capture more compromises than the repeated sightings reports. In this respect, daily

[5] As discussed in the introduction to this report, the repeated sightings reports provide less than five per cent of the compromises reported in the daily reports. Therefore, providers that only rely on AISI repeated sightings reports miss a substantial number of computer compromises.

reports were regarded by some providers as easier from a systems perspective to match with dynamic IP addresses.

Reasons for using or mainly using repeated sightings information are its multiple reporting of cases over a number of days. Providers said they could be more certain that a problem exists. Some providers used the repeated sightings reports to verify the information before they notified customers of a malware problem.

At least six providers specifically used the repeated sightings reports to check that problems had been resolved by customers. Some others used the daily reports for checking purposes.

Almost two-thirds of the AISI participants interviewed rely primarily on AISI reports

Thirteen of the 21 internet providers interviewed who used the AISI reports indicated they rely solely on the compromised computer reports that are provided by the AISI. A few of these also used information from AusCERT[6] to complement the AISI reports. Two of the universities and one small-sized provider interviewed mentioned using only the AISI and AusCERT sources.

Medium- and large-sized providers were most likely to make use of other sources of information (in addition to the AISI and/or AusCERT reports) to identify and guard against malware and e-security attacks. Some of these providers were less reliant on the AISI reports but many also used them to complement or confirm other information sources.

The other sources of information and protections used to guard against malware and e-security compromises that were identified include the following:[7]

- ShadowServer
- Google Safe Browsing
- Arbor Networks products
- Honeypots
- Intrusion detection systems
- AOL products
- Abuse Reporting Format (ARF) email feedback reports.

Other practices included gathering information in-house, system reports and equipment solutions such as:

- customer care and fault finding
- data flow, traffic monitoring and usage reports
- methods to pick up unexplained activity on VoIP ports
- use of protective/preventative firewall and modem technology.

AISI reports are generally regarded as useful

Besides the evidence in this report showing that almost all interviewees use the reports, many also elaborated on how useful the AISI reports are for them. Some of the comments made were ‘very useful’, ‘very valuable’, ‘rely heavily on them’, ‘works well in the background’, ‘sufficient to do the job’, ‘important for customers’ and ‘helpful’.

[6] AusCERT is the Australian Computer Emergency Response Team based at The University of Queensland. It operates within a worldwide network of information security experts to provide computer incident prevention, response and mitigation strategies.

[7] Some information sources were not identified due to confidentiality agreements.

Details given in the reports about infection types, related IP addresses and date and time information were regarded as critical to being able to identify affected customers and help resolve the problems.

Some providers indicated they did not do much about compromises before they received the AISI reports, and one medium-sized provider described their surprise at the volume of infections listed for their networks as ‘a revelation’ and ‘scary’.

Most providers recognised the ongoing and developing malware and e-security threats to their networks. This is reflected in the broad use of AISI reports amongst providers, the use of other sources of information about compromised computers by many, and the actions taken by providers to notify their customers about compromises (discussed later). One medium-sized provider encapsulated this by saying that ‘it is in everyone’s interest to deal with the malware threat and [we are] keen to be good corporate citizens’.

AISI reporting is regarded as accurate

AISI reporting was generally regarded as accurate. One medium-sized provider observed that the compromises found on customer computers often correlated with cases that were listed in the AISI reports. Similarly one university found the reports to be ‘very reliable’ as they almost always found an infection.

Two other providers observed that some of the reported AISI compromises could not be found on customer computers, presumably by the customer. Failure to find a reported compromise may or may not reflect the accuracy of AISI data because some compromises require specialised assistance and tools to detect. The recent DNSChanger malware for instance could not be detected by many anti-malware products.

One provider also mentioned that virus names were occasionally incorrect but ‘not a big issue’. It is often the case, however, that various names are used to identify individual malware. For example, other names for the prevalent *Conficker* worm are *Downadup*, *Downup* and *Kido*. Different names are also used by different anti-malware software products that are used to detect viruses and malware.

Automated systems are used widely to process AISI reports, mainly by large and medium-sized internet providers

Providers adopted either manual, partly automated or fully automated systems to process the information that is provided in the AISI reports. Generally, most of the small-sized internet providers interviewed processed the reported information manually. Medium-sized providers used either manual or automated systems, while the larger providers seem to be mostly automated. However, exceptions were found to this general pattern as described below.

Processing of AISI reports by internet providers

Automatic and manual processing of the AISI daily and/or repeated sightings reports involved matching the reported computer compromises to individual customers (from IP addresses) so that customers could be notified. For providers that use dynamic or changing IP addresses, the reported time and date of each compromise was used to help identify individual customers. This was mentioned by many providers as a particularly time consuming task when undertaken manually. Some computer compromises could not be matched with customers.

For compromises that could be matched with customers, a standard email was usually generated and sent to affected customers. Emails were the main method used to notify customers about computer compromises but some providers made a phone call.

Almost all of the small internet providers processed AISI reports manually. The main reason given for manual processing was the small number of computer compromises that were listed for their services which did not warrant automation.

Medium-sized internet providers adopted a mix of manual and automated processes. A few of these providers also expressed their intention to shift from a manual to an automated approach in the future in order to save time, but they were constrained by limitations on resources needed to make this change. Manual identification of customers who use dynamic IP addresses was considered to be a particularly time consuming exercise that could be improved by automation.

The three large internet providers used semi-automated or automated systems to process the AISI information, particularly to match IP addresses with individual customers. Two of these large-sized providers also automated their customer notification system by generating standard emails, while one assessed the information about compromises manually against other sources of information before making phone calls to each of the affected customers. That provider had fewer customers with compromised computer reports than the other two large providers. Automated systems were generally used by providers with a large number of reported computer compromises.

Two of the three interviewed universities used a manual or mostly manual approach to process the AISI reports, and one used a completely automated system. Universities can use a manual approach because of the small number of computer compromises they receive in AISI reports. One reason for the small number of reports may be the e-security and malware protection measures they take to safeguard on-campus computer networks and systems which are also supported by a team of IT personnel.

Actions taken by providers to address compromises on customers' computers

One of the most notable findings from this research is the variety of approaches that are adopted by internet providers to address the problem of compromised computers. This variety is in terms of the in-house processes used by providers and the degree of assistance and support provided to customers.

Almost all AISI participants take some form of action to address compromised computers

Except for the three small-sized providers who were not acting on AISI reports and one provider that did not notify customers about compromises, all other providers took some form of action to assist their customers resolve computer compromises.

Four steps explain the basic approach:

1. notify the customers affected—usually via email but some did this over the phone
2. provide information about the problem and how to resolve the problem
3. request that customers rectify the problem—usually by installing and/or updating anti-virus or anti-malware software, and if required by seeking professional technical support
4. offer and provide further assistance to customers.

Notifying customers about compromised computers

Initial emails and phone calls made by providers to customers about compromised computer problems include some, most or all of the following information:

> notification that the customer may have a compromised computer (may identify the AISI program and/or the ACMA as the notifier, and they may provide some information about them)

> IP address, name/type of compromise, date and time of compromise

> recommendation that the customer update or install anti-virus or anti-malware software, and run that software

> some recommend specific anti-virus or anti-malware software, either their own or others that are available free or for a price

> some refer customers to their own website or the icode website for further e-security information

> most recommend that the customer seek advice and assistance from an IT technician or local computer shop if they cannot resolve the problem themselves

> some provide contact details for IT technicians in the customer's local area

> most report inviting the customer to call the provider if further information or assistance is required.

While the steps taken by providers to help resolve compromised computer problems with their customers were basically the same, the approaches varied considerably with regard to the degree of information and assistance provided, whether follow-up phone calls are made to customers and whether any measures are taken to limit or cancel the services provided to some customers.

Customers receive varying degrees of assistance from providers

The level of assistance provided to customers varied from what can be loosely described as limited, to moderate or considerable. More than half of the providers interviewed (who act on compromised computer reports) offered moderate to considerable assistance, while less than half provided limited forms of assistance. Levels of assistance generally reflect the type of support that is required by particular customers and that can be accommodated within the operational resources of individual providers.

Some medium and most large business clients required little assistance from internet providers to resolve compromised computer problems. After notifying and informing these clients about compromises there was an expectation that the client would fix the problem. Medium and large business clients tended to have greater capacity and technical skills to apply patches and deal with e-security problems in-house.

Some residential customers were also offered little assistance by providers beyond the information that was given in the initial email notifications. Emails gave details about compromises, recommended running antivirus software and suggested that customers seek professional IT assistance if needed. Primary responsibility for fixing

compromises was placed on customers. For instance, one provider did not give recommendations because of the risks involved, another had no helpdesk support, and another only provided further assistance if its recommended antivirus software had been purchased.

Most providers gave moderate to considerable assistance and support to residential customers and to small- and medium-sized business clients who required assistance. Moderate levels of assistance tended to involve information, helpful tips and greater support for customers. Support was most often given directly to customers over the phone and involved taking customers through the necessary steps to resolve a particular problem. Customer service or helpdesk staff would take customers through the process of installing or updating and running anti-virus software, give helpful tips, reinstitute a firewall if it had been disabled, isolate a modem port until the problem was fixed, and in one case offer to send out an outsourced IT person to fix the problem if necessary (for a fee). Many providers said they try to give as much assistance as possible over the phone. If phone assistance failed to solve the problem, the last step was usually a recommendation to take the computer to a professional IT technician or specialist retail outlet.

Each of the three universities interviewed provided staff and students with medium to considerable assistance to resolve malware problems. Central or delegated IT personnel were available on-site to personally assist staff and residential students to fix problems. Affected staff who worked in two of the universities were sent an initial email notification about a possible computer compromise and were then expected to request IT support from their faculty's IT staff if they could not resolve the issue themselves.

In many respects, universities operate in a similar way to the large business clients of internet providers. Like large businesses, universities have computers that are well-protected against malware and e-security threats and have easy access to their own IT personnel. One university also provided a web link to free anti-virus software for staff and students to download onto their personal computer equipment.

One of the large-sized internet providers interviewed stood out because of the high level of support it gave to customers to help them deal with computer compromises. This provider reported drawing on a range of information sources, including AISI reports, to identify compromised computers before making initial telephone contact with affected customers—mainly corporate customers and also residential customers. Follow-up continued by phone for as long as it took to resolve a problem. This included obtaining remote access to client computers with customers' permission, and phone calls that could stretch to a couple of hours each and sometimes a number of phone calls to an individual client before a problem was fully resolved. The attention paid by this provider to compromised computers and associated customer service appeared to be considerable.

Most internet providers have a strategy to assist customers to fix compromised computers

A few small- and medium-sized providers continued to provide email notifications to customers with information and a request to resolve the problem for as long as compromised computer problems kept arising in AISI or other reports. They continued in this way without any apparent escalation of the issue. In addition, one medium-sized provider only followed-up affected customers if they had purchased its recommended antivirus software. This provider was also still considering how it could address compromises that were experienced by its customers who did not have the recommended antivirus software.

Most of the interviewed providers adopted a follow-up strategy to assist customers further and resolve the problem. Three different communication strategies were used, two of which relied on the customer to initiate further contact:

1. customer initiates phone contact with the provider after receiving initial notification email/s about a compromised computer
2. customer initiates phone contact with the provider after their service has been restricted in some way by their provider
3. initiated by the provider when they continue to receive compromised computer reports that indicate there has been no resolution to the problem.

Customers initiate phone contact

The first strategy relies on customers receiving and reading an initial email notification. Generally, it was apparent from many of the interviews that a small proportion of affected customers responded to providers after receiving an initial notification. Many providers assumed that the problem had been resolved where subsequent AISI reports were not received for these customers.

One of the large-sized companies interviewed said it reached a relatively small proportion of affected customers by email and did not have the resources to contact every one of them by phone. Further contact was only made if customers responded to the initial email notification, or if the problem was still appearing after several weeks, seemingly leaving many customers without any notification of a potential problem for several weeks.

A few providers applied the second strategy to encourage a more rapid response from customers by slowing, limiting or cancelling those customers' internet services. These providers restricted the services of affected customers by putting them into an 'abuse state', a walled-garden or captive portal. The strategy effectively pushed customers to make contact with the service provider.

Providers make follow-up phone contact

A number of providers adopted the third strategy and, like many of the actions taken by providers, they applied different approaches. For instance, they applied various time periods to repeat or ongoing compromises before making further contact with customers (after initial email notification). This follow-up generally included making a phone call to the customer if compromises kept arising in AISI repeated sightings or daily reports.

As previously mentioned, some providers checked subsequent reports to identify repeat compromises that had not been resolved. This also triggered providers to make phone contact with customers. Different providers had different schedules that would trigger a follow-up phone call. Examples are when a compromise appeared once again in the next report, when a compromise appeared in the next three reports, or if a customer had been emailed three times over the next six weeks about a compromised computer, then phone contact was initiated.

Some providers isolate or cancel customer services to force customer contact

Two providers (a small-sized and large-sized provider) confined customer services with computer compromises to a captive portal or walled-garden. These 'abuse states' forced customers to make contact with the service provider to resolve the problem and regain access to their internet service. This approach was taken by the small-sized provider that had a small number of compromised computer cases, and by a large-sized provider, especially during times when staff resources were stretched.

This strategy was applied either at the beginning of the process (that is, when the initial email notification was sent out) or as part of an escalation process if customers were not attending to an issue.

Another small-sized provider said that it would cancel a service in order to force a customer's attention to resolve the problem.

Another large-sized provider was considering the strategy of using a walled garden or captive portal and said that it is too expensive to set up. That provider had also considered a physical mail-out strategy to all affected customers which had not been implemented because it was too costly.

Some providers permanently cancel some internet services

Cancellation of services occurred rarely and was mentioned by three providers as happening to a small number of their customers over a period of time. This course of action was used in circumstances where it was considered necessary to protect providers' operations or the internet services being provided to other customers.

One medium-sized provider cancelled a service only after numerous phone calls were made to the customer in order to resolve the issue.

One university interviewed had a policy to disable users of their wireless service who did not follow advice and fix a compromised computer problem; however, this policy had never been acted on.

Some providers have escalation processes for problems that are not resolved by customers

Almost a third of the providers interviewed referred to specific escalation processes, (and others also indicated some form of escalation) that were used to encourage their customers to respond to advice about compromised computer problems. Escalation follows the initial email or telephone notification to customers and depends on customers' responses.

The adoption of various approaches by different providers has already been described with regard to making follow-up phone calls and providing customers with additional information and more direct support. The final stage of escalation for most providers is a recommendation that customers seek advice from an IT technician or computer retailer to solve the problem if not already resolved. Some providers also used strategies to slow down, limit or cancel a service that would either prompt a response from customers or remove unwanted customers on rare occasions.

One of the internet providers interviewed said it would like further information about escalation procedures, and specifically how it might explain actions such as service quarantining to customers. Some other providers also expressed uncertainty about their obligations and responsibilities and the best way to act on computer compromises. These comments possibly reflect a lack of understanding by some ISPs about the environment they operate in. Providers are not required to meet any particular obligations and the best approach will depend on what is appropriate in each provider's particular circumstances. The ACMA suggests in its AISI information sheet (Attachment A) that ISPs reset their user password so that affected customers have to contact their provider to regain internet access. The icode also recommends possible actions.

Types of computer compromises that are addressed by providers

Approaches taken by providers also depended on the types of computer compromises involved. Some notified all of the affected customers that they could identify with IP addresses, others undertook an assessment of the reported data before notifying customers, and some others took action only against significant malware threats.

Half of the providers notify affected customers about all compromises listed in AISI reports

About half of the interviewees notified affected customers about all reported daily and/or repeated sighting compromises that were listed in AISI reports. Small- and medium-sized internet providers were the most likely to take this course of action, although one of the large-sized providers also sent out emails to all affected customers. Universities also tended to address each of the compromised computer cases they received.

Other providers assess the compromises before notifying customers

The remaining half (approximately) assessed and interpreted the data received against other available information sources before notifying their customers. This took a variety of forms and included the following practices:

- cross-checking the information provided in the two AISI reports
- identifying multiple reports of compromised computers from within individual sources or across different sources
- using AISI reports to complement other information sources and/or help confirm the accuracy of other sources (a total of eight providers did this: four medium-sized, two small-sized, and two large-sized providers)
- identifying and prioritising the most significant or serious compromises that posed the greatest risk to customers and the provider's network
- responding to customer calls about slow internet speeds or other unusual incidents that may indicate the existence of a computer compromise, and then match these instances against the computer compromises that had been reported.

Underlying these practices were considerations such as a desire to act cautiously and wait for additional information in order to be certain about a compromise before informing customers.

Some providers act only on the most persistent or significant malware problems

Some providers decided to act only on the most persistent and significant computer compromises. These included multiple compromises that were listed across different reports and particular infections that represented a risk to the provider's service. Having its IP ranges blacklisted was a major threat identified by one service provider. That provider also undertook periodic reviews to identify customers with multiple (about 20) reports for particular action.

In assessing the data received about compromised computers, another internet provider said it prioritised certain issues over others depending on the threat posed for the business. This provider commented that 'actioning AISI reports is a nice thing to do' but not a priority. At the same time, however, its staff were directed to deal with the AISI repeated sightings reports that indicate persistent infections as a priority. Other compromised computer problems experienced by clients were only acted on by this provider where a customer initiated contact to report issues such as slow internet speeds.

Another provider, one that chose not to notify customers about possible compromised computers, posted the information from the AISI reports in-house and crosschecked those reports against customers who called in about issues such as slow internet speeds. Like some other providers, they were not overly concerned about a couple of compromised computer reports against a customer's IP address. Action was generally based on the severity and regularity of compromises.

Barriers to resolving compromised computers

There were two main barriers experienced by providers that interfered with their capacity to help customers resolve compromised computers. The first was operational limitations on staff and budgets, and the second was not being able to easily identify specific customers or computers from the IP addresses listed in the AISI reports. The second barrier is essentially an operational manifestation of the first, that is, resource limitations impacted on the capacity of some AISI participants to successfully match IP addresses with specific customer computers that were compromised.

Lack of sufficient organisational resources is an issue for some providers

Adoption of various approaches to address computer compromises seem to be driven largely by practical and operational considerations about staff resources, time spent phoning customers, time spent matching data, costs to the business, judgements about the seriousness of computer compromises, other priorities, and addressing the needs of different customers (that is, residential customers, small-, medium- or large-sized businesses and universities).

Less than a third of providers interviewed reported that they experience difficulties fulfilling—to a high standard—the tasks associated with compromised computer problems. Operational issues were the main barriers for large- and medium-sized internet providers.

Achieving efficiencies in operational areas was the primary consideration for many of the interviewed providers. Responsibilities to address compromised computers often conflicted with providers' main business objectives to sell their services.

The strategies and approaches described above, such as encouraging customers to respond to provider advice, illustrate how providers try to fulfil customer service responsibilities to address compromised computer problems in the most efficient way possible.

Many providers have difficulties linking some computer compromises with customers or specific computers

Individual providers use a mix of dynamic and static IP addresses which they allocate to customers. Use of dynamic or changing IP addresses for individual customers means that customers with compromised computers may be harder to identify from AISI reports than those on fixed static addresses.

More than a third of the providers interviewed experienced at least some difficulties identifying computer compromises where customers had been allocated dynamic IP addresses. Automated processing of the AISI reports lessened this difficulty for a number of providers, but others often found the manual process—of matching IP addresses and times when compromises occurred with particular customers—very time consuming. This was the case for some medium- and large-sized companies and universities that manually process the data. One university said they were unable to identify or link compromised computer listings with some students, particularly those using wireless devices.

While many internet providers experienced difficulties matching customers to dynamic IP addresses, some other providers did not report the same difficulty. It is likely that

these other providers overcame the challenges by using software to assist this correlation, often achieved through an automated process.

An associated problem was experienced by business clients and universities who use one IP address for a number of computers. Additional work was created for some of these providers and clients when they tried to identify which computer was compromised. Without the use of software that could make identification easier, time consuming methods such as scanning individual computers were undertaken to locate the infection. Some of the universities interviewed and some providers with business clients expressed a desire for extra information that would enable them to identify an individual computer that was compromised.

Small-sized internet providers were least likely to report difficulties involved in matching IP addresses to customers.

Providers' perspectives on customer experiences

Interviews with internet providers can only give limited insight into the experiences of consumers who are affected by malware and e-security compromises. However, some intelligence has been gleaned from the perspective of service providers about the diversity of their customers, and the issues that some customers experience.

Residential customers and small- to medium-sized businesses experience most computer compromises

Providers identified residential customers, small-sized business clients and some medium-sized businesses as most susceptible to e-security risks, and as a consequence having a greater need for assistance to help resolve compromised computer problems.

Acting on e-security problems was not always straightforward for some of these customers. Key reasons for the problems experienced were the continuing use of old computers and old operating systems, and out-of-date (or no) antivirus software installed on computers.

One medium-sized provider said that many customers run older operating systems and have anti-malware that was probably free for a time when they bought the computer, and since then has not been updated. In some of these cases, this provider said that a malware problem can take up to two days to sort out by an experienced technician which is expensive and may not be affordable for some of these clients. The same provider said it hears occasional stories of customers who have used a third-party technician to resolve the problem which was not fixed despite spending a considerable amount of money.

Conversely, many providers observed that large-sized business clients received a small number of reports about computer compromises compared with residential customers and smaller businesses. Fewer reports were attributed to the capacity of large businesses to have in-house IT personnel and computer systems that are protected by anti-malware and other agency-wide e-security measures or practices.

Customers seem generally unaware about compromises and appreciate being informed

Internet providers interviewed did not formally seek or gather feedback from their customers. Many providers also said that customers generally responded in a positive way, were generally happy, thankful and grateful about being informed and were keen to fix the problem. This assessment was based on feedback received from a relatively small proportion of affected customers who had contacted providers or had been contacted by providers about a compromise.

Providers said that many customers they had contact with were surprised or shocked, as they were unaware of a problem. On the other hand, some customers had noticed their computer or internet service had been operating slowly or had another problematic issue.

According to providers, customers also typically found the information and assistance provided to be useful and helpful in rectifying the problem. Some appreciated being able to do something about the associated problems they had been experiencing. One small-sized provider reported that their customers did not always understand the details but relied on anti-virus software to fix the problem. Another said that some customers were confused and did not know what to do.

Some customers were less responsive to the news that they might have a compromised computer. One medium-sized provider had some customers who did not want to know about the problem. The same provider also said that infections are often the result of customers following a link to an infected website without being sufficiently protected, and that most infections seem to occur out of ignorance.

Another medium-sized provider said that most of its customers with compromised computers who do not have an antivirus or anti-malware application do not do anything to fix problems and are repeatedly reported in AISI reports. This provider assisted clients who were using its recommended antivirus software but were uncertain how they should respond to those other customers.

There were a couple of cases mentioned by a large-sized internet provider where customers were not happy because running antivirus software had not resolved the issues. That provider contacted the ACMA for additional information to assist these customers further.

Some customers are suspicious about notifications from their providers

Some customers were reportedly suspicious about receiving compromised computer notifications from their providers, thinking that it was a scam or a hoax.

Customer suspicions were mentioned by each of the large-sized internet providers interviewed, and by at least one medium-sized provider. Some providers said they found it difficult to prove to customers who they are, and that customers tended to ignore emails if they believed they were a hoax. One provider said that the customers most vulnerable to computer problems were the hardest to communicate with.

One incident came to light during the interviews where a customer tried to verify the source of a compromised computer notification email and was unsuccessful. Customer service care staff misunderstood the initial enquiry and advised that the email could be reported as spam. The process became somewhat protracted leading to frustration and confusion by this customer until they contacted the ACMA who helped resolve the confusion.

Another provider referred to some customers who wonder how the information about their computer has been obtained and whether it is a legitimate practice. The provider concerned said they needed to carefully explain their use of legitimate techniques that do not compromise their personal service, and were not illegally ‘sniffing’ or intercepting their internet traffic. This involved letting customers know that their sources were legitimate, that appropriate cross-checks of the data were undertaken by the provider, and that the information they had about a compromise was genuine.

One of the small-sized internet providers reported having an authorisation process in place so that customers feel confident in dealing with them about these problems.

Compromised computer problems seem to be resolved successfully by many affected customers

Although not quantifiable from this research, it would appear that many compromised computer problems are being addressed and resolved by computer users once they are notified and advised about a problem by providers. However, some are not being resolved quickly, and some are not being resolved at all where customers cannot be identified or where they are not being notified of minor compromises. It is also possible that some affected customers might not be receiving email notifications from their internet providers.

As reported, most of the providers interviewed took steps to notify their affected customers about compromises. Many providers gave ongoing customer assistance over the phone, some prompted customer attention by restricting the operation of their internet service, and some providers checked subsequent AISI reports to determine whether problems had been resolved. If reports stopped, providers assumed that the problem had been dealt with.

By adopting a combination of these actions, different providers appear to be facilitating the successful resolution of many computer compromises by affected customers—at least at a reasonable pace for the most persistent and serious events.

Suggested improvements to the AISI program

Each internet provider interviewed was asked if they could think of any improvements to the AISI program or its compromised computer reports. Their views about a new online self-serve portal were also explored.

Majority of providers are happy with the current AISI email reports

About three-quarters of the providers interviewed indicated being largely happy with the current AISI reports and email notifications. Generally, these providers reported getting the information needed, that the current system works well and the reports were easy to use. Many of them did not suggest any particular improvements during interview.

The extra work anticipated to implement any change to the AISI reports was clearly a reason for not suggesting changes or improvements to the reports for some providers. Receipt of AISI reports often initiated some form of action by service providers such as causing a customer ticket to be created. Many providers had also integrated the AISI reports into their internal systems and automated processes that were used to identify customers and generate standard emails. Changes to the current reports would interrupt their current processes, and for many it would demand extra work and resources that were not readily available.

Many providers report that extra information would be useful

While the majority of providers interviewed were largely happy with the content of the current email reports, about half of all the providers also identified improvements when asked. Suggested improvements were mainly about the provision of more detailed information and some comments were about the format of reports.

Some of the additional information identified below is already provided in the AISI information sheet (Attachment A) and the icode. This suggests that some providers are not familiar with the contents of those information sources.

Also, some of the additional information mentioned by providers to more easily identify individual computers that are compromised may not be available. While some additional information can be provided by the AISI—such as multiple sightings of a given IP address that has been compromised over a 24-hour period—the identification of individual computers may be best addressed using software and other strategies by the affected internet service providers, universities and business clients—resources permitting.

The extra information identified varied for different providers and covers:

- details that would help AISI participants identify specific computers that were affected by compromises, particularly those in office and university situations where numerous computers use a single IP address. This was mentioned as a particular problem by a number of providers because of the considerable time and resources that were needed by their business clients to identify affected customers. Examples given were:
  - port information for compromised computers
  - source and destination URLs
  - whether a Mac or PC was used
  - the version of Windows operating system being used
  - what the compromised software requested from the user
- details that would help AISI participants identify specific household customers whose computers are affected by compromises
- greater transparency about the sources of information used to compile the AISI reports, and how those sources are processed
- information about the volume of activity of compromised IP addresses
- information about infected websites
- better alignment of the reported compromises with the name given to the compromise (however, as mentioned earlier in this report, individual compromises or malware infections are often known by a variety of names)
- information that informs providers what they can do or are allowed to do, such as the quarantining of some customers who do not resolve their compromised computer problem. This was suggested to assist providers when they communicate with customers about reasons for taking certain actions
- more information that could be referred to while reading the report such as hyperlinks that define and explain the compromises listed.

While most additional information was for the purpose of providers, some information was also considered helpful for clients or customers. Such information included:

- greater education for end users about the significance of computer compromises, the consequences of compromises and how consumers can protect themselves.

A few interviewees mentioned some other improvements relating to the format of reports and their timeliness. These were:

- xml formatted information feeds to allow easier processing of reported data (apparently similar to the way that copyright information is presented)

  However, many of the providers interviewed regard the current tabulated reports as being sufficient for their purpose and for automation

> more timely reports that were not one to two days behind the occurrence of compromises.

Some providers are receptive to accessing an online self-serve portal for additional information

The AISI participants interviewed were asked if an online self-serve portal would be useful resource for additional information. Some said they were unlikely to use a self-serve portal as they did not see any additional benefit or value to be gained. However, the idea of a portal was of interest to others if it gave access to useful information they would otherwise not have, and if it were presented in a way that could be easily automated. This information included:

> historical information about customer's computer compromises

> information about infected websites

> intelligence or confidential information about e-security risks in order to promote awareness and preparation in advance

> capacity to be integrated into provider fault-finding systems so that customers could be informed about a possible compromise if they phoned in with a service complaint

> information in machine readable format and not requiring manual handling of the data (where relevant).

Conclusions and recommendations

1. For most of the AISI participants interviewed for this research, AISI reports were important sources of information that help identify compromised customer computers. They are particularly beneficial for participants who would not otherwise obtain and interpret such information. Current AISI report formats need to be maintained because they are integrated into many providers' automated systems.
2. The main barrier to more effective use of AISI reports was the limited resources available to or allocated by some participants to develop automated systems and improve customer assistance. The research found a general willingness by AISI participants to assist customers to resolve compromises within the resources they had available.

Sharing the research findings with AISI participants

3. There were a variety of approaches used by AISI participants to assist customers to resolve compromised computer problems. Having an understanding of those actions might be especially useful for participants who are not sure how to work with their customers within a voluntary scheme. The range of actions are summarised below.

Actions taken by AISI participants to address computer compromises

> The majority of the AISI participants (or providers) interviewed reported acting on AISI reports about compromised computers (21 of the 24 participants interviewed).

> AISI reports were generally regarded as accurate and useful by participants.

> Almost two-thirds of the providers interviewed who used AISI reports rely solely on these reports for information about malware infections.

> Almost all interviewed users of AISI reports had processes in place to address compromised computer problems with customers.

> The basic approach adopted by AISI participants to inform and assist customers resolve malware problems involved notifying customers of the compromise, providing information about the problem and how it might be resolved. This was usually achieved via an initial email notification.

> About half of the AISI participants interviewed sent a standard email to notify customers about all of the compromises listed in the AISI reports. Some others cross-checked the information first or waited for multiple instances of a compromise to occur before contacting customers, and some acted only on the most persistent or significant malware problems due to other operational priorities.

> Most providers interviewed adopted strategies that encourage customers to respond to compromised computer notifications: two of these strategies relied on customers making follow-up phone contact with providers (in response to email notifications or after their service had been restricted in some way); and another strategy was for providers to make follow-up phone calls to customers (where subsequent reports indicated that the compromise had not been resolved).

> Some providers temporarily isolated their customers (in a walled-garden or captive portal) or cancelled services to prompt customers to make contact with providers and deal with compromises.

> Some providers gradually escalated their actions to encourage customers to respond to advice and resolve compromised computer problems.

> Varying degrees of assistance were provided to customers to help resolve computer compromises, and over half of the participants interviewed offered moderate to considerable assistance. This tended to involve additional advice and direct customer support as required.

4. Sharing the research findings that are presented in this report could be of broad interest to AISI participants so they can learn how others are using the AISI reports and responding to malware problems. It might also help address managers' concerns and uncertainties that prevent or delay some small-sized internet providers from acting on the AISI reports they receive.

User-friendly information for AISI participants

5. While information is regularly provided to AISI participants about the operation of the AISI in the AISI information sheet (Attachment A), a number of those interviewed appeared not to be familiar with its content. Repackaging the material in a more attractive and user-friendly manner such as through a set of Frequently Asked Questions (FAQs) might help internet providers more easily access the information. The research findings indicate that such information could focus on:
   - how AISI report data are collected and processed to assist participants to better understand the range and coverage of the current AISI reports
   - the checks that are undertaken by the ACMA on data collected and the general accuracy of AISI reporting
   - differences between the daily and repeated sightings reports and their purpose. While this information is covered in the current information provided, some AISI participants might not fully understand the parameters of each report
   - general information about malware, including the fact that different names are given to individual malware infections.

User-friendly information for small business and residential customers

6. Internet customers, who learn about computer compromises from their ISPs, might also find it useful to have a series of FAQs or other presentation of information to which they could refer. The focus might be to help:
   - deal with customer uncertainty, frustration and suspicion about the legitimacy of ISP notifications, how the information about compromised computers is gathered, and how customers can confirm the source of notifications
   - customers learn about the consequences of malware infections and how they can best protect their computers.

AISI online portal for additional information

7. Business clients often use a single IP address to enable internet access for multiple computers. When they receive an AISI report from their provider, they can sometimes have difficulty matching the reported compromises with specific computers on their network. Similar difficulties can also occur where providers utilise dynamic IP addresses for individual customers. These difficulties are experienced by businesses and providers who do not have the analytical or network monitoring software that can match the IP addresses in AISI reports with specific computers or customers. Additional information focussing on the needs of these AISI participants would be useful where available.

8. More comprehensive information about computer compromises—such as multiple sightings of a given IP address over a 24-hour period—will be provided through an online self-serve portal that is currently under development by the ACMA. AISI

participants would be able to search the relevant databases for extra information that could help them identify the particular computers that have been compromised. The portal will also allow providers to more readily tailor compromised computer reports to their specific needs. The availability of a portal for this purpose would not impact on the current reporting of compromised computers to participants.

9. The portal could be a resource for AISI participants that also links to other information identified in the research as being of value to AISI participants and their customers. This includes information from CERT Australia[8] about how to report cyber security incidents, the educational material on cyber security for internet users that is provided on the Australian Government's website www.staysmartonline.gov.au, and the educational information provided by the ACMA for children, parents, carers, teachers and library staff at www.cybersmart.gov.au.
10. In a similar way, information links could be provided through the portal about the industry icode and its coverage of strategies that might be adopted to protect customers and networks from malware and e-security threats. In this way the portal could assist AISI participants to conveniently access information about malware and related issues.

Enhanced engagement with AISI participants

11. Subject to resource availability, it may be useful for the ACMA to more regularly engage with AISI participants and more actively encourage feedback about the program. As with the ACMA's current emails to participants, this might include the provision of news and information items and an invitation for comment on current AISI activities. Simply and attractively presented, such engagement might promote wider sharing of experiences between providers. Such engagement could promote the provision of extra information to AISI participants and reinforce an open line of communication. It could also be an opportunity to update provider contacts.

Further research

12. Further research may be useful to better estimate the size of the compromised computer problem that affects internet users in Australia. This cannot be determined from AISI data because many of the reported AISI cases can relate to one customer and many IP addresses can have thousands of customers connected. In addition, the AISI program does not identify all forms of compromises, and the amount of compromises not reported through the AISI is unknown.
13. Given that Australians of all ages and other demographics are now using the internet in many aspects of everyday life, the ACMA is undertaking research to establish the Australian community's understanding of malware threats, their use of protections against harmful software, and reasons for not using or updating anti-malware software. This research is expected to be published in late 2012.

[8] CERT Australia is Australia's official national computer emergency response team (CERT). It is provides access to information to help protect Australians and Australian businesses against cyber based threats and vulnerabilities.

Attachment A: AISI information for participants

The ACMA's Australian Internet Security Initiative—Information for ISPs

This document is intended for Australian internet service providers (ISPs) currently participating in the Australian Internet Security Initiative (AISI) and for Australian ISPs who may be considering joining the AISI. It provides some general information on:

- the objectives of the AISI
- the types of compromise reports identified through the AISI
- suggestions about interacting with customers on individual AISI reports
- some of the methods used to detect activity in AISI reports.

This document is regularly updated as new compromise types emerge and are added to the AISI.

General information on 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 to be controlled remotely for illegal and harmful activities.

While most anti-bot initiatives focus on combating 'botnets' (aggregations of compromised computers) by disabling their command and control or domain names, the AISI is focused on home and small business internet users whose computers are surreptitiously hijacked to send spam or steal personal information and login credentials. Most of these users are connected to the internet via broadband services.

Through the AISI, the ACMA collects data from various sources about computers that are exhibiting 'bot' behaviour on the Australian internet. Using this data, the ACMA provides daily reports to ISPs and universities identifying IP addresses on their networks that have typically been reported 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 the ISP contacts the customer.

The reports are provided in a plain text format that is easily parseable, including information on the IP address, timestamp and type of compromise identified. The IP address and timestamp should enable ISPs to identify the customer associated with the compromise at a given point in time.

When an AISI report is received, ISPs are expected to contact their customers to advise them that their computer appears to be compromised, and to provide them with information to assist them in addressing the problem. ISPs currently participating in the AISI have informed the ACMA that when contacted, their customers are generally unaware their computer has been compromised and are grateful that their ISP has informed them of the problem.

A trial of the AISI commenced in November 2005, and it has been running successfully since that time**.**

Why participate in the AISI?

Participating in the AISI allows you to assist your customers by providing them with advice that their computer appears to be compromised, thereby giving them the opportunity to remedy the situation. It also contributes to the overall security of the Australian internet by disinfecting computers that damage this security. The problems associated with compromised computers and botnets are many and varied; including:

- **identity theft**: the malware installed on the customer's computer potentially may extract personal information, such as internet banking passwords and login information, for criminal usage
- **Distributed Denial of Service (DDoS)** attacks on websites, which may render the website inoperable during the attack
- **dissemination of spam:** over 90 per cent of spam is now sent from compromised computers
- **dissemination of malware,** which is either embedded in the spam sent from botnets, or through directing spam email recipients to websites where malware is downloaded onto their computer
- **hosting of illegal content** on a compromised computer**,** such as child pornography.

Through participating in the AISI, you will contribute to the overall reduction of spam and e-security compromises, thereby reducing costs for all ISPs and internet users. AISI participants are listed on the ACMA website unless they request not to be listed. The current list of participants and some general information on the AISI is provided at www.acma.gov.au/aisi.

The AISI and the IIA's icode

In June 2010, the Internet Industry Association of Australia (IIA) launched a voluntary ISP code of practice The 'icode', aimed to promote a security culture among the internet industry by reducing the number of compromised computers in Australia. It is designed to provide a consistent approach for Australian ISPs to help inform, educate and protect their customers in relation to cyber security risks.

The icode encourages all Australian ISPs to participate in the AISI and to take steps to respond to AISI reports. It can be accessed at: www.iia.net.au/userfiles/iiacybersecuritycode_implementation_dec2010.pdf

The icode commenced operating on 1 December 2010 and the associated website is at www.icode.net.au. The website provides information on the icode, a list of current participants, advice on avoiding infections and how to obtain professional help to address a compromise.

What information do I need to provide to the ACMA if I decide to participate in the AISI?

If you decide to participate in the AISI, the ACMA will require the following information:

- your IP address ranges (preferably in CIDR format)
- an email address to send the daily AISI email reports to (ideally the email to send reports to would be a generic address that does not need to change if there is a change in personnel responsible for managing the reports)
- a direct contact number(s) and email address to discuss technical or operational matters concerning the AISI
- your Autonomous System Number (ASN) (if applicable)—this helps the ACMA confirm that there are no errors in the IP range information provided
- the name by which you want your company to be listed on the ACMA webpage and in the ACMA's publicity about the AISI.

How many individual compromise reports will I receive daily?

The number of compromises listed in the daily AISI reports will depend on your customer base and the quantity of the information feeding into the AISI on a given day. For example, ISPs with a large customer base are currently receiving hundreds of compromise reports per day, whereas ISPs with a very small customer base may rarely get any reports.

In the 2011–12 financial year, on average 16,517 reports per day were collectively provided to ISPs.

In some cases it may be possible to tailor the daily AISI report for the particular requirements of your IT system. Please contact us (details below) if you would like to discuss this matter.

What information should I provide my customers about the compromise?

It is recommended that you contact your customers and advise them:

- that their computer appears to be compromised, with information on how such compromises can occur and the possible consequences of not addressing the compromise (some examples of these consequences are provided in the section above which discusses the problems with compromised computers)
- that to protect others and to avoid network disturbance they need to rectify the problem as soon as possible
- of the steps they may take to fix their current problem
- of the steps they may take to help secure their computer for the future (for example, firewall, anti-virus software, regular security patches).

General information on how to prevent and respond to malware infections is provided at www.staysmartonline.gov.au/

Some ISPs immediately reset their customer's internet access password when they are reported with an AISI compromise. The customer is then required to talk to a customer service operator to obtain advice on how to fix their problem. Depending on your particular circumstances you may wish to consider this approach, or potentially consider it in the case of 'repeat offenders'—that is, customers who have been identified with a compromise that appear to have either taken no remedial action or to have continued the practices that led to the compromise occurring (such as visiting 'suspect' websites).

Section 6.3 of the icode also proposes a range of actions that ISPs can take when they become aware of a compromised computer on their network.

- **Trojan: Gozi:** Gozi targets bank accounts, and has features that allow it to, in some cases, defeat internet banking security measures such as two-factor authentication and one-time passwords. It can use HTTP, or more commonly in recent times, HTTPS for its C&C. Some known variants stop the Windows firewall and security centre services. There are many variants.
- **Trojan: Goldun**: Goldun acts as a HTTP and SOCKS proxy and has a backdoor for command and control. The proxy ports, uptime information, and whether or not it has detected PayPal, eBay or eGold accounts are sent to a web server via a GET request.
- **Trojan: Beagle/Bagel**: Beagle is a worm with many variants. It may spread by mass email or peer-to-peer file transfer, and may open a backdoor.
- **Trojan: Xarvester**: Xarvester is a spamming botnet which 'phones home' via HTTP. It uses a kernel-mode rootkit including its own TCP stack and as such may be difficult to detect on the infected computer.
- **Trojan: Sality**: Sality is a bot that uses a UDP-based (using random ports) peer-to-peer protocol to distribute lists of HTTP URLs (which may, in turn host lists of URLs) to download other malware with more specific functionality. It can infect executable files on disk and inject code into already-running processes. It is capable of running with full functionality even when Windows runs in safe mode. It may add registry entries that configure the Windows firewall to permit traffic from/to infected executables.
- **Trojan: Lethic**: Lethic is a spambot that may attempt to connect to its controllers via various TCP ports such as 1430 and 8090. It starts via the Winlogon and Run registry keys.
- **Trojan: Stormworm**: Storm has spam and DDoS capabilities. Earlier generations of Storm usually have executables named with a prefix and sequential number, such as 'game0.exe' 'game5.exe' and use the eD2k (aka eDonkey) peer-to-peer protocol for C&C. The most recent known generation may run as 'asam.exe' and uses HTTP for C&C.
- **Trojan: Mydoom**: Mydoom is a worm that spreads via email messages that look like 'bounce' messages, but contain an executable attachment. A backdoor is opened on TCP port 3127. Although this worm was originally released in 2004, it was resurrected in 2009 with a new variant which also aims to prevent the downloading of Windows and antivirus updates.
- **Trojan: Grum**: Grum spreads via spam (one known subject line is 'Hot Pictures of Britney Speers') with links to 'drive-by-download' sites which exploit a Windows vulnerability to infect WINLOGON.EXE with code to turn the machine into a spam bot. HTTP traffic is used to 'phone home' and inform the botherder of the machines (in)ability to send spam. A rootkit attempts to mask the infection.
- **Trojan: Festi**: Festi is a bot using a kernel-mode rootkit. It 'phones home' for instructions and may modify Windows firewall settings to permit inbound connections.
- **Trojan: Waledac**: Waledac is a spambot which harvests email addresses from your computer and uploads them to the botnet controller. When instructed, it will send spam containing a URL at which a copy of the worm is hosted with the aim of infecting the recipient of the message. The message subjects often refer to upcoming holidays (e.g., 'Merry Christmas wishes just for you'), current world events (for example, 'Breaking news about our president-elect') or some unspecified news ('Awful news') to tempt the recipient to open it. Waledac has also been part of the payload of some variants of Conficker.
- **Trojan: Zapchast, Trojan: Reposin**: Zapchast (sometimes identified by one of its aliases, Reposin) is a botnet that communicates using IRC. It is run on startup via the 'Run' registry key. Up-to-date anti-virus software can remove known variants but new variants continue to be discovered.

What do AISI reports look like?

AISI reports are emailed to ISPs with AISI data formatted into columns. Attached to the email is a .txt file which is tab delimited for machine processing.

An example of a daily AISI report for 'DEMO ISP' is below:

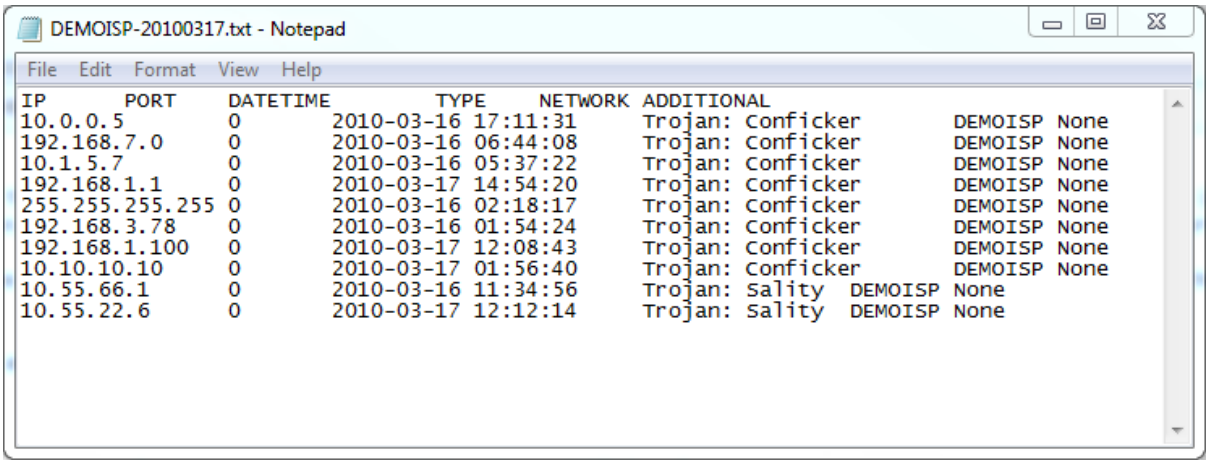
```
Dear DEMOISP Support,
This report is generated by the Australian Communications and Media Authority's
Australian Internet Security Initiative (AISI) service.
Below is today's list of open, compromised and malware infected hosts on your
networks.  For help interpreting this report, please contact
<aisi@aisi.acma.gov.au>.

All URLs contained within the report should be treated as hostile and capable of
infecting a user with malware without their knowledge.  As such http:// has been
replaced with hxxp:// to prevent against accidental infection.

Please note, all timestamps are relative to Coordinated Universal Time (GMT+0)

--- Report follows ---

IPv4 address     Timestamp            Type                 Network    Additional
10.0.0.5         2010-03-16 17:11:31  Trojan: Conficker    DEMOISP    None
192.168.7.0      2010-03-16 06:44:08  Trojan: Conficker    DEMOISP    None
10.1.5.7         2010-03-16 05:37:22  Trojan: Conficker    DEMOISP    None
192.168.1.1      2010-03-17 14:54:20  Trojan: Conficker    DEMOISP    None
255.255.255.255  2010-03-16 02:18:17  Trojan: Conficker    DEMOISP    None
192.168.3.78     2010-03-16 01:54:24  Trojan: Conficker    DEMOISP    None
192.168.1.100    2010-03-17 12:08:43  Trojan: Conficker    DEMOISP    None
10.10.10.10      2010-03-17 01:56:40  Trojan: Conficker    DEMOISP    None
10.55.66.1       2010-03-16 11:34:56  Trojan: Sality       DEMOISP    None
10.55.22.6       2010-03-17 12:12:14  Trojan: Sality       DEMOISP    None
```



This .txt file contains one header row, followed by one or more data rows. All fields in this file are delimited by a single tab character. Please note there is an additional field (Port) in the .txt file that does not appear in the AISI email report. This column is currently unused.

Weekly 'repeated sightings' reports

In addition to daily AISI reports, the ACMA also sends a weekly repeated sightings report in order to assist you to identify high-priority/recurring compromises on your network. This report covers the previous 14 day period.

In order to avoid reporting compromises that have potentially already been resolved the repeated sightings report details compromises sighted for ten days or more out of the previous 14 day period, and which have been sighted once or more in the last three days. The reports are sent every week, so the period of one report overlaps the period of the next.

The subject line of these reports has the form:

"[YYYY-MM-DD] - repeated sightings report mailing for $ISPNAME - $NUM host(s) detected [SEC=IN-CONFIDENCE]"

where:

* YYYY-MM-DD is the date, for example: '2009-09-01'
* $ISPNAME is the full name of your ISP, as supplied to us
* $NUM is the number of compromises in the report

The columns used in the reports are (in order, from left to right):

* IP address
* Timestamp of earliest sighting (min timestamp)
* Timestamp of most recent sighting (max timestamp)
* Number of days on which the compromise has been reported
* Compromise type (as per current daily AISI reports)

Note that the 'earliest sighting' reported is within the scope of the previous 14 days.

The compromises are listed in descending order of priority and days reported, that is, highest priority compromises and highest number of days reported appear toward the top.

As with the daily AISI reports, the attached .txt file will contain one header row, followed by one or more data rows. All fields in this file are delimited by a single tab character.

By default, these reports will be mailed to the address which currently receives the daily AISI reports. If you would prefer them sent to another address, or need any assistance interpreting this report, please drop us a line at aisi@acma.gov.au.

Technical information on compromise types contained in the AISI reports

Below are a number of commonly reported compromise types, however, new types may appear at any time depending on enhanced detection or new botnets arising.

> **MALWARE SERVING HOST**: although rarely identified, these reports appear at the top of the daily list as they are considered to be in need of rapid action. As the name suggests, these IP addresses have been identified as hosting URLs that are serving malware. For these reports, the 'Additional' column contains the URL that has been identified as serving the malware. Often many URLs originating from the same IP address will be identified in the report.

  If you receive one of these reports, the ACMA recommends that you advise your customer that their page has been modified to include a malicious link or a 'drive

by download' frame. Compromised webpages often contain either obfuscated javascript or in rare cases, a plain html IFRAME tag.

- **Rootkit: TDSS:** TDSS is a rootkit that is used to hide other malware. It is a particular type of rootkit known as a 'bootkit', as it infects the Master Boot Record (MBR) and therefore is the first piece of software loaded and executed from the hard disk by the BIOS, before the operating system, whereupon it hooks BIOS disk I/O calls (INT 13h). It has its own file system which is encrypted and stored toward the end of the hard disk. It has kernel-level hooks that prevent the MBR and hidden file system from being read from within Windows. Depending on the variant, it may access a HTTP C&C independent of the C&C of the malware it is being used to hide. Kaspersky's TDSSKiller is able to detect and remove some common variants.
- **Trojan: MEBRoot**: MEBRoot is often coupled with the 'Torpig' or 'Sinowal' trojan. MEBroot is a trojan best known for stealing online brokerage logins and hiding in the Master Boot Record of the host system. Due to the trojan being loaded on boot and advanced rootkit functionality we recommend scanning from a clean environment (such as a rescue CD or USB stick). The more recent 'TDSS' rootkit uses similar techniques, and as such, Kaspersky's TDSSKiller is able to detect and remove at least some known variants of MEBroot.
- **Trojan: Clampi**: Clampi is a 'dropper'; it connects to one of a list of remote sites to download a more specific malware component.
- **Trojan: Silon**: Silon uses a 'man in the browser' type technique to inject code into banking website login forms and then transmit the captured credentials to URLs listed in a registry key that is unique per machine. Silon's code is loaded into the iexplore.exe process from C:\Windows\System32\msjet51.dll.
- **Trojan: Spyeye**: Spyeye shares many similarities with Zeus and is able to steal web form inputs, email, credit card details, as well as passwords used over HTTP, POP and FTP. It uses HTTP for C&C and (like Zeus) does so via a URL whose filename component often is 'gate.php'.
- **Trojan: Cutwail(2),Trojan: Pushdo**: Pushdo is a 'dropper' which uses a kernel-mode rootkit to download various malware components including Cutwail, a spambot. The driver which is used to load the rootkit is specified in the registry, but the rootkit, once loaded, hides its files and registry keys from view as well as those of its components. It uses Internet Explorer (hiding the process from view of diagnostic tools) to download updates for itself over HTTP from one of several different hosts from a list which is periodically updated. The HTTP request used to retrieve the updates is a HTTP/1.0 GET request, with the location part consisting of a long hexadecimal string. Pushdo is believed to propagate via drive-by-download and via dropping by other malware.
- **Trojan: Rustock**: Rustock is a spambot that uses a kernel-mode service executing in services.exe. It downloads encrypted spam templates via HTTP URLs with PHP files and random strings of numbers. It may also download random Wikipedia articles in order to include text from the articles to confuse anti-spam detection engines.
- **Trojan: Delf.HPT**: Delf.HPT is a dropper which connects to remote sites to download more malware. It drops a file called sxserv101.exe and attempts to issue a HTTP POST to http://74.208.64.191/hk1xx/getconf.php.
- **Trojan: Delf.FZ**: Delf.FZ creates a number of .exe files on the infected system and connects to a number of remote URLs, some of which have a path component of '/surf/stat.php?uin=[string of numbers]'. It has an adware component and is also a malware dropper.
- **Trojan: Zeus**: Zeus is a keylogger that is able to steal internet banking details. It uses a rootkit to attempt to avoid detection. It uses a HTTP C&C that typically has the filename part of 'gate.php'.

- **Trojan: Cimbot**: Cimbot is a spambot which communicates with its controller using HTTP. The commands are encoded in what appear in protocol analysis to be GIF files.
- **Trojan: Iflar**: Iflar connects to a HTTP server and downloads a new copy (if there is a newer one available) of itself along with data for constructing spam messages, which it then sends.
- **Trojan: Maazben**: Maazben effectively turns the computer into an anonymous open relay. Some variants use the default mail client to send mail rather than using an SMTP engine of their own. It checks itself against several blacklists before sending spam. It may also contact various HTTP servers for updates and open a backdoor on a random TCP port.
- **Trojan: Gheg**: Gheg is a spambot that uses HTTPS to communicate with its controller. It configures the Windows firewall to allow itself through and modifies the registry so that it runs on startup (via Winlogon and run keys).
- **Trojan: Netsky**: Netsky is a worm that propagates via email, attaching itself to messages it sends to addresses found on the computer. The messages have various fraudulent inducements for the recipient to open the attachment, for example, that it is an important document, the recipient's computer is infected and must be cleaned with the attachment.
- **Trojan: Donbot**: Donbot is a spambot that connects to its controller on random TCP ports above 2200. It can send spam not only via SMTP, but also Twitter. The executable is typically C:\Windows\System32\sysmgr.exe which is added to the run registry key so that the bot is executed on startup. Donbot has been known to be dropped by worms exploiting Windows vulnerabilities.
- **Trojan: Darkmailer**: Darkmailer, AKA YellSoft Direct Mailer, is a mass-mailing web application with features designed for spammers. It is often installed on compromised webservers and by default has the filename 'dm.cgi' although it is frequently renamed.
- **Trojan: Dlena**: This family contains many variants; most of the known variants are stored in C:\Windows\System32\rpcc.dll which is loaded as a network service on startup via modifications to the registry, and enable use of the infected computer as a HTTP proxy server and a spambot.
- **Trojan: Bobax**: Bobax modifies C:\Windows\System32\drivers\etc\hosts to make various anti-virus update sites unreachable. It communicates with its controller using HTTP from which it is given instructions to send spam. It propagates via LSASS vulnerability in Windows.
- **Trojan: Asprox:** Asprox permits the machine it is installed on to be used as a proxy server. It typically listens for requests on port 80 or 82, and is installed to C:\Windows\System32\aspimgr.exe.
- **Trojan: Fivetoone**: Fivetoone, also known as DMSpammer, communicates with its C&C server via HTTP, which sends it information for carrying out spam campaigns. It installs kernel mode drivers at C:\Windows\System32\hdfile.sys and C:\Windows\System32\hdport.sys. The user mode program is typically installed at either C:\Windows\System32\qtplugin.exe or C:\Windows\System32\services.exe.
- **Trojan: Avalanche**: Avalanche is a spamming botnet and phishing reverse-proxy. It listens on port 80 for HTTP requests which it proxies to the actual phishing web host. It is installed to C:\Windows\System32\sysservice.exe and loads C:\Windows\System32\sysservice.dll. It runs via the registry key HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run.
- **Trojan: Conficker**: Conficker is also known as Downadup. This identifies a machine seen connecting to a Conficker sinkhole. Anti-botnet organisations have purchased a number of domains used by Conficker for command and control, and have pointed these domains at 'sinkhole' servers. These servers then log the connecting IPs and report them to the ACMA. The only real chance of a false

positive in this case is if a user has attempted to access the botnets coordination servers. This is unlikely as there are no actual 'pages' live on these servers; they talk in an XML variant via port 80.

- **Trojan: Ponmocup**: Ponmocup modifies the Windows hosts file (C:\Windows\System32\drivers\etc\hosts) in order to direct traffic intended for particular websites elsewhere, or effectively disable them. It uses a HTTP C&C mechanism; known URLs contain very long hexadecimal strings.
- **Trojan: Ramnit:** Ramnit is known to evade firewalls and other detection mechanisms by injecting itself into running processes, such as svchost.exe and iexplore.exe. It may modify the registry to ensure that it starts on boot. It uses a custom protocol on TCP port 443 for C&C.
- **Trojan: Artro:** Artro, also known as CodecPack, can be distributed by many methods; known methods include the use of browser security exploits, posing as a 'legitimate' executable, such as a software license key generator ('keygen') or audio-video codec pack, and installation via another botnet that the machine is already a part of. Artro uses HTTP for C&C; requests and responses are base64-encoded and RC4-encrypted. Typically, the bot is instructed to download and execute further malware- adware/clickfraud, and sometimes more bots.
- **Trojan: Carberp:** Carberp adds itself to the current user's startup directory, hides itself using rootkit techniques, attempts to disable a wide variety of anti-virus software, and steals passwords for many different applications, using HTTP for C&C.
- **Spam Sender**: An IP address reported as a Spam Sender has connected to a spamtrap and submitted mail to it, which has then been submitted to the ACMA's Spam Intelligence Database (SID). A description of spamtraps is provided in the section on detection methods below. For this type of compromise, the number of messages submitted that were sent by the reported IP address over the 24-hour time span of the query to SID is supplied in the AISI report, for example, 'Messages reported: 102'. Redacted versions of the spam messages relating to these reports may be made available to ISPs on request.
- **Spam Sender—SendSafe**: An IP address reported with this compromise type has been detected to have sent spam to spamtraps where the operators of the spamtrap have fingerprinted it with particular characteristics of mail sent by SendSafe, a bulk email software package. In such cases, the ACMA receives reports from the source indicating this compromise type, rather than having the spam messages submitted to SID.
- **Fast Flux**: Fast Flux entries are IP addresses which are pointed to by a rapidly changing domain (these reports are currently quite rare). These 'fast fluxing' domain names are typically used by bulletproof hosting services to make it difficult for e-security and anti-spam organisations to get all of the hosting servers shut down. Fast Flux is typically used to host content like phishing sites and child pornography. Reports of Fast Flux in the AISI typically include a URL that has pointed to the reported IP address in the last 24 hours. A trojan horse and a web server will generally be found on the infected computer and require removal as per any other trojan compromise.

  There is a chance of a 'false positive' in Fast Flux, as the bulletproof hosting organisation may be pointing a domain name to an address that no longer belongs to the trojan infected machine. However, we are unaware of any instances of this occurring in the AISI data to date.
- **Trojan: Spyeye**: Spyeye shares many similarities with Zeus and is able to steal web form inputs, email, credit card details, as well as passwords used over HTTP, POP and FTP. It uses HTTP for C&C and (like Zeus) does so via a URL whose filename component often is 'gate.php'.
- **Trojan: Gbot:** Gbot modifies the registry in multiple locations to ensure that it runs when the system boots. Known locations that it may use include

HKML\SOFTWARE\Microsoft\Windows\CurrentVersion\Run, HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows\Load, and HKCU\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell. It configures itself as a HTTP proxy via HKCU\SoftwareMicrosoft\Windows NT\CurrentVersion\Internet Settings\ProxyServer. Gbot makes HTTP requests to pages that return a 404 status, but may still log system information sent to them.

- **Trojan: Oddbob**: This worm spreads via Windows vulnerabilities in the LSASS and RPC subsystems.
- **Trojan: Ozdok**: Ozdok is a spamming botnet which infects computers via 'drive-by-download' on websites.
- **DDOS Drone**: A DDOS Drone is typically reported by sources which provide DDOS detection and mitigation services to their customers; the IP address reported has been detected as having participated in a DDOS attack. While some DDOS attacks may be willingly participated in by customers, generally, they will have been initiated by a botnet, and the malware may be detected as per 'Trojan: Generic' as described below.
- **Trojan: Dirtjumper**: Dirtjumper is a DDOS bot that uses HTTP for C&C communications. It polls the C&C server for instructions and can be returned a list of URLs to attack, in plain-text. The bot's executable file may begin with 'svd', but not necessarily. The file C:\WINDOWS\syskey2i.drv, which contains a numerical per-bot ID, may be present. Up-to-date antivirus should detect Dirtjumper, though possibly under synonyms, or generic malware categories, like 'Downloader'.
- **Trojan**: **DNSChanger**: DNSChanger refers to a class of malware that modifies the settings of an infected computer so that it uses DNS servers that are associated with the malware publisher as its local nameservers. These DNS servers return IP addresses of webservers also associated with the publishers of the malware, so that they may potentially log web browsing, steal login credentials, return fraudulent content for a given URL or otherwise interfere with web content requested from an infected computer. Infection by currently known variants can be confirmed by examining the configured DNS servers in the TCP/IP properties or 'ipconfig /all' and comparing to the known-correct settings of the ISP and/or LAN. Some DNS servers that have been used for this purpose are being sinkholed in order to identify IP addresses used by infected computers.
- **Trojan**: **Virut**: Virut refers to a family of file infecting viruses that target and infect .EXE and .SCR files on the compromised system. The malware contains an IRC-based backdoor that provides unauthorised access, file download and remote execution capabilities on the infected system. As of April 2012, typical infection symptoms include an increase in file size of infected files with recent modification date and possible execution failures, as well as network traffic on TCP 65520 with connections to IRC server proxima.ircgalaxy.pl, on channel #virtu.
- **Trojan: Kelihos**: Kelihos is a spambot. It may install WinPcap, a kernel-mode driver for capturing network traffic. If so, the files packet.dll, wpcap.dll and drivers\npf.sys will be found in C:\Windows\System32, though if the computer legitimately had WinPcap installed, for example, for Wireshark, this would not indicate a compromise. Known variants add a value named 'SmartIndex' to HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run in order to ensure the bot starts when Windows does.
- **Suspicious URL**: Suspicious URLs are URLs that have been identified as hosting or being involved in activity such as phishing, malware hosting, browser exploits, drive-by-download, and a more specific description of that activity is not available from the original source report**.**
- **Trojan: Flashback:** Trojan Flashback affects OS X based computers. It uses a Java vulnerability to infect the system. No user interaction is required other than visiting a compromised website. The Trojan uses HTTP to communicate with the C&C and includes the Apple unique hardware id in the communication to

differentiate itself from other bots. Apple released a fix for Java on 12 April 2012 and a free Flashback removal tool through the Software Update Application in OS X. The reported harmful consequences of Flashback include the harvesting of personal information provided through web browsing activities, including usernames and passwords.

- **Trojan**: **Feodo**: Feodo is a banking trojan similar in operational features to Zeus, SpyEye, Bugat or Carberp. Feodo hooks into web browser processes and monitors active sessions for accessed URLs matched against a list of target URLs from its configuration file. Captured form data is then transmitted to a C&C server. The trojan is capable of injecting rogue forms in order to trick the victim into providing more information than requested by the original legitimate form. Feodo targets not only banks but also a number of additional online services like Paypal, Amazon, MySpace or Gmail.

Information on some methods used to detect activity reported in the AISI

The ACMA obtains data on compromised IP addresses from a variety of sources. These sources, some of which are confidential, are continually updated and new sources added. The ACMA's experience with the AISI is that over time, some detection methods become outdated and are superseded by new sources with alternative ways of detecting compromises.

Occasionally multiple instances of the same IP address will be identified in the reports, with a different compromise type identified in each instance. This is generally because different sources have identified activity originating from this IP address.

The ACMA is always interested in receiving information about potential new feeds of data for the AISI, and would welcome any suggestions of potential new sources. (New feeds are rigorously tested before being integrated into the daily AISI reports.)

The original sources of data fed into the AISI detect the activity reported using a variety of methods. Some of those methods are as follows:

- **Sinkholes:** If a family of malware is known to send traffic to a particular domain name (such as that of the C&C server), it may be possible for a security monitoring and reporting organisation to, with co-operation of the domain registry and/or registrar, obtain control of the domain name. The organisation can then log data relating to the traffic they receive that is destined for that domain name and report this data to relevant parties such as the ACMA. Conficker is an example of malware that is tracked with the use of sinkholes.
- **Honeypots**: A honeypot is a machine that appears to have security vulnerabilities, to encourage attackers to attempt to break into it. For example, a honeypot may send a server header as part of a HTTP response that indicates it is running IIS 4.0, when in fact it is the webserver component of a honeypot software suite. The details of the attempted attacks are logged and reported.
- **Spamtraps**: A spamtrap is a mailbox, or more typically, entire domain or mailserver, to which legitimate mail is never sent, because the owner has never consented for mail to be sent there. Therefore, it can be inferred that mail that is sent there is spam. This spam sometimes contains anomalous properties (such as misspelt headers or mismatching identifiers) that indicate it was sent by a certain malware family.

Further information

More information on the AISI is available on the ACMA website at: www.acma.gov.au/aisi.

Once you have been receiving daily reports for a while, the ACMA may contact you to obtain information on issues relating to the reports, such as how customers are

responding to the advice you provide and any suggestions you may have to further enhance the initiative.

Please also remember to periodically provide the ACMA with updates to your IP address ranges.

For general enquiries about the AISI please contact the ACMA by email at aisi@acma.gov.au. Alternatively AISI staff can be contacted by telephone on the ACMA's spam/e-security general enquiries number: 1300 855 180.

Attachment B: Example of AISI daily report

Dear XXXXX,
This report is generated by the Australian Communications and Media Authority's Australian Internet Security Initiative (AISI) service.

Below is today's list of open, compromised and malware infected hosts on your networks. For help interpreting this report, please contact
<aisi@aisi.acma.gov.au>.

All URLs contained within the report should be treated as hostile and capable of infecting a user with malware without their knowledge. As such
http:// has been replaced with hxxp:// to prevent against accidental infection.

Please note, all timestamps are relative to Coordinated Universal Time (GMT+0)

--- Report follows ---

IPv6 address	Timestamp	Type	Network	Additional
XX2.XX.1XX.1	2012-08-08 21:28:18	Trojan: Zeus	ISPXXX	None
XX0.0.72.81	2012-08-08 0X:01:X7	Trojan: Zeus	ISPXXX	None
XX0.0.X1.X5	2012-08-08 21:05:XX	Trojan: Zeus	ISPXXX	None
XXX.2XX.X.7X	2012-08-07 15:X7:25	Trojan: Conficker	ISPXXX	None
XX2.XX.17X.1XX	2012-08-07 0X:1X:2X	Trojan: Conficker	ISPXXX	None
XX0.0.X7.57	2012-08-07 05:XX:2X	Trojan: Conficker	ISPXXX	None
XX0.0.71.10X	2012-08-07 01:01:00	Trojan: Conficker	ISPXXX	None
XX0.0.X1.X5	2012-08-07 0X:5X:0X	Trojan: Conficker	ISPXXX	None
XXX.2XX.10.220	2012-08-08 2X:X8:55	Trojan: Ramnit	ISPXXX	None
XXX.XX.178.2XX	2012-08-08 0X:5X:18	Trojan: Ramnit	ISPXXX	None
XX2.XX.18X.171	2012-08-07 07:X0:0X	Trojan: Flashback	ISPXXX	None

Attachment C: Example of AISI repeated sightings report

Dear XXXXXXX,
The following report lists compromises that have been reported 10 or more days over the last 14.
The list is sorted by 'Type' (in descending order from the most significant compromise type) the 'Days Reported' in descending order.

For help interpreting this report, please contact <aisi@aisi.acma.gov.au>

Please note, all timestamps are relative to Coordinated Universal Time (GMT+0)

--- Report follows ---

IPv6 address	Min Timestamp	Max Timestamp	Days Reported	Type
XX0.21X.XX.1XX	2012-07-15 11:X1:2X	2012-07-27 15:51:25	13	Trojan: Sality
XX0.21X.X2.X1	2012-07-16 1X:XX:5X	2012-07-28 1X:57:0X	13	Trojan: Ramnit
XX0.21X.12X.X5	2012-07-15 1X:00:2X	2012-07-27 0X:5X:2X	13	Trojan: Conficker
XX0.21X.XX.171	2012-07-15 17:X0:2X	2012-07-27 11:XX:00	13	Trojan: Conficker
XX0.21X.1XX.11	2012-07-15 05:X1:00	2012-07-27 10:XX:25	13	Trojan: Conficker
XX0.21X.10X.XX	2012-07-17 0X:XX:XX	2012-07-27 1X:X0:0X	12	Trojan: Ramnit
XX0.21X.5X.11X	2012-07-15 11:5X:2X	2012-07-27 0X:X5:2X	12	Trojan: Conficker
XX0.21X.0.255	2012-07-17 0X:2X:00	2012-07-27 11:X2:X7	11	Trojan: Generic
XX0.21X.10X.X2	2012-07-16 1X:51:XX	2012-07-27 1X:XX:XX	11	Trojan: Ramnit
XX0.21X.5X.XX	2012-07-18 17:1X:XX	2012-07-28 17:10:1X	10	Trojan: Ramnit
XX0.21X.12X.15X	2012-07-16 1X:1X:11	2012-07-28 1X:X7:57	10	Trojan: Ramnit
XX0.21X.1X.1XX	2012-07-17 01:0X:X2	2012-07-28 1X:17:X1	10	Trojan: Ramnit
XX0.21X.X0.1XX	2012-07-16 21:X1:57	2012-07-28 05:55:0X	10	Trojan: Ramnit

Attachment D: Research methodology and sampling

Methodology

Personal telephone interviews were conducted with 24 randomly selected AISI participants between 8 December 2011 and 2 February 2012. These 24 were selected from a stratified list of the 90 AISI members who received compromised computer reports from the ACMA in late 2011.

Although randomly selected, the sample size of 24 is too small to be statistically representative of all AISI participants. The results in this report provide an indication of how a broad cross-section of small-, medium- and large-sized internet providers and universities use the AISI reports.

Telephone interviews were chosen as the most appropriate research methodology because they allow for a detailed and comprehensive exploration of the research topics. This methodology was also chosen due to lessons learned from telephone and survey research that has previously been undertaken with AISI participants. An interview guide of the issues to be explored was developed to help capture the required information and to allow a flexible line of questioning. Three interviewers took part in teleconference calls for the first few interviews to ensure a common understanding of the research topics. Attachment E provides the interview guide used for this research.

Interviews were undertaken by ACMA staff in the Digital Society Policy and Research Section (DSPRS) with assistance from the E-Security Operations Section (EOS) who administers the AISI program. The initial research brief and issues covered in the interviews were developed in close consultation between DSPRS and EOS.

An email was sent to all AISI participants before the interviews commenced to provide information about the research and to foreshadow that some participants would be contacted for a phone interview.

Interviewees were predominantly from managerial and technical areas that had varying levels of knowledge about, and interactions with, customers. Many appeared to have a very good understanding of their customers but some were not involved with customers on a day-to-day basis. Each interview took approximately 20 minutes, and ranged from 15 minutes to as long as one hour.

Selection of interview participants

The AISI participants interviewed were selected randomly from a list of all AISI participants that was stratified to ensure coverage of small, medium and large ICT businesses, as well as universities.

Small, medium and large businesses were defined on the basis of the number of infections usually reported for each participant organisation (Table 1). A general assumption was been made by the researchers that the number of cases reported generally reflects the number of clients or customers and the general size of the provider organisation. Universities have been treated as a separate category and generally received less than 10 reports per day.

While the research findings are not representative of the issues faced and practices adopted by all AISI participants, they do cover the views of a broad range of AISI participants of different internet business types and organisation sizes across Australia. The organisations selected in the interview sample operate from most states

in Australia and the Australian Capital Territory (ACT), and include companies that provide national services. Table 1 also shows the number of providers interviewed compared with the AISI participants.

Table 1 Comparison of interviewed sample with AISI participants

Size of internet provider (categorised by the number of compromises reported per day)	AISI participants who received reports		Interview sample	
	Number	*%*	Number	***%***
Small (up to 20 cases reported per day)	45	*48*	10	***42***
Medium (21–599 cases reported per day)	24	*26*	7	***29***
Large (600–5,000 cases reported per day)	10	*11*	4	***17***
University (usually <10 cases reported per day)	14	*15*	3	***12***
TOTAL	**93**	***100***	**24**	***100***

Note: despite the random selection of the total interview sample, a sample of 24 is too small to be statistically representative of all AISI participants who received compromised computer reports. The results in this report provide an indication of how a range of internet providers used the AISI reports.

Attachment E: Interview guide

Personal telephone interviews—key issues and questions for the person who deals with the AISI reports
Telephone interviews will cover the following issues (along with sufficient probing in a way that is not leading, for example, do you use the reports in any other ways? Can you give me an example? Can you take me through that process?).

1. **Explore how each provider makes use of, and takes action on, the daily AISI reports provided by the ACMA**

   Examples of follow-up questions:

   > What information, advice and assistance is offered to customers (about compromised computers), if any?
   > Are processes automated?
   > What other data about compromised computers are used? How is that information used?
   > Why do you wait for multiple compromises to be reported in AISI reports before you take action?
   > Are there certain problems that you notify customers about, and others that you don't?
   > Does your approach vary with the severity of the compromises reported?

2. **Explore how each provider makes use of, and takes action on, the AISI repeated sightings reports**

   Then ask follow-up questions similar to question 1.

3. **Roughly estimate the proportion or percentage of daily reports and/or repeated sightings reports that are used to inform customers that their computer/s may be compromised**

   Examples of follow-up questions:

   > How often do you take action?

4. **Identify reasons for not using all or part of the data contained in the AISI reports, and what the reasons for non-use are**

   Examples of follow-up questions:

   > If participants say they cannot match the IP addresses in the reports with their customers: Why is that?

5. **Identify any additional information that the ACMA could provide to make it easier for participants to act on either the daily or weekly AISI reports?**

   > PROBE for details.
   > Ask for additional information that the ACMA or others could provide to make it easier for the provider/university to act on AISI reports. (For instance, there may be information provided by some other party—but not provided through the AISI—that would make it easier to action AISI reports).

6. **If customers are contacted about compromised computers, identify the types of feedback that providers receive from their customers.**

   Examples of follow-up questions:

   > How much customer feedback is received?

   > What is the nature of that feedback? Is it mostly positive or negative?

   > To what extent are problems fixed?

   > Do customers request more information? What type/s of further information do they request?

   > Do you have staff that are devoted to the customer service aspects of handling AISI reports?

   > Also query to what extent customers who are alerted to a compromise on their computer are unresponsive or resistant to advice from provider.

7. **Separate from any action that is taken on the AISI reports, what other activities are undertaken to detect and respond to malware-related threats to your network?**

   > For example, what monitoring activities do you undertake of your network (if any)?

   > Do you report malicious activity detected in your network to internal security or fraud control, or to any external authorities?

8. **Can you think of any improvements that could be made to the AISI program or to the compromised computer reports that it produces?**

   > PROBE fully for ideas and details about possible improvements.

9. **The AISI program is considering the introduction of a self-serve portal that providers could use to access reports and other information. What do you think about that idea?**

   > PROBE for details.

10. **Before we finish, is there anything else that you would like to add about the AISI program with regard to you or your customers?**

    > PROBE as necessary

For the ACMA's purpose only, record:

> name of contact, company or university

> whether small, medium or large company

> market focus, that is, residential and/or business.

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

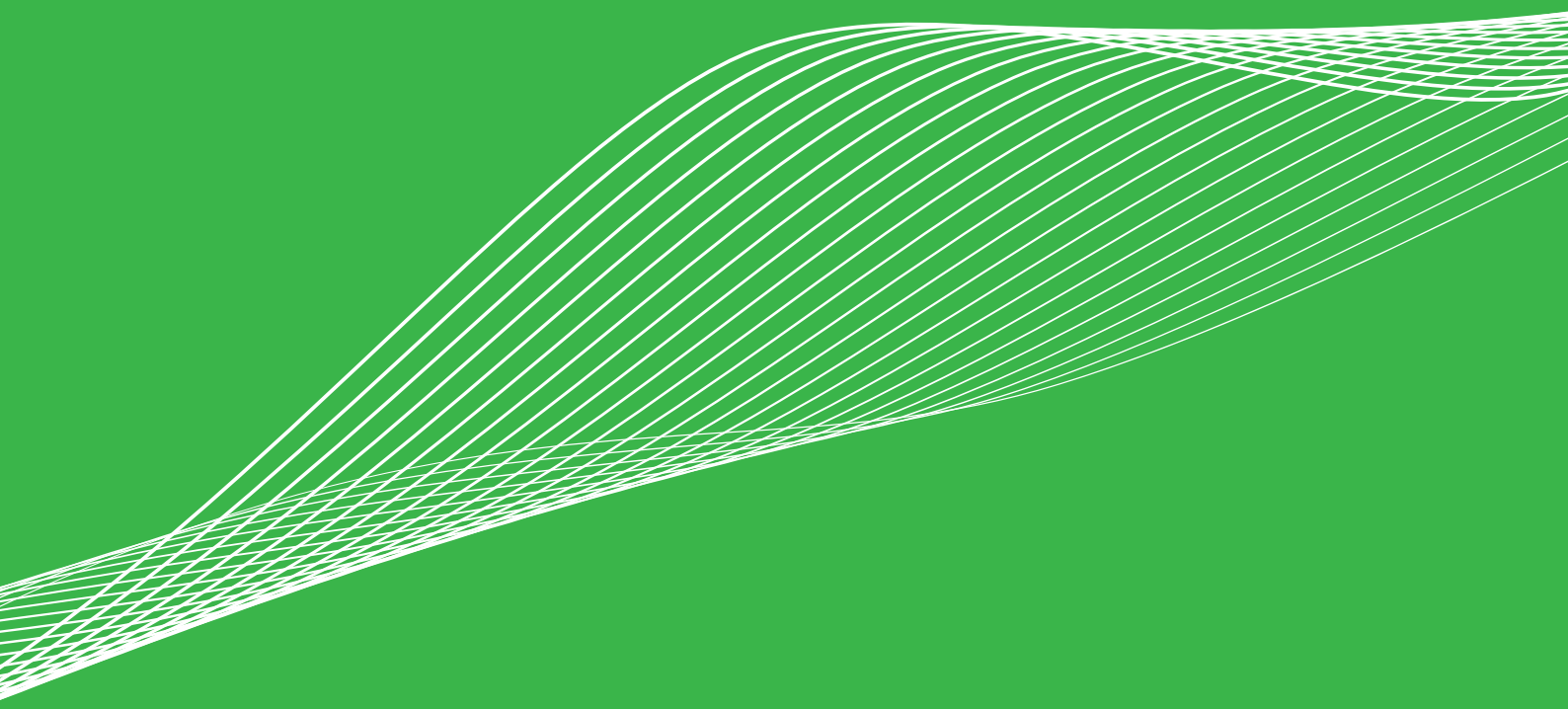
T +61 3 9963 6800
F +61 3 9963 6899

Sydney
Level 5
The Bay Centre
65 Pirrama Road
Pyrmont NSW

PO Box Q500
Queen Victoria Building
NSW 1230

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

acma research



acma.gov.au
engage.acma.gov.au