Australian Government

acma

Australian
Communications
and Media Authority

researchacma
Evidence
that informs

The Australian Internet Security Initiative

Interviews with industry participants

OCTOBER 2015

communicating
facilitating
regulating

Canberra
Red 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 32
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 or 1800 226 667
F +61 2 9334 7799

Contents

Contents (Continued)

Contents (Continued)

Executive summary

The Australian Internet Security Initiative (AISI) is a program operated by the Australian Communications and Media Authority (the ACMA) to help AISI participants address the problem of computing devices that are ‘compromised’ by malware (or malicious software). Malware infections enable cyber criminals and state-sponsored actors to steal personal and sensitive information from these devices and control them remotely for illegal or harmful purposes, without the users’ knowledge. These infections often undertake activities that cause harm to other internet users, including the mass distribution of spam, hosting of phishing sites and facilitation of identity theft.

When this research was undertaken, there were 137 AISI members—including 18 universities—participating in the AISI program. These members receive daily AISI reports identifying internet protocol (IP) addresses on their networks observed as having malware infections. Members can use the information in the reports to identify the relevant customer or user with the malware infected computing device and help that customer or user to resolve the problem.

The ACMA introduced an online AISI portal in 2014 that provides access to more information on malware incidents associated with individual IP addresses than is contained in the daily AISI email reports. AISI members can download their AISI data directly from the portal to either complement or replace the data received in the daily AISI email.

In March 2015, the ACMA began reporting internet services vulnerable to known ‘exploits’[1], expanding the focus of the AISI program to prevention as well as resolution of problems.

The ACMA undertook research with AISI members to help it:

> assess the effectiveness of the AISI program

> better understand the measures AISI participants use to help their customers resolve computer compromises

> identify additional information or assistance that participants consider would improve the program.

Personal telephone interviews were conducted with 24 randomly selected AISI participants between 23 February 2015 and 27 March 2015. These 24 were selected from a stratified list of 82 AISI members who had received AISI reports over the period of a few weeks in early 2015. This group was stratified into four subgroups to help ensure broad coverage of AISI members in this research.

[1] In this context, an exploit is a known vulnerability that enables a cyber-criminal to surreptitiously intercept or directly access an Internet connected service, potentially obtaining data and credentials that can be used to cause harm to the service owner or user.

Table 1: AISI participants interviewed—number interviewed in comparison to number of AISI members that received reports

Type of AISI member (by number of infections reported)	No. of completed interviews	Total no. of AISI members
Large ISP (600–5,000 infections reported per day)	5	6
Medium ISP (21–599 infections reported per day)	5	24
Small ISP (up to 20 infections reported per day)	9	39
Educational institution (usually <10 cases reported per day)	5	13
Total	**24**	**82**

Note: 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 internet providers and universities use the AISI reports. When observations about differences between the various types of internet providers are noted, as with the sample as a whole, these observations about subgroups should not be regarded as statistically representative measures.

Key findings

Participants' use of the AISI reports

AISI reports are the predominant source of data AISI participants use to identify malware-infected customers on their networks. For a third of the participants interviewed, the AISI reports are their sole source of information identifying customers with malware infections. With one exception, all small ISPs interviewed relied solely on AISI reports to identify their infected customers.

The majority of the AISI participants interviewed (22 of 24 participants) reported 'acting' on the daily AISI email reports. While the extent of action varies from occasional to daily use of AISI data, most use this data to help their customers in some way.

Participants' use of the AISI portal

Only a fifth of the participants indicated using the AISI portal (four large ISPs and one small ISP). Some participants were aware of the portal but did not require the additional functionality it provides, preferring to receive their AISI information solely by email. Overall, AISI participants appeared to have a low level of awareness of the portal's functionality and, in some cases, its existence. Based on these responses, the ACMA plans to work to improve the level of awareness of the portal and its additional functionality and benefits.

Current processes to deal with the data in the AISI reports

A third of the participants interviewed—mostly large and some of the medium ISPs—indicated having automated or semi-automated processes in place to deal with the data provided in the daily AISI report. (These processes enable a non-manual correlation of the IP address data in the AISI reports with the provider's customer information.) Two-thirds of participants—mostly small ISPs and educational institutions—currently process this information manually. Some of the participants interviewed, mostly medium ISPs, are considering developing automated processes. Educational institutions and small ISPs advised that manual processing of AISI data is not a problem for them, as they generally only receive a small number of reports.

Actions to inform and help customers deal with malware infections

AISI participants deal with the information they receive on malware infections affecting their customers, and provide support and assistance to them, in a variety of ways. The most common approach is to notify their customers of their compromise and advise how the problem might be resolved. This is usually achieved via an initial email, while some providers notify their customers by phone.

Participant responses on the extent of feedback received from customers about a malware infection report varied—some rarely receive feedback and others never receive feedback. This is especially true for those participants using an automated system. For those who do receive customer feedback, its nature is mainly positive—most customers appreciate being informed of their malware infection and the support provided by the ISP to address the issue.

Other sources of information about malware infections

While a third of the participants (seven out of 22[2]) rely solely on the AISI reports for information about malware infections, for two-thirds of respondents these reports are not the sole source of data to detect and prevent malware infections.

Utilising the data in the daily AISI reports does not present major difficulties, according to interviewed participants. Many have integrated the reports into their internal systems and automated processes, showing the importance of keeping report formats consistent. When asked about possible improvements to the AISI program, participants mentioned the provision of more detailed information and changes to how it is delivered, to either facilitate automated systems or improve customers' direct access to information on malware infections. One large provider suggested that the delivery of the AISI information be enhanced to enable customers to directly access information about their malware infections.

Changes to cybersecurity and related customer assistance in the last two to three years

Most participants have undertaken continuous changes to or refinements of their system in the past two to three years, since the previous AISI research undertaken in 2012. A quarter of participants indicated there had been no changes, while four participants had started using the AISI reports and were positive about them. One ISP said:

> Before the AISI, we didn't have anything in place; we dealt with problems on [a] case-by-case basis; and we did this only if a customer brought a problem to our attention.
>
> The AISI is great for us because we can help our customers. (Small ISP)

Another small ISP said:

> We are now using AISI, and because we use AISI we now have a policy to detect and prevent malware and botnet viruses. Previously to receiving the AISI reports, we were just monitoring high upload usages on the customer network.

Reporting significant cybersecurity risks to external authorities

All of the large ISPs interviewed have regular to occasional contact with CERT Australia (Australia's national computer emergency response team). However, medium and small ISPs, and education institutions, have limited contact with

[2] Out of the 24 ISPs interviewed, two mentioned not currently receiving the AISI reports.

government organisations and are uncertain about which is the appropriate organisation to whom they should report cybersecurity incidents.

Organisations mentioned as appropriate to report cyber incidents to include AusCERT (a non-government organisation), the Attorney General's Department, the Australian Federal Police, the Australian Security Intelligence Organisation and the ACMA. Most participants, however, consider they have not had a need to report any incidents.

Participants interviewed suggested possible improvements in how government helps providers and customers with malware infections. Some large ISPs commented on the need to consolidate the number of agencies dealing with cybersecurity. Other suggestions were about providing and sharing information on malware infection threats for industry and education programs for citizens.

Conclusion

Based on the interviews conducted for this research, participant ISPs value the AISI highly. While a number of possible improvements are suggested, which the ACMA will consider, the AISI clearly plays a central role in how many ISPs manage malware.

Given this research shows a wide variation in the extent to which ISPs use AISI data, it is likely that this data could be used more broadly in the ISP industry to manage malware threats.

Introduction

The AISI is a program operated by the ACMA to help internet and communications providers address the problem of ‘compromised’ computing devices.

The main activity of the AISI is to obtain data and report information that participants can use to identify customers on their networks with computing devices compromised by malware (or malicious software). Its aim is to enable AISI participants to reduce the harm malware infections cause to individuals through the loss of personal and sensitive information, and to contribute more broadly to the reduction of spam and other e-security compromises. Participants are expected to advise customers that they may have a compromised computing device, 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’ computing devices and their own communications networks.

In conducting this research, the ACMA was interested to understand participants’ perspectives on the operation of the AISI, how effective the program is and how it might be improved.

Background

The AISI was one of the world's first anti-botnet initiatives. It is removed from the ACMA's regulatory activities, and instead relies on partnerships between the ACMA and industry to facilitate better cybersecurity among Australian users. The AISI has grown and evolved—from an initial six participants, 137 participants were involved at the time of the research, including 119 ISPs and 18 universities. These organisations are estimated to cover more than 90 per cent of Australian residential internet users. It has also expanded—from initially reporting only a few variants of malware, there are now more than 750 malware types listed in the AISI database.

More recently (commencing during the period this research was conducted), the AISI has begun reporting vulnerabilities affecting internet services such as webservers and routers. The AISI is now regarded as providing one of the most extensive pictures of the extent of malware infestation on Australian internet services, and has recently been used for this purpose in the Australian Cyber Security Centre's 2015 Threat Report.

Participation in the AISI is voluntary and free-of-charge. Organisations are eligible to receive AISI reports if they have their own allocated IP ranges. Most organisations participating in the AISI provide internet and associated communications services to a range of customers.

The AISI operates alongside the iCode— a voluntary cybersecurity code of practice—that places an emphasis on detection of malware infections in ISPs’ networks and draws attention to the AISI as a means of doing so. The iCode was developed in 2010 by the Internet Industry Association in consultation with the ACMA and government. On 24 March 2014, responsibility for the ongoing development and oversight of the iCode was taken over by Communications Alliance, and an updated version of the code was released in August 2014.

The iCode provides guidelines to help ISPs provide consistent messages to their customers when they receive AISI infection reports or otherwise identify infected computing devices on their networks. Information about educating customers and reporting 'malicious activity' to appropriate authorities is also detailed in the code.

Acting on AISI reports involves informing customers they may have a compromised computing device and helping them to resolve the problem. Whether any action is taken, and the degree to which action is taken, is at the discretion of the individual provider. Similarly, customers are not required to take action in response to the advice of a malware infection from their provider unless not taking action contravenes their provider service agreement.

Previous AISI research

This research updates and builds on research into the AISI conducted in late 2011 and early 2012 with participating ISPs and educational institutions.

This research, *The Australian Internet Security Initiative—provider responses to security-compromised computers: Interviews with industry participants*, undertook in-depth interviews with a sample of 24 AISI members, in different Australian states, including small, medium and large internet providers, and universities.

The research identified how providers act on malware reports and help customers to resolve malware problems. One finding from this work was strong support from ISPs for the ACMA to develop an AISI portal. The portal was introduced in 2014 and the 2015 research includes questions about the use of the portal and possible improvements.

Diversity of AISI participants

AISI participants represent a diverse and extensive 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, subscription and on-demand television or video, as well as telephone, data, video and mobile communications. Their customers encompass residential, business, government, university staff and student users.

Characteristics such as the type and size of service providers and the resources available to them help determine how providers use the AISI information and their capacity to help customers.

Information provided to AISI participants

Through the AISI program, the ACMA provides information and advice to AISI participants, along with data reports that identify compromised customer computing devices.

The following information about the AISI program is available:

- access to a list of AISI participants. The list of AISI participants is provided in Appendix 1.
- three charts, updated daily, on malware infections and service vulnerabilities observed on Australian networks.

AISI reports

As part of the AISI, the ACMA emails daily reports to registered internet providers where compromises have been found on the IP ranges assigned to their networks. It is the providers’ responsibility to inform the ACMA of any changes to their IP range assignments. Providers can also access this information through the AISI portal rather than by email.

The daily reports identify the number of unique infections detected for each AISI participant since the previous report (data older than 72 hours is not included), a list of infected IP addresses, the corresponding name of the malware type and additional information on the infection where this is available from the source supplying data to the ACMA. This information has generally been reported to the ACMA in the previous 24 hours.

Extensive ‘vulnerable service’ data was introduced into the daily AISI reports on 13 March 2015 (during the period of the interviews), with some interviewees responding positively to this initiative.[3]

Appendix 2 provides examples of these daily reports.

AISI reports are compiled from a broad range of data sources from the global cybersecurity community. Currently, over 30 discrete data feeds are utilised for AISI reporting, received from 13 different entities, including the Shadowserver Foundation and Microsoft.

The data feeds are carefully analysed before they are utilised for AISI reporting. Some feeds contain multiple malware or service vulnerability types and often only some of these types are reported from these feeds. A high premium is placed on only reporting reliable data to ensure the integrity of the program and because considerable expense may be involved in seeking to remediate an infection. Many of the data sources the AISI uses are not readily available to providers or ISPs as data providers prefer to deal with one national organisation in providing this information.

While the AISI program utilises a comprehensive set of data, it does not identify all forms of compromises or service vulnerabilities affecting Australian internet users. The number of compromises existing on Australian networks but not reported through the AISI is unknown.

AISI online portal

After a soft launch in mid-2014, an AISI portal was formally launched in November 2014. This portal provides access to a more comprehensive set of data than is contained in the daily AISI reports. For example, a given IP address may have numerous reports of a malware type over a 24-hour period—in cases where there is no new information about that malware infection, only the most recent report is included in the daily AISI email.

The portal enables providers to perform granular searches on the different network elements associated with malware infections and vulnerable services, such as all observations over a given date period that utilised a local port of 14646 (or any other local or remote port where this data is available from the AISI data feed). The portal currently contains approximately 16 months of AISI data and 233.3 million observations.

Appendix 3 provides an example of the information available on the AISI portal.

[3] Post-fieldwork (on 25 May 2015), the ACMA transferred this vulnerable service data into a separate daily AISI email report due to the different nature of this data.

Nature of the malware problem

The deployment of malware has interrelated harmful consequences for service providers and internet users. Computing devices compromised through the surreptitious installation of malware can be controlled remotely for illegal and harmful purposes without the user's knowledge. These compromised devices 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. A number of providers interviewed deal with DDoS attacks and spamming activity that adversely affects their network performance and availability.

For individual internet users, the main harmful consequences arising from malware infections are the theft of personal and sensitive information from their infected computing devices. This information can then be used for multiple purposes, such as enabling banking and identity fraud and extortion. A trend in recent years has been the installation of 'ransomware', where a malware infection causes files on a computer (and potentially connected network drives) to be encrypted. The computer owner must pay a ransom to decrypt these files.

Quantitative research undertaken by the ACMA in 2013 with 1,500 Australians aged 18 years and over indicated that nearly one-fifth of Australian internet users (18 per cent) don't have sufficient protective software on their home computer.[4] Another 10 per cent (1.46 million users) have no protection at all, while eight per cent (1.12 million users) don't regularly update their software.

[4] ACMA, *Malware and harmful software—consumer views on software threats and use of protections*, October 2013.

About the research

Research with AISI participants was undertaken to help the ACMA refine the AISI program. The aim was to better understand what measures participants use to help their customers resolve malware compromises, and any additional information or assistance that participants consider would enhance the program.

Research methodology

Personal telephone interviews were conducted with 24 randomly selected AISI participants between 23 February and 27 March 2015. These 24 were selected from a stratified list of 82 AISI members who received compromised computer reports from the ACMA in early 2015. The interviewed AISI members were stratified into four subgroups to help ensure broad coverage of AISI members in this research (see Table 1).

Interviews were undertaken and this report written by staff from the ACMA's Research and Analysis section.

Research issues

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

- use of, and action taken on, the daily AISI reports and/or data downloads from the AISI portal
- other methods and practices providers use to deal with malware infections that affect their customer/user network
- actions taken to inform and help customers deal with malware infections detected on their computer/s
- whether these cybersecurity and related customer assistance practices have changed in the last two or three years (since AISI research from early 2012)
- the nature of customer feedback after they are contacted about malware incidents
- reporting of significant cybersecurity risks to external authorities
- improvements to the AISI and additional government assistance that may help deal with malware and other cybersecurity threats.

Details of the research methodology and sampling are provided in Appendix 4.

Limitations

The research does not address in detail the extent to which internet providers use AISI data to combat malware and help their customers. It also does not assess to what extent internet providers follow the guidelines in the voluntary cybersecurity code of practice, the iCode.

research**acma**

Our research program—research**acma—**underpins the ACMA's work and decisions as an evidence-informed regulator. It contributes to the ACMA's strategic policy development, regulatory reviews and investigations, and helps to make media and communications work for all Australians.

research**acma** has five broad areas of interest:

- market developments
- media content and culture
- social and economic participation
- citizen and consumer safeguards
- regulatory best practice and development.

This research contributes to the ACMA's social and economic participation research theme.

Main findings

This section presents the results of 24 telephone interviews undertaken with a selection of AISI participants. They are indicative of the ways internet providers respond to the information they receive about customers' malware infections.

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

The main themes identified for the research are reflected in the presentation of findings.

Use of, and action taken on, daily AISI reports and/or data downloads from the AISI portal

The majority of the AISI participants interviewed reported acting on the daily AISI reports received by email (22 of the 24 participants interviewed).

A representative from a small ISP mentioned not being aware of the daily AISI report received by their organisation.[5]

More differences were evident in the use of the AISI portal by AISI participants (launched in mid-2014). Only a fifth of the participants indicated having used the AISI portal (four large ISPs and one small ISP). Other participants were either aware of it but not using it (two medium ISPs, one small ISP and education institutions), or not aware of it. The most common reason given for not using the portal by those aware of it was the preference for daily email reports as these were processed by the provider's ticketing system. It was considered easier to receive data via this mechanism than to retrieve information using the portal.

Participants in the research had a mix of manual and automated processes in place to deal with the information in the daily AISI reports. A third (three large ISPs, two medium ISPs and one small ISP) have automatic or semi-automatic processes in place, while two-thirds (three medium ISPs, seven small ISPs and five educational institutions) currently manually process the information.

[5] The ACMA's experience is that this happens not infrequently—personnel change and information about the AISI report is not passed over to new staff. To address this issue, the ACMA encourages internet providers to use generic email addresses that can be accessed by multiple staff.

Table 2: Summary of use of daily AISI report and AISI portal, by type of ISPs

Type of ISP	Using daily AISI reports	Using AISI portal	Automated or manual process
Large ISP	3	4; 1 aware but not using	3 automated or semi-automated; 1 under consideration[6]
Medium ISP	All (5)	2 aware	2 automated, 3 manual
Small ISP	8 (1 not aware)	1 using; 1 aware	1 fully automated; others manual
Educational institution	All (5)	none	All manual

How providers deal with malware infections that affect their customer/user network

A third of the participants (seven out of 22) who use the AISI reports rely solely on them for information about malware infections affecting customers on their networks. Small ISPs are more likely to rely solely on AISI reports—all small ISPs interviewed except one rely solely on AISI reports for this data.

For two-thirds of respondents, the AISI daily reports were not the sole mechanism to identify and help prevent malware infections affecting their customers. Other sources of malware infections mentioned were AusCERT reports, reports generated by automated in-house abuse detection systems, AOL and Yahoo reports, and specific packages dealing with malware detection and alerts. All participants use spam and email filtering solutions.

Table 3: Other sources used to detect malware infections, and use of spam and email filtering solutions

Type of ISP	Use of other sources to detect malware	Use of spam and email filtering solutions
Large ISP	All	All
Medium ISP	3 solely AISI; 2 other sources	All
Small ISP	4 solely AISI; 5 other sources	All
Educational institution	All	All

[6] One large ISP had previously developed an automated system to process AISI 'repeated sightings' reports, which were discontinued in mid-2014. It has yet to update its system to process data either from the AISI portal or in the daily AISI reports.

Actions taken to inform and help customers deal with malware infections

Participants use a variety of approaches to address the problem of compromised computing devices, both in terms of processes in place and level of assistance provided to customers.

Almost all participants have processes in place to address compromised computer problems with customers

With very few exceptions, participants indicated they use the information in the daily AISI report to deal with malware infections on their customer networks, albeit to varying degrees. Some ISPs only make limited use of the AISI; others are more proactive, taking some form of action to inform their customers of the malware infection and help them fix the problem.

For example:

- A typical approach involves notifying customers of the compromise and providing information about how it might be resolved. This is usually achieved via an initial email, while some providers make this initial contact by phone.
- Some ISPs are concerned that passing on information to customers may confuse them. They simply let customers know they have been affected by malware and ask them to contact the providers' customer service centre.
- Some participants do not notify their customers and just suspend or restrict accounts as a way to encourage customers to contact the provider.
- Some participants only contact a customer when repeated incidents occur.

Notifications of malware infections and sources of support and information for customers

In order to prevent viruses from infecting their customers' devices, participants use a range of approaches to inform and help customers deal with the risk of malware infections. Most large and medium ISPs provide general information on internet security on their website, with questions and answers on different security topics, and terms and conditions for use of their networks.

Another source of customer information is the ISP's customer service or technical support teams. These teams provide help over the phone to affected customers, including reference links and sites with more information on how to resolve and prevent malware infections.

The nature of the assistance provided can vary depending on whether the customer is a residential or business user. Participants indicated that business customers tend to require less support than residential customers as they have their own IT teams to deal with the malware infection.

Participants seem to use different strategies in terms of how much information from the AISI malware report they pass on to their customers, as well as the timing and handling of these notifications. Some participants do not pass on all the AISI report information to customers in order not to confuse them. They prefer to just advise the customer of the malware infection and ask them to contact the customer service centre for further information.

Some participants only send notifications to affected customers if an incident is repeated:

> We look for repetitions, trends over a number of days. It makes more sense to focus on incidents that continue to show up on the reports—usually it corresponds to customers with no anti-virus protections or out-of-date protections. (Large ISP)
>
> For residential customers, there are a lot of reports, and it is challenging for us to action all of the reports, but we definitely look at the ones that are repeat offenders.' (Medium ISP)

Some participants do not notify their customers, and just suspend or restrict their account to get them to react and call the customer service centre.

Customers are encouraged to respond to notifications in two ways:

- asking customers to call back the provider in response to an email informing them that their service has been affected or restricted
- making a follow-up call to customers if it appears the malware infection has not been resolved—in these cases, providers may impose a limit of three email notifications or phone calls made to customers, after which they consider it the customer's responsibility to resolve the issue.

Varying degrees of help in remediating malware infections

The level of assistance participants provide to customers varies greatly, from limited to considerable:

- A number of participants provide considerable assistance and support to residential customers, and small and medium-sized business customers.

  Support is most often given directly over the phone and involves taking customers through the necessary steps to resolve a particular problem—for instance, the process of installing or updating and running antivirus software. Those participants indicated they try to give as much assistance as possible over the phone.

  The last resort is usually to recommend the customer takes the computer to a professional IT technician, with some participants having a list of trusted IT experts for referral.
- Some participants indicated that medium and large business clients require little assistance from them to resolve malware infections. These clients generally have internal IT assistance to rely on and there is an expectation that, after notifying these clients about the computer compromise, the client will be able to fix the problem.
- Some participants only provide minimal assistance to residential customers, instead placing primary responsibility for fixing the problem on the customer. A common approach by these participants is to provide a generic email informing their customer that they have a malware infection, with a recommendation that they resolve the problem with antivirus software. In cases where the customer is unable to resolve the malware problem, it is recommended that they use the services of a professional IT expert.

Examples of provider approaches to customer assistance

- For customers who continue to have an infection for a period of one month, one provider follows up its emails with telephone contact and claims to get '100 per cent resolution' through this process. They supplement this approach with an alert that provides 'a page popping up on their screen informing them there may be a problem and asking them to contact us'.
- A university said that it has multiple approaches depending on the category of client (server administrator, staff member or student). For students, it disables their

account, then sends out IT support staff to help remove the infection. This university also noted:

> In a lot of cases, it may be international students with a wrong [i.e. non-genuine] version of Windows. We provide it [a genuine version of Windows] to them for $12 with free anti-virus. (University)

- One university locks out access to its network if the malware has not been removed after three reports:

  > We send an email to the contact with advice on how to get rid of it. Sometimes it gets ignored. We lock after three times in a row if it gets ignored.'(University)

- One small service provider has the following process:
  - after informing customers, they follow up in 48 hours to ensure action is being taken
  - if no action has been taken in seven days, they suspend the service
  - if they receive notification that customers are receiving repeated incidences of malware, they shut down the service.

Different approaches to residential and business customers

Some ISPs treat business/corporate customers and residential customers differently and separately:

> We have two key customer service teams that manage malware infections: business/corporate and residential. As a general thing, malware infections are significantly lower for business/corporate customers than in the residential market. Direct contact is made with corporate customers; they are handled a higher level of support than residential customers. (Medium ISP)

Another medium ISP takes a different approach:

> We offer limited assistance; we provide advice; we make suggestions about what steps to take; we offer limited technical support. The assistance offered is the same for residential and business customers. However, the majority of business customers tend to have their own internal IT assistance, so we don't really to do much for them. For residential, we offer more assistance.' (Medium ISP)

One small ISP does not treat residential and business customers differently:

> We don't really treat residential and business customers differently. An email is sent to affected customers, and if they want to contact us, they can. They then get verbal advice over the phone. We can send scanning programs to them; if the customer has no idea, we suggest they see a computer expert. Some customers may think our email is a spam. We don't provide SMS notifications. Most of the time, people do call back.' (Small ISP)

Another small ISP takes a different approach:

> We treat customers differently. We provide a wholesale service to a number of customers. For these customers, we solely on forward the AISI reports. For users with our managed service—generally business customers—we provide a full clean up service to remove the malware infection and have managed plans that can take responsibility of updating security software on behalf of the customer. (Small ISP)

Recent changes to cybersecurity and related customer assistance

Participants were asked about changes to the cybersecurity and related customer assistance practices that had occurred in the past two to three years (since the previous AISI research was undertaken in 2012).

Most participants have undertaken continuous changes to, or refinements of their systems, while a quarter have made no changes. Four participants have started using the AISI reports and are happy with the information they provide. One ISP said:

> Before the AISI, we didn't have anything in place; we dealt with problems on [a] case-by-case basis; and we did this only if a customer brought a problem to our attention. The AISI is great for us because we can help our customers. (Small ISP)

Another small ISP indicated:

> We are now using AISI, and because we use AISI, we now have a policy to detect and prevent malware and botnet viruses. Previously to receiving the AISI reports, we were just monitoring high upload usages on the customer network. (Small ISP)

Examples of changes include:

- continuing refinements in IT security systems for improved detection and prevention
- improvements in how information is relayed to customers
- the provision of more technical assistance
- improvements in the education of staff and customers on security issues.

One participant, while not changing their level of customer assistance, has found it easier to help customers affected by malware infections because the AISI reports now provide more information.

A medium ISP has become better at relaying information to customers:

> We are taking these issues of malware infections more seriously in the past three years and we provide more technical assistance. Generally, we offer a better customer service with resolving the issues quicker and with less hassle. (Medium ISP)

Prospective future changes that ISPs mentioned are mostly ways to further automate or consolidate their existing processes.

Educational institutions have mostly had to respond to external changes to the security environment with an increase in capacity.

> Distributed denial of services (DDoS) have been ramping up and required us to expand in terms of capacity. We have had to hire extra consultants. (Educational institution)

Educational participants are also faced with some specific challenges, for example, students using their own devices on campuses:

> 'A large number of users are bringing their own devices. This makes it more difficult to manage malware infections. Users have to handle malware infections themselves. We provide information and advice.' (University)

Two providers commented on an increase in DDoS attacks and expending additional resources to deal with these.

Customer feedback following contact about malware incidents

AISI participants do not systematically receive feedback from customers in response to malware reports—some rarely receive feedback and others never. For those who do, the nature of the feedback appears to be generally positive; customers are mostly grateful for being informed of the malware infection and any support from the ISP.

Given this diverse customer response to reports of malware infections on their services, the ACMA intends to conduct research into home users' experience of malware infection and what level of assistance they receive in dealing with the infections.

Asked about the nature of this feedback, a medium ISP indicated:

> Most people are deliriously happy. 99 per cent of the customers are happy to hear about problems. They want to be good network citizens and they want the issues resolved. (Medium ISP)

When questioned about customer responses to malware reports, one large ISP said:

> Overwhelmingly, customers tend to be quite grateful and happy to be contacted—especially with the DNS Changer—as many customers are not technically knowledgeable. Customers simply had no idea that this infection/virus was on their system.[7] (Large ISP)

However, three of the large ISPs interviewed believe customers don't like being contacted—even to be notified they have been affected by malware infection.

Participants described customer attitudes to the notification of malware infections as ranging between disbelief, hostility and resentment that the ISP monitors their data; appreciation that the ISP is helping them; or simply wanting to be left alone. Participants indicated there are very few unresponsive customers. Being able to represent the AISI malware report as originating from an official government source helps to address some of these reactions, as it enhances the legitimacy of the communication.

Small ISPs and educational institutions mentioned most uncooperative customers tend to be Mac users because of the perception these devices aren't affected by malware infections.

Reporting significant cybersecurity risks to external authorities

Tracking cybersafety incidents

Participants were asked if they keep records and track information on malware infections on their networks. However, few could provide information about tracking—data is not available for large ISPs and for some of the medium ISPs. And few of the AISI participants who provide information appear to track whether a particular malware infection is resolved, or the general level of malware infections on their networks.

[7] Prevalent in 2011 and 2012, the DNS Changer malware was used to redirect infected users to fraudulent domains by hijacking the user's DNS settings. After taking action against the malware perpetrators, the FBI facilitated the ongoing operation of the DNS servers used by the malware so that infected users could continue to have internet access. These servers were turned off on 9 July 2012. The ACMA and AISI participants mounted an extensive campaign to warn and help infected users to address the infection before this date.

Some participants use their ticketing system to track information about malware infections. However, not all participants with a ticketing system in place use it to track data and report on malware infections.

Reporting significant cybersecurity incidents to external authorities

Participants were also asked if they report significant incidents affecting their networks to any external authorities.

All of the large ISPs have regular to occasional contact with CERT Australia. One medium ISP is in contact with AusCERT, the Attorney General's Department and ASIO. Only one small ISP has contacted any government organisation—both CERT Australia and the AFP. Two educational institutions have also reported cybersecurity incidents to CERT Australia and the AFP.

There seemed to be some confusion about which government organisation participants should report a cybersecurity incident to. Small ISPs cited a range of organisations—the AFP (two ISPs), the ACMA (three), AusCERT (one). Medium ISPs most often mentioned AusCERT and CERT Australia.

It is not clear whether respondents understand the distinction between the roles of CERT Australia and AusCERT:

- CERT Australia is the official national Computer Emergency Response Team and a government organisation. It helps protect Australians and Australian businesses against cyber-based threats and vulnerabilities.
- AusCERT is the Australian Computer Emergency Response Team based at the University of Queensland and is a non-government organisation. It operates within a worldwide network of information security experts to provide computer incident prevention, response and mitigation strategies.

Improvements to the AISI and additional government help to deal with malware and other cybersecurity threats

All internet providers interviewed were asked if they could identify any improvements to the AISI program, the daily AISI reports or the AISI online portal.

Participants are satisfied with the current AISI email reports

Generally, participants are satisfied with the current AISI reports and email notifications. While the information is basic, the reports meet their needs.

One large ISP commented favourably that the formatting of the AISI report has remained consistent over time. Such consistency is important as a number of providers have integrated the reports into their internal systems and developed automated processes to identify customers and generate standard malware notification emails.

Participants also commented that the information in the AISI report is getting richer, with more explanations of specific events and details, and a greater range of cybersecurity incidents targeted. This enables them to make their messaging to customers more consistent and detailed:

> We are happy with the AISI report. The formatting of the AISI reports is consistent which is good. The information is getting richer. There is more explanation of specific events and details per event. [Also, the report has changed in the last month or so.] The details provided in the reports make our messaging to customers more consistent and fuller also. (Large ISP)

Some participants are ambivalent about introducing more detailed information about the malware infection in the AISI incident reports. Although extra information is good for the customer, one large ISP is concerned that approaching customers about a malware infection without overwhelming them with detail is a delicate balance. Two other participants (medium ISPs) worry the information in AISI reports could be too technical for customers to understand.

Generally, participants view the malware infection information in the AISI reports as appropriate. The few that have experienced some issues would like additional information or information not currently covered in AISI reports. However, some of the information mentioned as lacking in the current AISI reports—that is, identification of spam-sending computing devices and infected routers—is often provided.

Suggested improvements to the AISI program

When asked to identify possible areas of improvements for the AISI program, participants identified two main areas:

- the provision of more detailed information
- the format of the reports or how information can be accessed.

Provision of more detailed information

One large ISP has difficulties reconciling all the data to all customers.

> We are not able to reconcile all of the data to all customers (port issue). (Large ISP)

Two large ISPs noted that having the source port information in the reports is critical, but this information is not always available in the reports.[8] In cases where there are many network users behind a given IP address, the source port can help identify the individual computing device that is infected.

ACMA comment: The source port information is often, but not always, available to the AISI. In cases where it is available, this information is always included in the AISI email reports.

A small ISP mentioned:

> Daily AISI report[s] could be improved by providing more up-to-date time stamps. Some of the reports have a time stamp from a few days prior.

ACMA comment: The AISI provides time stamps accurate to the second. However, the reports may include malware infection observations identified in the preceding 72 hours not previously reported to the internet provider (which will be the most recent data available to the ACMA).

The same provider also queried if there might be a way to check if the malware infection reported has been removed when the time stamp is from a few days ago.

[8] The source port, along with the transport protocol (such as TCP or UDP), uniquely identifies the communications endpoint that has sent the IP traffic on which the AISI report is based. In this context, the source port reported, together with the public IP address reported, could be used to search through logs pertaining to the infected device (for example Netflow data) to find the private IP address of (and thereby identify) the specific infected device.

Another small ISP recommended that the AISI portal indicate when a report is completed, so the ISP knows the problem is resolved.

ACMA comment: The portal contains a tag system and participants could use this facility to identify resolved problems themselves if they wish to do so. If the IP is not reported again for that customer, it can be inferred there is a strong likelihood their device is no longer infected. For the problem to be marked resolved in the portal, the customer must inform their ISP they have removed the infection and for the ISP to indicate this in the portal.

Some educational institutions suggested adding more information or commentary in the report on what infection/malware/spam is affecting its users, to decrease the time needed to communicate and research the malware infection internally. For universities, having an authoritative source to rely on when they pass on the information to IT support internally or to their users would be helpful and save time.

ACMA comment: The ACMA will consider such an enhancement.

One university suggested some trending analysis may be useful to provide historical information on the malware infection when staff go on leave.

ACMA comment: The AISI portal provides historical trend information.

Changes to the format of the reports or how information can be accessed

One small ISP was interested in being able to automate its system so emails can go directly to affected customers; for example, a .csv file or an excel file to upload to a server.

ACMA comment: The ACMA has been considering providing .csv reports and .csv-formatted files for download from the AISI portal. An issue, however, is maintaining consistency for ISPs who have already developed automated procedures for processing the AISI data. A possible solution is to offer numerous formats to maintain continuity of services for all providers. The ACMA will consider such an enhancement.

A couple of participants suggested making information on the latest malware infections available for customers to access directly from the AISI portal. This included the recommendation for a more user-friendly, self-help website that would enable customers to search for more information on specific malware infections they had been notified about.

ACMA comment: The ACMA will consider such an enhancement.

Rather than a portal, another ISP suggested having a consumer web system that gathers information directly from the web service into a threat management system.

One ISP commented that the AISI portal does not appear to keep up with changes in the AISI reports, and it would be good to update the AISI website with the most current information from the reports.

ACMA comment: The AISI subsection of the ACMA website contains information on the top five malware infections currently being reported with a brief description of these. This information is updated every day.

Some ISPs suggested that additional information and documentation be available from the ACMA that the ISP could attach to emails to affected customers—for example, a two-page document with information about the malware infection, spam protection programs and other basic recommendations.

ACMA comment: Under consideration.

Suggested improvements to how government helps deal with malware infections

When asked for how government help with malware infections could be improved, outside of the AISI reports, two large ISPs suggested consolidating the number of agencies dealing with cybersecurity incidents:

> The number of agencies that deal with cybersecurity issues can be confusing. (Large ISP)
>
> There is a real lack of government coordination on cybersecurity and public messaging in this area [the way government assists malware infections]. (Large ISP)

These ISPs point to the desirability of a whole-of-government approach to coordinate information and activities.

ACMA comment: Greater coordination of government responses to cybersecurity issues is a particular focus for the Australian Cyber Security Centre. The government is currently conducting a Cyber Security Review that is examining further mechanisms to promote coordination of government cybersecurity efforts.

There was also a concern that government and industry are not sufficiently preparing for the future—for example, potential cybersecurity breaches affecting smart fridges and smart cars. Participants in the research also commented that more could be done to share information—for example, for government to provide analysis of upcoming malware risks. The ACMA will consider the possibility and opportunity to provide further information and analysis on upcoming risks through the AISI portal. Providing information on upcoming malware infection threats would allow ISPs to manage and prepare for major attacks before the problem gets too big. One medium ISP and one education institution suggested this could be delivered in the form of a monthly report or newsletter.

One educational sector provider called for an anti-DDoS mechanism to be put in place for the sector to mitigate large-scale DDoS attacks. It is noted that DDOS mitigation services are readily available from commercial providers.

Other suggestions for improving how government addresses malware infections related to education programs[9] and information:

- One ISP suggested further education and awareness-raising programs for citizens about malware risks and cyber-attacks.
- Another ISP recommended more resources be made available on where customers go to find information on malware infections, and how to prevent and resolve them.

[9] As noted above, the Communications Alliance iCode also contains information and recommendations for internet service providers about educating their customers in how to prevent and respond to malware infections.

- One ISP asked to receive some form of feedback from government on serious malware infections, particularly on what has been done and the outcomes achieved.

Improving the AISI

The research has identified a number of possible ways to improve the AISI. The ACMA will actively consider all of these.

Information is regularly provided to AISI participants about the operation of the AISI—including disclosing the sources of AISI compromise data (where permitted by that source) and the expected actions of the AISI recipients. However, a number of participants appeared to not be entirely familiar with, or to have misperceptions about, the content of the AISI reports or portal.

One area of improvement for the ACMA to consider is to provide additional user-friendly information on the AISI website for AISI participants and customers—such as individuals and small businesses—in the form of frequently asked questions. This would include items such as how the data is captured, how customers are affected and what information the AISI is unable to provide.

Another related suggestion from AISI participants was to have a self-help website, where affected customers could learn what to do to prevent and address malware infections, access more information on specific malware infections and search for incidents. While the ACMA agrees this information would be beneficial to customers, the fast pace of change of malware infections means that providing comprehensive definitive advice is challenging. The ACMA will look at ways to provide more detailed and helpful information on malware infections, which may include linking to other government sites containing this information.

Another suggested improvement was for the AISI portal to enable instant and automated queries from the AISI data. For example, when a customer rings a customer care service with a query, the service staff member could send an automated query to the AISI portal to determine whether that customer has had any recent malware incidents. This development would require considerable resources to implement and will be considered as part of future portal development activities.

Some AISI participants feel there is insufficient information about particular AISI infection types in the AISI section of the ACMA website, which currently only describes the most prevalent types of malware infections. Potentially, the ACMA could consider enhancing the AISI section of its website or the AISI portal to contain more detailed information about the infection types currently being reported through the AISI. However, given there are over 750 malware types identified in the ACMA database, and new types are constantly emerging, this would be very resource-intensive to maintain.

It is beyond the ACMA's current resourcing capability to provide comprehensive information about all the malware infections it reports through the AISI (many of which have numerous and constantly changing variants). There are also numerous customer-related variables that affect the effectiveness and accuracy of any advice given, such as different operating systems, computing devices and home network configurations. As noted above, however, the ACMA will look at ways to provide more detailed and helpful information on malware infections.

The ACMA is currently considering the best way to provide a standardised set of information to AISI participants (standardised messaging from ISPs about malware infections is also something the iCode aims to provide). The ACMA aims to publish a one- to two-page document that would provide links to websites such as Stay Smart Online, some general information about what to do about malware infections and information about emerging risks. This would be made available on the AISI portal for ISPs to use as they choose.[10] In the past, similar information was provided to AISI members through occasional emails.

Among the possible improvements identified as a result of the research, the ACMA is considering the addition of frequently asked questions about the AISI as a priority, as this appears likely to deliver the most immediate benefits to AISI members.

Next steps

In 2015–16, the ACMA is also considering undertaking research on customer perceptions of malware notifications and experiences in responding to malware alerts from providers. This would, for the first time, give the ACMA a comprehensive understanding of the experiences of the end-user beneficiaries of the ACMA's anti-malware program. This research will provide a more comprehensive understanding of the effectiveness of the AISI program and actions taken by internet providers to inform their customers about malware infections.

[10] The ACMA has now included an AISI update section in the portal that contains some information about particular malware or vulnerability types reported through the AISI. See Appendix 3 for a screenshot.

Appendix 1—List of AISI participants

Current participants as at September 2015.

AAPT Limited
Access Net Pty Ltd
Ace Internet Services
Activ8me
Adam Internet
AINS
Albury Local Internet Pty Ltd
Amnet
AOL
Apex Internet
Asian Pacific Telecommunications
ATU Internet Group
Aussie Broadband
Aust Domains
AUSTARnet
BarNet
Bekkers
Bendigo Community Telco
BigAir Group Limited
BKB Internet
Brennan Voice and Data Pty Ltd
Catholic Education Network
Catholic Network Australia
Centorrino Technologies Pty Ltd
Central Data
Chariot CI Internet
Cirrus Communications
Cloud365 Australia
ClubTelco
Comcen
Conetix Pty Ltd
Connectivity I.T
CQ University
CSIRO
Daraco Services
DCS Internet
Deakin University
Dedicated Servers
Digital Pacific Pty Ltd
Dodo Australia
Dreamtilt
earthwave
ECN Pty Ltd
Edith Cowan University
EFTel
Enterprise IP
EscapeNet
e-wire connection point
Exetel Pty Ltd
Flinders University
Fortana Networks Australia
FoundationIT
Foxtel Broadband
GCOMM
Global Dial
gotalk
GoWireless
GPLHost Networks Pty Ltd
Grapevine
HaleNET
Highway 1
Hotkey
HugoNET
IDL Internet
iiNet
Indigo Pty Ltd
Internet Information Group
Internode
Inticon
IntraPower
Ipera Communications
iPrimus
iseek
KDDI Australia
La Trobe University
Legion Internet
M2 Telecommunications
Macquarie Telecom
Matilda Internet
Melbourne IT
Micron21
Monash University
Montimedia
Murdoch University
MyNetFone
Neighbourhood Cable
Net Logistics Pty Ltd
Net Niche Pty Ltd
Netbay Internet
Netspace
Netspeed
NetYP
NewSat
Nexon Asia Pacific
Nextep
NICTA
NSW Office of State Revenue
Nuskope Pty Ltd
Oceania Business Solutions Pty Ltd
On Q Networks
OntheNet
Optus Internet
Orion Satellite Systems
Over The Wire Pty Ltd
Oz Servers Pty Ltd

Pacific Internet (Australia)

PingCo Pty Ltd

Planet Ozi

PPS Internet/StudentNet

Seccom Global

Servers Australia

SkyMesh

Somerville

Soul Communications

Speedweb Internet

Spin Internet

Spirit Telecom

State Library of Victoria

Swinburne University of Technology

Tas Communications

Telstra Bigpond

(The) Australian National University

(The) Galaxy GateWay Computer System

(The) Smelly Black Dog Company

(The) University of Adelaide

(The) University of Melbourne

(The) University of New South Wales

(The) University of Newcastle

(The) University of Western Australia

TPG Internet

Uecomm

University of Wollongong

Unwired

UQconnect

Velocity Internet

Virgin Broadband

vividwireless

Vodafone Hutchison Australia

WAnet

West Australian Networks

Westnet

Appendix 2—Example of AISI daily report

Dear AISI Participant,

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>.

Messages sent to the sender/from address of this email will be summarily ignored.

All URLs contained within the report should be treated as hostile and capable of infecting a user with malware without their knowledge. As such

URLs have been deliberately broken to prevent against accidental infection.

Please disclose any data provided which identifies the remote computer on a need-to-know basis only. Public or other unnecessary disclosure of such data may lead to, for example, pollution of sinkhole data, requiring the sinkhole to be moved. If such data is disclosed to customers, please provide this instruction with the data.

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

--- Report follows ---

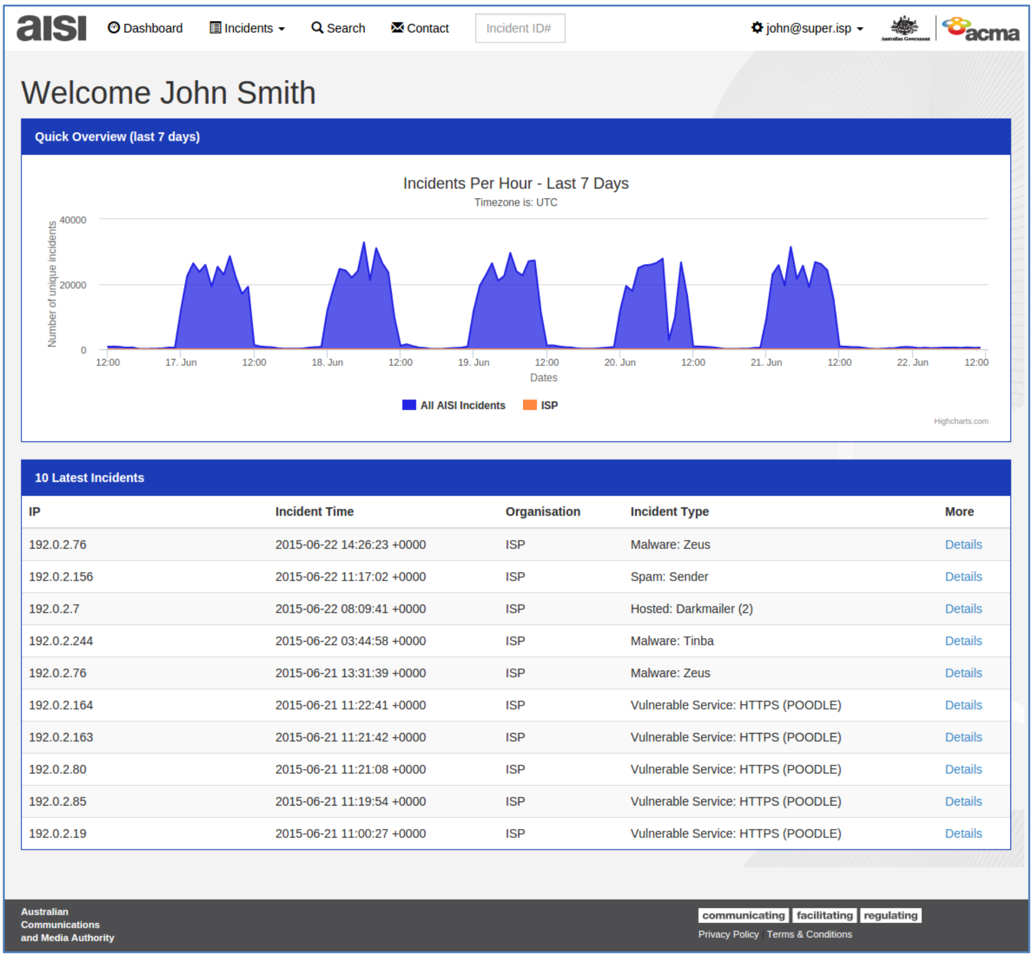
```
IP      DATETIME       TYPE                  NETWORK

ADDITIONAL

192.0.2.25    2015-03-23 20:34:05   Malware: Torpig              ISP
local_port: 55800, remote_ip: 108.61.18.43,  remote_port: 80, domain_name:
egcwbtwh. com, data: /

192.0.2.185  2015-03-23 11:52:04   Malware: ZeroAccess           ISP
protocol: udp, local_port: 17815, remote_ip: 72.196.208.62,
remote_port: 16470, domain_name: ip72-196-208-62. dc. dc. cox. Net

192.0.2.106  2015-03-23 22:23:22   Malware: Zeus                 ISP
local_port: 22823, remote_ip: 82.165.37.26,
remote_port: 80, domain_name: damnpops. com, data: /can/DSC_5870.jpg

192.0.2.119  2015-03-23 21:31:54   Malware: ZeroAccess           ISP
protocol: udp, local_port: 51239, remote_ip: 184.187.165.111,
remote_port: 16471, domain_name: ip184-187-165-111. sb. sd. cox. Net

192.0.2.108  2015-03-23 18:38:03   Malware: Torpig              ISP
local_port: 42292, remote_ip: 108.61.18.43, remote_port: 80, domain_name:
egcwbtwh. com, data: /

192.0.2.202  2015-03-22 08:35:48   Malware: ZeroAccess           ISP
local_port: 58800, remote_ip: 24.252.0.2, remote_port: 16464
```

```
192.0.2.24    2015-03-23 10:46:48   Vulnerable Service: HTTPS (FREAK)  ISP
remote_port: 443

192.0.2.253  2015-03-23 06:25:09   Vulnerable Service: HTTPS (FREAK)  ISP
    remote_port: 443, data: 203.213.248.253

192.0.2.59    2015-03-23 07:45:48   Vulnerable Service: HTTPS (FREAK)  ISP
    remote_port: 443, data: localdomain

192.0.2.58    2015-03-22 06:51:26   Vulnerable Service: HTTPS (FREAK)  ISP
    remote_port: 443

192.0.2.207  2015-03-23 10:58:26   Vulnerable Service: HTTPS (FREAK)  ISP
    remote_port: 443, data: localdomain

192.0.2.7 2015-03-23 07:28:40   Vulnerable Service: HTTPS (FREAK)  ISP
    remote_port: 443

192.0.2.33    2015-03-23 05:43:56   Spam: Sender   ISP     data: HELOs as destination
server

192.0.2.136  2015-03-23 11:30:54   Vulnerable Service: HTTPS (FREAK)  ISP
    remote_port: 443, data: localdomain

192.0.2.49    2015-03-24 14:29:08   Spam: Sender   ISP     data: Broken HELO
bzckbackbdzkdhcad:bzckbackbdzkdheez:bzckbackbdzkdhgba:bzckbackbdzkdhgbd:bz
ckbackbdzkdhgfc

192.0.2.39    2015-03-24 15:49:00   Spam: Sender   ISP     data: Broken HELO
bzckbackbdzkchaza:bzckbackbdzkchazg
```

Appendix 3—Example of content for AISI portal

This appendix includes three snapshots of the AISI portal—two examples of dashboard views and an example of an incident.

Figure 1: Example of dashboard view



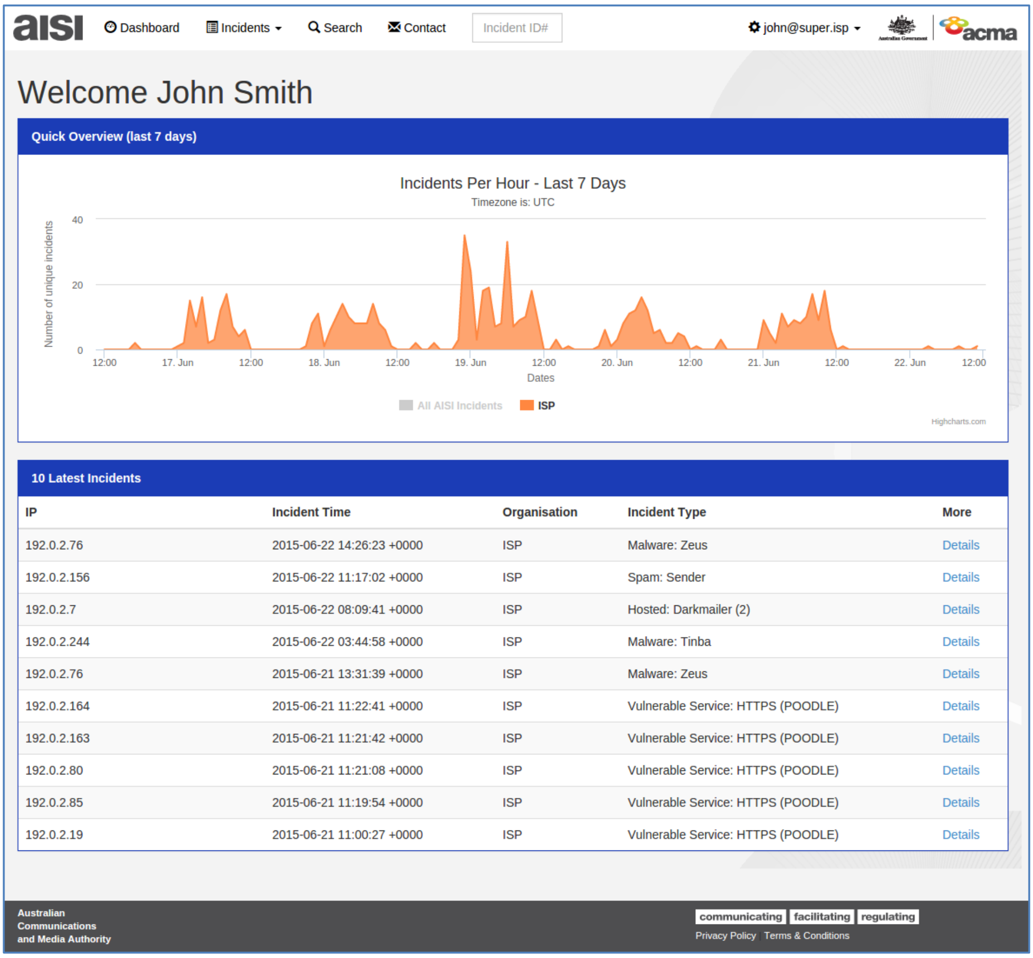
Welcome John Smith

Quick Overview (last 7 days)

10 Latest Incidents

IP	Incident Time	Organisation	Incident Type	More
192.0.2.76	2015-06-22 14:26:23 +0000	ISP	Malware: Zeus	Details
192.0.2.156	2015-06-22 11:17:02 +0000	ISP	Spam: Sender	Details
192.0.2.7	2015-06-22 08:09:41 +0000	ISP	Hosted: Darkmailer (2)	Details
192.0.2.244	2015-06-22 03:44:58 +0000	ISP	Malware: Tinba	Details
192.0.2.76	2015-06-21 13:31:39 +0000	ISP	Malware: Zeus	Details
192.0.2.164	2015-06-21 11:22:41 +0000	ISP	Vulnerable Service: HTTPS (POODLE)	Details
192.0.2.163	2015-06-21 11:21:42 +0000	ISP	Vulnerable Service: HTTPS (POODLE)	Details
192.0.2.80	2015-06-21 11:21:08 +0000	ISP	Vulnerable Service: HTTPS (POODLE)	Details
192.0.2.85	2015-06-21 11:19:54 +0000	ISP	Vulnerable Service: HTTPS (POODLE)	Details
192.0.2.19	2015-06-21 11:00:27 +0000	ISP	Vulnerable Service: HTTPS (POODLE)	Details

Figure 2: Example of dashboard view—overview of incidents



Welcome John Smith

Quick Overview (last 7 days)

Incidents Per Hour - Last 7 Days

Timezone is: UTC

10 Latest Incidents

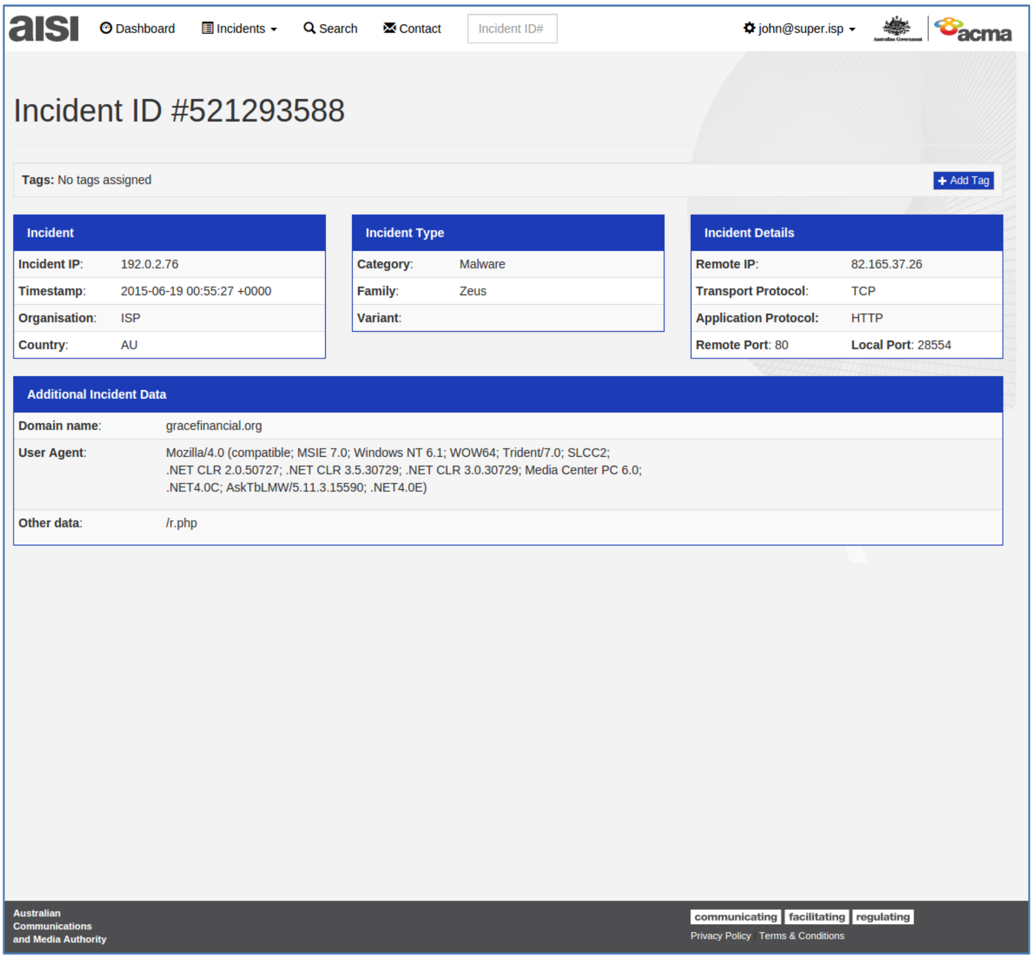
IP	Incident Time	Organisation	Incident Type	More
192.0.2.76	2015-06-22 14:26:23 +0000	ISP	Malware: Zeus	Details
192.0.2.156	2015-06-22 11:17:02 +0000	ISP	Spam: Sender	Details
192.0.2.7	2015-06-22 08:09:41 +0000	ISP	Hosted: Darkmailer (2)	Details
192.0.2.244	2015-06-22 03:44:58 +0000	ISP	Malware: Tinba	Details
192.0.2.76	2015-06-21 13:31:39 +0000	ISP	Malware: Zeus	Details
192.0.2.164	2015-06-21 11:22:41 +0000	ISP	Vulnerable Service: HTTPS (POODLE)	Details
192.0.2.163	2015-06-21 11:21:42 +0000	ISP	Vulnerable Service: HTTPS (POODLE)	Details
192.0.2.80	2015-06-21 11:21:08 +0000	ISP	Vulnerable Service: HTTPS (POODLE)	Details
192.0.2.85	2015-06-21 11:19:54 +0000	ISP	Vulnerable Service: HTTPS (POODLE)	Details
192.0.2.19	2015-06-21 11:00:27 +0000	ISP	Vulnerable Service: HTTPS (POODLE)	Details

Australian
Communications
and Media Authority

communicating | facilitating | regulating

Privacy Policy Terms & Conditions

Figure 3: Example of incident



Incident ID #521293588

Tags: No tags assigned

Incident	
Incident IP:	192.0.2.76
Timestamp:	2015-06-19 00:55:27 +0000
Organisation:	ISP
Country:	AU

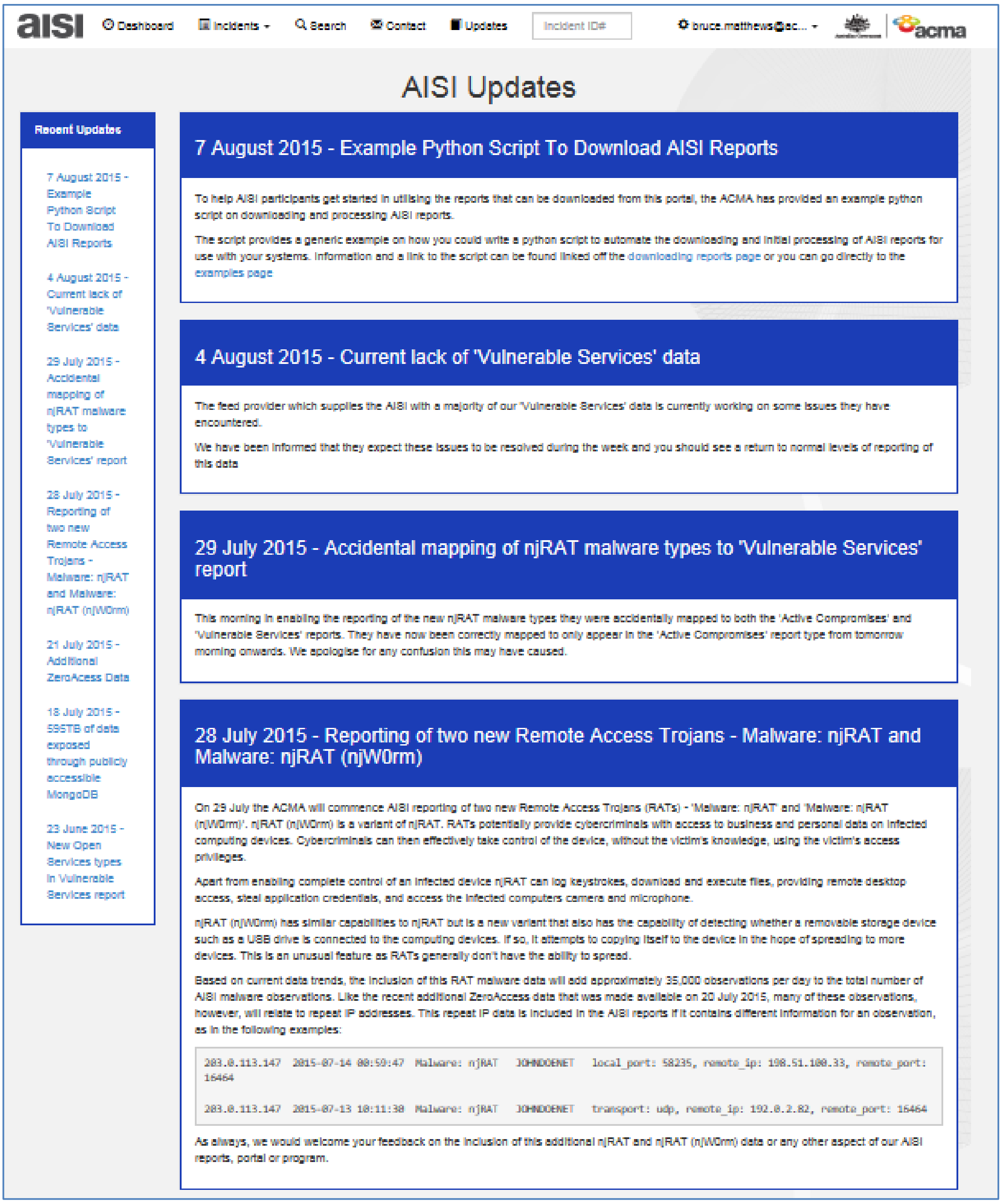
Incident Type	
Category:	Malware
Family:	Zeus
Variant:	

Incident Details	
Remote IP:	82.165.37.26
Transport Protocol:	TCP
Application Protocol:	HTTP
Remote Port: 80	**Local Port**: 28554

Additional Incident Data	
Domain name:	gracefinancial.org
User Agent:	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; AskTbLMW/5.11.3.15590; .NET4.0E)
Other data:	/r.php

Australian
Communications
and Media Authority

Figure 4: Screenshot of AISI updates



AISI Updates

Recent Updates

- 7 August 2015 - Example Python Script To Download AISI Reports
- 4 August 2015 - Current lack of 'Vulnerable Services' data
- 29 July 2015 - Accidental mapping of njRAT malware types to 'Vulnerable Services' report
- 28 July 2015 - Reporting of two new Remote Access Trojans - Malware: njRAT and Malware: njRAT (njW0rm)
- 21 July 2015 - Additional ZeroAcess Data
- 18 July 2015 - 595TB of data exposed through publicly accessible MongoDB
- 23 June 2015 - New Open Services types in Vulnerable Services report

7 August 2015 - Example Python Script To Download AISI Reports

To help AISI participants get started in utilising the reports that can be downloaded from this portal, the ACMA has provided an example python script on downloading and processing AISI reports.

The script provides a generic example on how you could write a python script to automate the downloading and initial processing of AISI reports for use with your systems. Information and a link to the script can be found linked off the downloading reports page or you can go directly to the examples page

4 August 2015 - Current lack of 'Vulnerable Services' data

The feed provider which supplies the AISI with a majority of our 'Vulnerable Services' data is currently working on some issues they have encountered.

We have been informed that they expect these issues to be resolved during the week and you should see a return to normal levels of reporting of this data

29 July 2015 - Accidental mapping of njRAT malware types to 'Vulnerable Services' report

This morning in enabling the reporting of the new njRAT malware types they were accidentally mapped to both the 'Active Compromises' and 'Vulnerable Services' reports. They have now been correctly mapped to only appear in the 'Active Compromises' report type from tomorrow morning onwards. We apologise for any confusion this may have caused.

28 July 2015 - Reporting of two new Remote Access Trojans - Malware: njRAT and Malware: njRAT (njW0rm)

On 29 July the ACMA will commence AISI reporting of two new Remote Access Trojans (RATs) - 'Malware: njRAT' and 'Malware: njRAT (njW0rm)'. njRAT (njW0rm) is a variant of njRAT. RATs potentially provide cybercriminals with access to business and personal data on infected computing devices. Cybercriminals can then effectively take control of the device, without the victim's knowledge, using the victim's access privileges.

Apart from enabling complete control of an infected device njRAT can log keystrokes, download and execute files, providing remote desktop access, steal application credentials, and access the infected computers camera and microphone.

njRAT (njW0rm) has similar capabilities to njRAT but is a new variant that also has the capability of detecting whether a removable storage device such as a USB drive is connected to the computing devices. If so, it attempts to copying itself to the device in the hope of spreading to more devices. This is an unusual feature as RATs generally don't have the ability to spread.

Based on current data trends, the inclusion of this RAT malware data will add approximately 35,000 observations per day to the total number of AISI malware observations. Like the recent additional ZeroAccess data that was made available on 20 July 2015, many of these observations, however, will relate to repeat IP addresses. This repeat IP data is included in the AISI reports if it contains different information for an observation, as in the following examples:

```
203.0.113.147  2015-07-14 08:59:47  Malware: njRAT   JOHNDOENET   local_port: 58235, remote_ip: 198.51.100.33, remote_port:
16464

203.0.113.147  2015-07-13 10:11:38  Malware: njRAT   JOHNDOENET   transport: udp, remote_ip: 192.0.2.82, remote_port: 16464
```

As always, we would welcome your feedback on the inclusion of this additional njRAT and njRAT (njW0rm) data or any other aspect of our AISI reports, portal or program.

Appendix 4—Research methodology and sampling

Methodology

Personal telephone interviews were conducted with 24 randomly selected AISI participants between 23 February and 27 March 2015. These 24 were selected from a stratified list of the 82 AISI members who received compromised computer reports from the ACMA in early 2015.

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 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. Appendix 5 provides the interview guide used for this research.

Interviews were undertaken by ACMA staff in the Research and Analysis section (RAS) with assistance from Internet Security Programs section (ISPS), which administers the AISI program. The research project has been developed in close consultation between RAS and the Unsolicited Communications branch of the ACMA.

An email was sent to all AISI participants before the interviews 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 30 minutes, and ranged from 20 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 4). Researchers made a general assumption 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 fewer 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, and include companies that provide national services. Table 4 also shows the number of providers interviewed compared with the AISI participants.

Table 4: 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)	39	*48*	9	***37***
Medium (21–599 cases reported per day)	24	*29*	5	***21***
Large (600–5,000 cases reported per day)	6	*7*	5	***21***
University (usually <10 cases reported per day)	13	*16*	5	***21***
TOTAL	**82**	***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.

Appendix 5—Interview guide for the 2015 AISI research

Telephone interviews with internet service providers—key discussion topics and questions for the person who knows most about malware infections (incl. use of AISI reports) and related customer assistance.

1. Methods and practices used by providers to deal with malware infections that affect their customer/user network

> What, if anything, does your company/university do to detect malware on your customer network?

PROBE to understand the different methods and sources used, including whether AISI reports are used, and the extent that AISI reports are relied upon in the mix.

> Do you do anything to restrict spam or emails with malicious content from entering or leaving your customer network?

PROBE for details as needed.

> Does your company/university provide any general information to your customers/users about how to minimise the impact of malware on their computer/s?

- o What type of information? Where do you provide that information?

2. Use of, and action taken on, the daily AISI reports and/or data downloads from the AISI Portal

> Does your company/university use the daily AISI reports?

- o Are the reports received via email or do you download the reports from the AISI Portal?
- o Are you aware of the AISI Portal?

> What do you do with the information in the daily AISI reports—how do you process the information?

PROBE FULLY for details about how the daily AISI reports are processed internally.

- o Are your processes automated, manual or a mix of both?
- o Do you experience any difficulties using the AISI data? What difficulties?
  - ▪ is it easy to identify your customers from the information in the AISI reports? What are the difficulties (if any)?
  - ▪ do you use static and dynamic IP addresses for different customers? Why are they allocated in this way?

> Does your company/university offer mobile data services? *IF IT DOES:* Do you notify users of these mobile data services if a malware infection is detected on the service?

> Can you think of any ways that the daily AISI reports could be improved?

PROBE FULLY for ideas and details about possible improvements that would assist ISPs/universities to assist their customers/users.

IF AISI PORTAL USED:

> What are your experiences with the new AISI Portal? What data have you used from the Portal? How useful is it? Any difficulties or problems? Can it be improved in any way?

IF AISI REPORTS NOT USED:

> Can you tell me the reasons why your company/university does not make use of the daily AISI reports?

PROBE for reasons

3. Actions taken to inform and assist customers deal with malware infections detected on their computer/s

- What, if any, follow-up actions does your company/university take to assist customers/users deal with malware detected on their computing devices?

  PROBE FULLY for details of the steps and actions taken to assist customers resolve infections on their computer/s, including information, advice and assistance.

  - Is the same information and assistance offered to all customers e.g. between corporate and residential customers? *IF IT DIFFERS:* Why does it differ?
- Can you give a rough estimate of the proportion of data in the daily reports that is used to inform customers of compromises? Why is this?
  - Are some compromises notified to customers/users and not others? Why is that?
  - Does assistance vary with the number or severity of the compromises detected?
  - How often do you notify customers/users about compromises. For instance, is it everyday, weekly, fortnightly?
- Are any steps taken to promote confidence that the advice given of a malware infection is an authentic communication from your company/university?
- Can you estimate the proportion of your customers/users that have experienced malware infections over the last month?

4. Whether these cyber security and related customer assistance practices have changed in the last two or three years (since AISI research was previously undertaken in early 2012)

- Have the internal practices used to identify malicious threats changed in the last two or three years?
- Has the assistance provided to customers/users changed in the last two or three years? How has it changed? Why has it changed?

5. The nature of customer feedback after they have been contacted about malware incidents

- Do you receive much customer feedback when you contact them about compromised computing devices? What is the nature of that feedback? Is it mostly positive or negative?
- Do you know the extent to which problems are fixed by customers/users?
- Do customers request more information? what type/s of further information is requested?
- To what extent are customers/users unresponsive or resistant to advice?

6. Reporting of significant cyber security risks to external authorities

- > Do you keep internal records to track malware infections on your network?
- > Does your organisation share or report information about malicious activity to any other organisations or external authorities? Which organisations and authorities?
  - o how regularly does this happen?
  - o do you know the external authority to report significant cyber security risks to?

7. Improvements to the AISI and additional Government assistance that would help deal with malware and other cyber security threats

- > Besides the AISI program that is run by the ACMA, can you think of other ways the Government could work with industry to address malware risks and cyber attacks?
- > Before we finish, is there anything else you would like to add about the things we have been talking about?

PROBE as necessary for details

For the ACMA's purpose only, record: name of contact, company or educational institution; and whether the ISP is small, medium or large.

Appendix 6—Detailed findings for large ISPs

Practices and process

All five large ISPs interviewed use AISI data to varying degrees to deal with malware infections on their customer networks.

Two large ISPs only make limited use of AISI data:

- for one, use of the data is at the 'early design stages' and it is developing a policy about how to use this data
- another only uses the AISI portal to explore and search malware incidents against customer IP addresses when they become aware of an issue.

Three of the five large ISPs actively use the emailed AISI daily reports in their management of malware. One further ISP had previously used the now-defunct *Repeated sightings* report with an automated set-up.[11]

Four of the five large ISPs interviewed have used the AISI portal. The one large ISP that does not use the portal has an internal system in place that already captures malware threats from different sources, including the daily email reports. One ISP is using the portal to concentrate on customers who are repeatedly affected, pulling data on repeatedly affected customers, date, time and type of infection from the portal into its system.

The AISI daily reports are not the only method large ISPs use to detect malware infections; they tend to use a number of different sources to help identify malware on their customer network. As one ISP puts it, 'it is the bread and butter work of any ISP to protect and manage its network'. Three of the large ISPs currently use an automated or semi-automated system to provide alerts to their customers about their malware infections. One further ISP is considering using the daily AISI data from the portal if internal funding becomes available.

Approach to malware infections

Large ISPs tend to have diverse approaches to dealing with malware infections, whether they are identified from AISI data or other sources. These include:

- concentrating on repeated incidents or trends over a number of days—this usually indicates customers with no antivirus or out-of-date anti-malware protection software
- providing general advice and assistance to customers who are affected by malware viruses
- suspending accounts that have been compromised—to prompt customers to call the customer service desk so they can be advised of the malware infection

[11] The *Repeated sightings* reports were discontinued in mid-2014 because equivalent (and far more comprehensive) data was made available through the AISI portal at this time, albeit through a different mechanism. These weekly reports identified IP addresses with malware infections that had been reported frequently over the previous fortnight. The data in the AISI portal now extends beyond one year, so searches can be undertaken of repeated reports of IP addresses for any given period and the results downloaded from the portal.

> letting customers know straight away—however, if a customer asks not to be contacted about malware anymore, a note is made not to call that customer.

All of the large ISPs interviewed are concerned about the perception of spamming their customers and tend to limit their email contacts with them. One large ISP, for example, only sends emails to affected customers on a fortnightly basis, although it uses the data internally on a weekly basis:

> We send an email to affected customers on a fortnightly basis (not more regularly). We use the data weekly internally. We don't want to overwhelm customers or spam people. (Large ISP)

Difficulties and improvements

Using the AISI report does not seem to present any major difficulties for large ISPs.

One ISP likes that the formatting of the AISI report has remained consistent, while the more detailed and targeted information makes its messaging to customers more consistent and substantial:

> We are happy with the AISI report. The formatting of the AISI reports is consistent which is good. The information is getting richer. There is more explanation of specific events and details per event. [Also the report has changed in the last month or so.] The details provided in the reports make our messaging to customers more consistent and fuller also. (Large ISP)

One large ISP is concerned that approaching customers about a malware infection without overwhelming them with too much extra information is a delicate balance. When asked about areas of possible improvements for the AISI, large ISPs made a number of suggestions, both on providing more information and using a different format.

Suggestions for content

One large ISP has difficulties reconciling all the data to all customers.

Two large ISPs note that having the source port information in the reports is critical, but that this information is not always available in the reports. In cases where there are many network users behind a given IP address, the source port can help identify the individual computing device that is infected.

Suggestions for format

Rather than a portal, one large ISP suggested having a consumer web system that gathers information directly from the web service into a threat management system.

Another suggestion was to have a more user-friendly, self-help website to help consumers identify what to do and enable them to search for more information on specific malware infections.

One ISP commented that there is insufficient information on the website about particular infection types and that it does not appear to keep up with changes reflected in the AISI reports. It advocated updating the AISI website with the most current information from the AISI reports.

Suggestions for improving how government helps with malware infections

When asked for possible improvements in how government helps with malware infections (outside of the AISI reports), two of the five large ISPs recommended consolidating the number of agencies dealing with cybersecurity. Having multiple agencies can be confusing and, according to one ISP, there is a real lack of coordination on cybersecurity and public messaging in this area. That ISP pointed to a need for a whole-of-government approach to coordinate information and activities:

> The number of agencies that deal with cybersecurity issues can be confusing. (Large ISP)
>
> There is a real lack of government coordination on cybersecurity and public messaging in this area [the way government assists malware infections]. (Large ISP)

There was also a concern that government and industry are not sufficiently preparing for the future:

> We don't have the basic 'stuff' such as anti-virus software, so what about smart fridges and smart cars in the future? (Large ISP)

Information and feedback

To prevent viruses occurring and inform customers about malware infections, most large ISPs provide general information on internet security on their website, with questions and answers on different security topics. However, one ISP's approach is to simply direct its customers to the ACMA's AISI website for more information.

Over-the-phone help is generally provided as part of a normal help-desk function, with no dedicated team to advise on cybersecurity issues. Customer care staff usually deal with these issues; however, their limited knowledge about how to address malware viruses and related concerns means they can only provide general guidance, and cannot help customers remove malware. Staff will often suggest that customers seek an independent ICT technician's advice. One large ISP has a separate business line, offering technicians who can provide immediate action to help with malware infection—but at a cost.

One large ISP handles government and corporate clients separately, as they require different support to residential customers. Government and corporate clients usually have their own IT team to deal with malware viruses and related problems. Identifying affected customers can be an issue for businesses using many computing devices.

Large ISPs receive various type of customer feedback—both positive and negative.

- one ISP does not receive much feedback at all
- three ISPs perceive that, in general, customers don't like being contacted, even in cases where the report is about a malware infection on their service
- one ISP says its customers are grateful for notifications about malware on their network and happy to be contacted—many of its customers are not technically knowledgeable and have no idea that an infection/virus is on their system.

Overall, there are various types of feedback from customers:

- disbelief that the ISP is contacting them
- hostility and resentment that the ISP is monitoring their data
- appreciation that the ISP is helping them
- wanting to be left alone—'I don't care' attitude.

Proportion of malware infections

Most large ISPs have a small proportion of customers affected by malware infections. One large ISP notes that high traffic on its network does not equate to an increase in malware infections. Another has done some analysis and is surprised by the very low percentage of customers affected by malware infections. However, three of the five large ISPs interviewed suspect not all infected customers are detected in the AISI reports.[12]

Large ISPs don't necessarily know the extent to which malware infections are resolved by customers, although two ISPs have a lot of customers repeatedly affected by malware infections. One ISP has a threshold in place for customers that are repeatedly affected—notifying a customer up to three or four times in six months before they leave that customer alone. Generally, ISPs try not to annoy customers who just want to be left alone. One ISP had tried to contact customers by phone when they saw three reports over six weeks but stopped because this practice was associated with scam phone calls.

Changes

When asked about changes to cybersecurity and related customer assistance practices that have occurred over the past two to three years, large ISPs mentioned either continual improvements or refinements of systems in place, or no changes but plans for the future. This included:

- Implementing a total malware solution in response to AISI—including systems and practices to handle the AISI reports, and customer care agents to notify customers and comply with a voluntary code of practice. Every time the ISP's network changes, there are rolling changes to this malware solution.
- Implementing a service that enables parents to manage internet access during certain times of the days—for example, they can block sites so children don't go online during homework time.
- Working on a solution to collect and analyse information from the portal 'on the fly', and to identify a trigger to collect further information from the portal.
- Trialling outbound phone calls to customers affected by malware for six months—however the number of people taking advice was very small, so email has remained the main contact.
- Stopping plans to utilise other data sources that identify malware infections—the AISI reports already include this information.

Among plans for the future, another large ISP is considering a service that alerts customers of phishing activity. However, this ISP is aware that some customers may associated such a service with 'surveillance' activities.

[12] The ACMA makes no claim that the AISI data identifies all infected customers—in fact, the number of infections the AISI identifies is probably only a small proportion of the total number of infections on Australian networks.

Records and reporting

None of the large ISPs interviewed provided information about tracking malware infections that occur on their network.

In terms of reporting to government organisations, the five large ISPs have different approaches:

- Three ISPs indicated they talked to CERT Australia on a regular to occasional basis.
- One ISP is part of the Critical infrastructure Group in the Attorney-General’s Department, an information-sharing forum between carriers, utilities and major retail that convenes to discuss information on their networks two or three times a year. It shares information and incidences that occur on its network.
- Another large ISP initiates contact with CERT Australia on a needs basis—for example, reporting of Russian spam campaigns.
- Two of the large ISPs have infrequent and ad hoc discussions with CERT Australia.

Interviewees did not spontaneously mention any other government organisations.

Appendix 7—Detailed findings for medium ISPs

Practices and process

All of the five medium ISPs interviewed use the AISI daily email reports.

Only two of them were aware of the AISI portal—one had not used it very often, the other not at all. The other three ISPs were not aware of the portal. However, when the interviewer explained more about the portal, two showed interest, particularly in its ability to automate the process of dealing with malware infections.

The five medium ISPs interviewed use a mix of manual and automated processes to deal with the daily AISI reports:

- Three have a manual process in place and, for two of them, the daily AISI report is the main source used to identify malware infections and botnets:
  - One uses the information in the daily reports to pick up on repeat reports and inform customers about infections every week or fortnight.
  - The others relay all the information in the AISI daily reports by getting in touch with affected customers. These ISPs alert affected customers to the fact that they have a virus and advise of the action to be taken.
- Two have automatic processes in place:
  - One ISP has developed software for their residential customers that identifies affected customers from the AISI reports. The information is then made available to technical support who contact customers via phone and follow up by email.
  - The other ISP has a fully automated process whereby AISI information goes into a drop-box and is automatically sent via email to affected customers. This email informs customers that they are affected by malware and asks them to contact customer service.

The AISI daily reports are not the only method medium ISPs use to detect malware infections. While three of the five medium ISPs interviewed mostly rely on the daily AISI reports, two ISPs use other sources, including in-house spam and automated abuse detection systems. Reports generated by these detection systems are used in association with AISI reports, which are useful in providing confirmation of the IP addresses the ISP has separately identified as sending spam. Three of the medium ISPs mentioned that their email and spam filtering systems are a key area of focus and a priority for their business.

Another ISP uses reports from AusCERT[13] and general information from blogs such as AUSNOG[14], SAGE and others as sources of information on malware infections. ISPs also detect malware infections through direct customer contact reporting slow traffic occurring on the network.

One ISP also identifies training as a source of prevention.

[13] AusCERT provides reports of infections associated with given IP addresses.

[14] Blogs such as AUSNOG provide general information about malware infections that are prevalent at a given point in time.

Approach to malware infections

Medium ISPs have diverse approaches to dealing with their customers' malware infections:

- One medium ISP identifies affected customers using the AISI daily report, and then notifies them about the malware infection via phone or email. All the information in the AISI report is passed on. A large customer team of approximately 10 callers is available for this. This ISP's service desk staff doesn't provide advice over the phone about how to remove the malware infection, as they don't have the expertise.
- Similarly, another medium ISP notifies affected customers by phone or email, and provides generic information on how to resolve malware infections (such as reference sites and links where they can get further information). Customers are emailed and phoned a total of three times. After that, if the problem continues to show up on AISI reports, the customers are just notified by email. At that stage, it is considered the customer's responsibility to solve the problem.
- Another medium ISP waits until a large number of problems or a trend is identified on its customer network, and then sends an email to affected customers with fact sheets and information on how to manage the problem. Customers with malware infections are either blocked or suspended until they do a full scan and remove the malware.
- Another ISP will send an email to affected customers with only basic information in order not to confuse them, and ask them to contact customer service. Customers do usually contact the ISP. If they ignore the email and remain on the affected customers list for a month, the ISP tries to assist over the phone.
- Another ISP contacts affected customers by email to advise them they have a virus and of the action to be taken; these customers are also given a copy of the initial AISI report. Customers are given a couple of days before the ISP starts following up to make sure they understand what it means. If no action is taken, the ISP will follow up again and refer to terms and conditions for the use of their network.

Difficulties and improvements

Generally, the use of the AISI report does not seem to present any major difficulties. However, three of the five medium ISPs interviewed mentioned the following issues:

- Perception that some symptoms of malware infection are not currently covered by the AISI report—such as spam, infected routers[15] and infected telephone adapters.[16]
- AISI report information can be too technical for customers to understand.
- Given the high number of reports received for residential customers, one of the medium ISPs finds it challenging to action all of them. That ISP has elected to focus on repeat malware infections.

[15] Spam-infected bots and infected/vulnerable routers are already included in AISI reports.

[16] USB chargers and other devices could theoretically be an infection vector but the ACMA has no evidence this has occurred.

When asked about possible improvements to the AISI daily reports, one medium ISP mentioned that AISI reports don't cover DDoS attacks—this would be a possible improvement as they are currently experiencing multiple DDoS attacks every hour.[17]

When asked for possible improvements in how government helps with malware infections (outside of the AISI reports), three of the five medium ISPs suggested the provision of:

- information on emerging/upcoming malware infection threats, which would allow ISPs to manage and prepare for major attacks before the problem gets too big. This could be delivered in the form of a monthly report or newsletter
- information on problems with customers' routers and telephone adaptors
- further education and awareness-raising programs for citizens about malware risks and cyber-attacks.

Information and feedback

To prevent viruses occurring, medium ISPs inform and help customers with malware infections in a variety of ways. This includes providing:

- general information on internet security and recommendations for use of their network (two of the five medium ISPs interviewed)
- general guides about malware infections including information from AISI reports on their website (three of the five medium ISPs interviewed).

Another source of information was ISPs' customer service or technical support teams, who give customers reference sites and links where they can find more information on how to resolve and prevent malware. For one medium ISP, its biggest issue is that customers don't know how to solve the problem, so it provides some help over the phone, as well as a list of IT specialists with whom they have good relationships that customers can contact if they need further assistance. Another ISP mentioned the importance of education and staff training on malware infections, highlighting the need to continually educate their customer service staff on malware issues.

Two of the medium ISPs handle both residential and business customers. One has a lot of malware infection reports for its residential customer and so must deal with notifications of the AISI daily reports differently for those. A higher level of support is delivered for business and corporate customers; for residential customers, the ISP waits to send notifications until bigger problems or trends emerge.

For another medium ISP, the same—limited—level of assistance is offered to both residential and business customers. However, its business customers have their own internal IT assistance to deal with malware infection notifications, and so requires less support from the ISP.

Medium ISPs did not comment much on the nature of their customer feedback, but overall seem to receive both positive and negative feedback.

Two medium ISPs mentioned that customers sometimes question or deny the malware advice/notification and ask for further evidence. When this occurs, the ISP

[17] Some sources of DDoS activity are reported through the AISI, such as open resolvers, which can be associated with DDoS attacks. Most of these DDoS attacks will be from IP addresses that are not located on a given ISP's network—that is, attacks are being made from infected or misconfigured devices on other networks. The appropriate government organisation for advice on DDoS mitigation strategies on Australian networks is CERT Australia.

provides the AISI report and mentions that the information comes from the ACMA, an authoritative government source.

Three medium ISPs mentioned that customers are usually thankful that customer service or technical support has taken the time to contact them and help solve the problem. One ISP mentioned:

> 99 per cent [of] customers were happy to hear … the notification as they wanted to be good network citizens and for the issues to be resolved. Very few customers were unresponsive. (Medium ISP)

Proportion of malware infections

At four of the five medium ISPs, only a small proportion of customers is affected by malware infections—three estimated this proportion at under one per cent.

A couple of medium ISPs interviewed also mentioned that while a lot of their residential customers are affected, they see a lower number of malware infections for their business/corporate customers. No estimate for the proportion of customers with malware infections was provided.

Changes

When asked about changes to cybersecurity and related customer assistance practices that have occurred over the past two to three years, three of the medium ISPs mentioned improvements or refinements of the systems in place:

> One had started using the AISI reports in 2013 and had become more proactive in dealing with customers' malware infections as a result.

> Another had developed automatic processes and was now looking at having a rolling five to 10 days use of IP addresses. That ISP also mentioned Carrier Grade Network Address Translation (CGN), which will require the need for IP address, source port and IP destination address.

> A third had improved the way it relays information to customers. Although the practices themselves have not changed, that ISP now provides more technical assistance to its customer, helping resolve issues more quickly and with less hassle.

One medium ISP considered there had been no changes.

Another ISP hired a new security manager to oversee security changes, with plans to consolidate and improve processes in the next three years. This is considered an increasingly important issue for the business as the malware infection worsens.

Records and reporting

Two medium ISPs use their ticketing system to track information about malware infections, albeit in slightly different ways:

> For one, the ticketing system is mainly used to help its approach to repeat malware infections—it proactively contacts these customers and guides them to resolve the problem. The ticketing is not used to go back and analyse data or report on malware infections on their network.

> For the other, the ticketing system is mainly used to keep internal records of malware infections on its network, so that reports can be produced.

One ISP does not keep track or monitor persistent malware infections that occur on its network, while two ISPs provide no information about tracking.

Only one of the five medium ISPs contacts government organisations and other relevant bodies about malware infections, including AusCERT, the Attorney General's Department and ASIO (about intercept issues), and has contacts at multiple layers.

The other four medium ISPs have not had to report any risks to any external agency. Two ISPs are aware of AusCERT and receive their reports on malware infections. One ISP nominated CERT Australia as the government organisation ISPs can report to if there is a big malware infection incident.

Appendix 8—Detailed findings for small ISPs

Practices and process

Eight of the nine small ISPs interviewed use the AISI daily reports received by email. One small ISP was not aware of the AISI daily report or the portal.

The small ISPs mainly use manual processing, with only one having a fully automated system in place to process the reports and email notifications to affected customers. That system generates a daily summary with the number of emails sent out.

Other small ISPs review the AISI reports manually. This involves a physical search for the IP address to identify and contact the affected customers, usually by email. One small ISP contacts customers either by email or by phone.

Few small ISPs are using the AISI portal. One of the nine small ISPs interviewed uses the portal to search for more information on malware incidents if the affected customer requested it, but prefers using the daily email report because it goes into their ticketing system. Another ISP has used the portal in the past. Two small ISPs were not aware of the portal and were provided more information about it. The remainder of small ISPs were aware of the portal but do not use it.

For four of the eight small ISPs using the daily AISI reports, these are the sole method of detecting malware infections on their customer network. Other small ISPs have a range of prevention systems in place, including:

- traditional firewall intrusion prevention systems
- specific packages that deal with malware detection and alerting
- AOL and Yahoo reports
- AusCERT reports
- checkpoint platform—a security platform that covers anti-bot and anti-malware
- DDoS mitigation software tools.

Approach to malware infections

Small ISPs have relatively similar approaches to notifying their customers of malware infections. Slight differences are apparent in the extent of information shared with customers:

- One ISP provides quite a lot of information to affected customers, including the information that comes from the AISI/ACMA and the date, time, IP address and nature of the infection. It recommends its customers do a virus scan and update their operating system. Finally, it provides contact details and links to the Stay Smart Online website.
- Two small ISPs invite affected customers to contact their customer service.
- One small ISP prefers not to mention the ACMA so customers don't think they are being monitored.

The level of assistance provided to affected customers varies.

- Three of the small ISPs provide phone help to affected customers to remove malware infections, including help to install antivirus software or scanning programs. If the problem is more complex, they suggest the customer contacts an

IT technician—one ISP has a few computer technicians they recommend to customers.

- One small ISP with corporate clients goes to the client's site to help remove the malware infection.
- Two small ISPs with both wholesale service and managed services take a different approach depending on the type of customer. Customers of the managed service are provided a full clean-up service, whereas information in the AISI report is forwarded to wholesale customers so they can take action themselves.
- For another ISP, the action taken depends on the customer—more support is given to big customers.
- One small ISP offers professional ICT assistance to specific customers—for example, patch servers, installing a firewall.

Only one of the nine small ISPs does not provide any help to its customers—it just notifies customers that they are affected by a malware infection.

Difficulties and improvements

For small ISPs, using the AISI report does not seem to present any major difficulties. One of the nine small ISPs has problems using the daily reports when insufficient data is provided, while another has an issue identifying the affected devices.

Other small ISPs mentioned some areas for possible improvements, either to the content or format of the information provided by the AISI.

Suggestions for content

A small ISP said:

> Daily AISI report[s] could be improved by providing more up-to-date time stamps. Some of the reports have a time stamp from a few days prior.

The same provider also queried if there is a way to check if the malware infection reported has been removed when the time stamp is from a few days ago.

Another small ISP recommended that the AISI portal indicates when a report is completed, so that ISP knows the problem is resolved.

Suggestions for format

One small ISP would like to be able to automate its system so that emails can go directly to affected customers—for example, a .csv or an Excel file to upload to a server.

Another small ISP is interested in receiving additional information and documentation from the ACMA that it could attach to emails to affected customers—for example, a two-page document with information about the malware infection, spam protection programs and other basic recommendations.

One ISP suggested that information on the latest malware infections could be made accessible to customers on the AISI portal.[18]

[18] The AISI section of the ACMA website only describes the most prevalent types of malware infections. See pages 19-20 for the ACMA's response to this suggestion.

Suggestions for improving how government helps with malware infections

When asked for possible improvements in how government helps with malware infections (outside of the AISI reports), three of the nine small ISPs interviewed proposed providing:

- information on where customers go to find information on malware infections, and how to prevent and resolve them
- feedback from government on serious malware infections, what has been done and the outcomes it achieved
- more information on IP reputation lists—that is, blacklisted IPs.

Information and feedback

To help prevent malware infections on their customers' networks, three of the nine small ISPs interviewed provide educational material. This includes:

- online blogs to educate customers on how to deal with malware and encourage them to keep their security systems up to date
- customer newsletters that publicise malicious content and infections to be aware of, and how to mitigate them
- very basic information on their website.

One small ISP sends information at customers' request—for example, an urgent Microsoft update.

Not all of the small ISPs commented on the nature of the feedback they receive from customers affected by malware infections. Of those who did:

- Four tend to receive positive feedback—customers are grateful for the notification and advice provided.
- Two do not receive any feedback because they send automatic notifications—it is left to the customer to resolve the problem or contact the ISP. As a result, it is hard for the ISP to know if the customers have acted on the report.
- Two have had customers question the authenticity of the contact. Apple Macintosh users are most uncooperative because of the perception Mac computing devices don't get viruses.

Proportion of malware infections

Only a small proportion of customers of the small ISPs are estimated to be affected by malware infections—fewer than one per cent of customers, with an average of between two and five reports per day.

Changes

When the small ISPs were asked about changes to cybersecurity and related customer assistance practices that have occurred over the past two to three years:

- Three reported no changes.
- Three had starting using the AISI reports and improving internal policies to detect and prevent malware and botnets. One of these ISPs had previously only dealt with the problem on a case-by-case basis when contacted by customers; another had only been monitoring high upload usage in its network.
- Three mentioned continuous improvements of their IT security system with emphasis on education, detection and prevention. One has changed how it manages both internal systems and client assistance—introducing a new service

where it manages malware threats and attacks for its clients. Another small ISP has invested in checkpoint platform to improve network visibility.

Records and reporting

Only four of the nine small ISPs interviewed commented on whether they are tracking and reporting malware infection information on their networks. Two do not keep any records, while the other two record malware infections as part of their ticketing systems and can trace security issues on their network.

In terms of reporting to government organisations, only one of the nine small ISPs has a security incident-handling procedure whereby it reports cybersecurity incidents to external authorities. For commercial customers, small ISPs work with CERT Australia; for government customers, with the AFP. The ISP mentioned has regular contact with these organisations.

Other small ISPs had no major cybersecurity incidents to report. Three small ISPs would probably inform the ACMA if they had a need, while two would go to the AFP. One small ISP was aware of AusCERT.

Appendix 9—Detailed findings for educational institutions

Practices and process

All of the educational institutions interviewed use the AISI daily reports received by email. None used the AISI portal, and the reasons for this varied:

- all universities are aware of the portal, but have not found value in using it—they consider receiving email alerts is easier than having to retrieve the information
- one university prefers the daily email reports because it allows for everything to be in their ticketing system
- one university says the portal is not part of its routine and suggests the ACMA sends a monthly reminder with a summary of what's on the portal.

Universities have computing devices that are well protected against malware and cybersecurity threats, and have easy access to their own IT personnel.

The AISI daily reports are not the only methods educational institutions use to detect malware infections, with participants mentioning the following range of methods:

- basic antivirus
- endpoint antivirus
- netflow network traffic data
- metadata analysis
- Shadowserver reports
- centralised dashboards to monitor activity on the network
- statistical tools on the network
- visualisation tools on monitors to detect unusual activity
- email filtering
- intrusion detection system (IDS)
- firewalls
- AusCERT reports.

Approach to malware infections

Five of the educational institutions interviewed—four universities and one educational network—currently manually process the information in the daily AISI reports; one is looking at ways to automatically process these reports. For the universities, the small number of computer compromises they receive in AISI reports means a manual approach to processing this data is sufficient. One reason for the small number of reports may be the cybersecurity and malware protection measures they take to safeguard on-campus computer networks and systems, which are also supported by a team of IT personnel.

All educational institutions interviewed tend to use the AISI reports in a similar way—to map it to the source port to identify what user to notify. Some educational institutions remove malware infection for the users or ask local IT staff to do it; others just notify the users and ask them to remove it.

Depending on categories of users—staff or students using university devices, or students using their own devices—educational institutions will support the user to deal with a malware infection. Students using their own devices are usually notified but do not receive support to remove the malware infection; they have to do it themselves.

All 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 help staff and residential students to fix problems. Affected staff are sent an initial email notification about a possible computer compromise and are then expected to request support from their faculty's IT staff if they cannot resolve the issue themselves.

Students are usually notified by email of the malware infection. Some universities block accounts identified as having malware infections until they are cleaned. One university gives three notifications before locking the account.

One university disables the affected account as the best way to make students contact them. These students are then directed to IT services for help removing malware and installing proper antivirus. That university provides a free antivirus software for staff and students to download onto their personal computer equipment.

Universities also tend to address each of the compromised computer cases they receive.

Difficulties and improvements

Overall, the educational institutions are satisfied with the AISI reports—the information is simple and corresponds to what they need. Two universities see no need to improve them, while one mentioned that the reports never had a 'false positive' and this situation should remain.

Two universities find it difficult to identify affected computing devices (as one IP address could represent many computing devices) or lack information on IP addresses—for example, the use of translated IP addresses. One university is unable to identify or link compromised computer listings with some students, particularly those using wireless devices.

When asked, three universities had suggestions for possible improvements:

> Two suggest adding more information or commentary in the report on how the infection/malware/spam is affecting its users, to decrease the time needed to communicate and research the malware infection internally. When universities pass on the information to IT support internally or to their users, having an authoritative source to rely on would be helpful and save time.

> One suggests some trending analysis may be useful to provide historical information on the malware infection when staff go on leave.[19]

When asked for possible improvements in how government helps with malware infections (outside of the AISI reports), one educational network suggested implementing a mechanism for the sector to prevent large-scale attacks, such as DDoS. Another suggested scanning for FREAK vulnerabilities, while one said more

[19] Historical information is available in the AISI portal.

could be done to share information—for example, for government to provide analysis of upcoming malware risks.[20]

Information and feedback

Universities provide information about preventing malware infection in a range of ways. While one educational network does not provide any information as it has network IT specialists available to help, other universities tend to provide information on their website, including links to the government's Stay Smart Online website. On the same page of that university website, students can also find a link to free antivirus software.

The majority of the educational institutions interviewed do not always receive feedback from users, but when they do, it tends to be positive—users are usually quite grateful the malware infection has been detected. Universities do not always know if their users have been able to remove the malware infection, but sometimes do get information from the user that it has been resolved. Other times they know because it stops appearing in the report.

One university has received negative feedback from users not wanting to admit their computer has been infected. That university had to resort to shock tactics with its users to get them to react. Two universities found some of their users to be unresponsive when contacted about malware infections.

The educational institutions interviewed have a very small proportion of users affected by malware—with reported weekly infections ranging from a couple to 12–15 infections. This represents a small proportion of the network.

Changes

Any changes that had occurred in the educational institutions over the past two to three years were in response to their external environment, requiring them to adapt or refine their IT security processes/practices. External changes mentioned were:

- DDoS—one university said these had been ramping up and it needed more resources to respond to the problem
- the increasing number of users using their own devices (rather than university-supplied), which makes it more difficult to handle malware infections.

Other universities mentioned internal incremental changes to their processes, including:

- refreshing their own IT networks to provide greater network visibility
- modifying settings in their wireless network, enabling them to reduce the infection rate
- starting to use the AISI reports; for one university this was only in the past year.

Records and reporting

None of the educational institutions interviewed track the number of malware infections on their network per se. However, three are able to use their ticketing system to record and track the information. One university keeps records of any alerts received about malware and cross-reference them with new alerts. In cases of repeat incidents, they

[20] FREAK is an SSL/TLS security vulnerability that potentially allows communications to be decrypted. The ACMA started reporting FREAK and other vulnerable service data through the AISI in March 2015.

use the information to clean malware infections on computing devices and educate the users.

Educational institutions do not regularly report incidents to government organisations and other relevant bodies:

- one university reports activity to CERT Australia but only infrequently (at most once a year)
- one educational network has discussed becoming one of CERT Australia’s partners
- one educational institution has reported DDoS attacks to the AFP
- one educational institution reports phishing campaigns to AusCERT each time it happens so the phishing webpages can be removed
- two of the five educational institutions have not have incidents that require them to report to external organisations
- one university has asked a government organisation to contact a company overseas for notifications of malware infections.

It is not clear whether respondents correctly distinguish between CERT Australia and AusCERT or use those terms interchangeably.

researchacma

Canberra
Red 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 32
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.gov.au