Australian Government

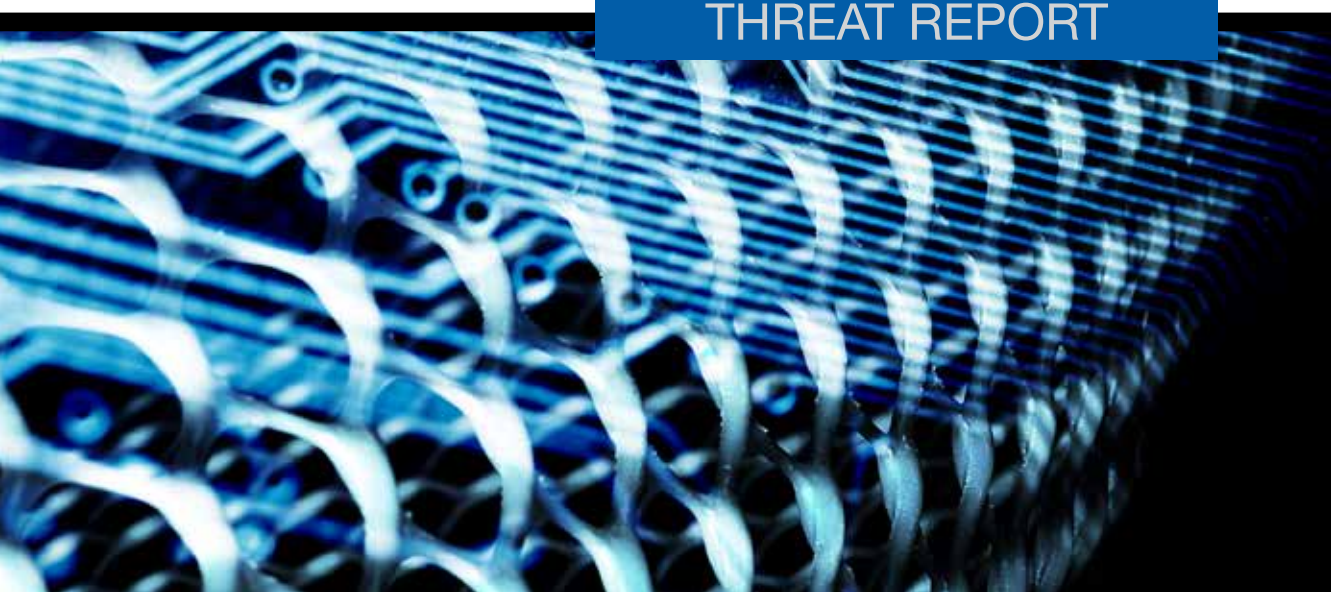
Australian Cyber Security Centre

ACSC

AUSTRALIAN CYBER SECURITY CENTRE

2017

THREAT REPORT



Contents

Foreword 2

About the Australian Cyber Security Centre 4

Executive Summary 15
- Current challenges 15
- Broader trends 16

Current Challenges 26
- Ransomware 26
- Credential-harvesting malware 28
- Social engineering 29
- Threats associated with outsourcing and supply chain 33
- Personally identifiable information 38
- Malicious use of leaked tools 38
- Router scanning 40
- Distributed Denial of Service threats 41
- Internet of Things (IoT) 41
- Prevention as an investment 43

Broader Trends 46
- Cybercrime 46
- Cyber espionage 48
- Cyber attack 50
- Cyber terrorism 52
- Threat to Government 52
- Threat to the Australian private sector 55
- Threat to financial institutions 59
- Threat to Australian academic institutions 59

Further information 60
- The Australian Government Information Security Manual (ISM) 60
- Strategies to Mitigate Cyber Security Incidents 60
- Stay Smart Online 60
- Contact details 60

Foreword

The last year has again demonstrated the growing public appetite to understand and defend against the evolving cyber threats facing Australia. High profile incidents of cybercrime have exemplified the speed with which cyber threats can propagate globally, how rapidly adversaries can adapt to security responses, and how easily a compromise can impact an organisation's core functions or services.

There are thousands of adversaries around the world willing to steal information, illegally make profits, and undermine their targets. Malicious software in the form of ransomware – such as the WanaCry incident – is deliberately crafted to exploit known vulnerabilities and take advantage of gaps in cyber defences. Australia was not significantly impacted by WanaCry, but as tradecraft and threats adapt and evolve, adversaries will act faster to exploit new vulnerabilities and develop more innovative approaches.

The ACSC has observed two distinct trends when it comes to the level of sophistication employed by adversaries and cybercriminals. At one end of the spectrum, increasingly sophisticated exploits are being developed and deployed against well-protected networks, particularly government networks. This reflects investment in new tools and techniques to keep pace with our efforts to protect networks. On the other end, the ACSC continues to observe many adversaries, particularly criminals, compromising networks using publicly known vulnerabilities that have known mitigations. Too many of the incidents the ACSC responds to could have been prevented had organisations employed established and relatively straight-forward cyber security measures. WanaCry, for example, used a publicly known vulnerability that had been patched months before and that the ACSC had publicly reported.

Also worthy of highlighting has been the global campaign by advanced adversaries to compromise some private sector providers of ICT services, including ICT security. Some managed services providers and ICT providers around the world, including in Australia, have been compromised by these adversaries. And of concern, we know that through this compromise, adversaries have accessed the networks of some of these companies' clients. The ACSC has been working with affected services providers, but when even ICT security providers are being compromised and exploited, it is a clear wake-up call for everyone to be conscious of contemporary cyber security risks and best practice mitigations.

Defending a network from compromise is far less costly than dealing with the costs of compromise. The old adage of "good security is built in, not tacked on" still rings true today. Cyber security must be a consideration at the start of a project, not an afterthought when critical vulnerabilities are discovered. The Australian Signals Directorate's (ASD) Essential Eight provides a prioritised list of practical actions that organisations can take to make their computers and networks more secure. These are the answer to the cyber threat and are now considered to be the baseline for Australian organisations. Additionally, CERT Australia's Stay Smart Online program provides simple, easy to use advice on how to protect yourself online as well as up-to-date information on the latest online threats and how to respond.

Looking forward, the ACSC will maintain a focus on providing world-leading advice to protect Australia's most sensitive information from highly skilled adversaries and criminals. We will also work with the Australian private sector to ensure that a strong security baseline is in place to stop opportunistic adversaries getting 'easy wins'. While government plays a role, the responsibility remains with all of us – individuals, the private sector and government – to increase the effectiveness of our prevention, detection and response capabilities.

Next year will see the ACSC adapt our operational response, stakeholder engagement and technical capabilities. As the Prime Minister announced in July, the Independent Review of the Intelligence Community recommended a suite of reforms to the ACSC designed to further boost Australia's cyber security. Among them, the ACSC will grow its 24/7 capability to respond to serious cyber incidents and take a whole-of-economy focus. The ACSC's leadership is working with partners across government and the private sector to develop the model for how this will work. The ACSC will also move to a purpose-built facility, which will allow it to operate at lower-classifications and much more closely with the private sector and academia.

For the first time, this year's Threat Report also includes insights into how the ACSC works and highlights some of the ways in which we have both proactively and reactively responded to cyber threats. Due to the sensitivity of some of the information used by the ACSC, and because of our focus on protecting relationships with victims, much of what we do is not visible and very little of the efforts of the staff of the ACSC agencies, or the significant success stories, can be promoted publicly. Similarly, much of the preventative efforts and tailored advice is not recognised. By highlighting our efforts, we hope to build public awareness of the role the ACSC plays within the cyber security environment, and draw attention to the tools and information available to government agencies, businesses and the public alike.

Clive Lines
Coordinator
Australian Cyber Security Centre

About the Australian Cyber Security Centre

The ACSC brings together key operational elements of the Government's cyber security capabilities in one facility to:

- enable a more complete understanding and sharing of sophisticated cyber threats
- facilitate faster and more effective responses to significant cyber incidents
- foster seamless interaction between government and industry partners.

We work with government and business to reduce the security risk to Australia's government networks, systems of national interest, and targets of cybercrime where there is a significant impact to security or prosperity.

The ACSC is the focal point for the cyber security efforts of the Australian Signals Directorate (ASD), Computer Emergency Response Team (CERT) Australia, the Defence Intelligence Organisation (DIO), the Australian Criminal Intelligence Commission (ACIC), the Australian Federal Police (AFP), and the Australian Security Intelligence Organisation (ASIO).

ASD is the Commonwealth authority for cyber and information security and provides advice and assistance to Commonwealth and State authorities on matters relating to the security and integrity of information that is processed, stored or communicated by electronic or similar means. ASD undertakes its cyber and information security mandate from within the ACSC and is the lead for the operational management of the Centre through the position of Coordinator ACSC. In addition, ASD carries out an intelligence mission in support of its cyber and information security mandate.

CERT Australia is the Government lead for cyber security issues affecting major Australian businesses including owners and operators of Australia's critical infrastructure and other systems of national interest. CERT Australia helps these organisations understand the cyber threat landscape and better prepare for, defend against, and mitigate cyber threats and incidents through the provision of advice and support on cyber threats and vulnerabilities.

DIO leads the ACSC's Cyber Threat Assessment team – jointly staffed with ASD – to provide the Government with an all-source, strategic, cyber threat intelligence assessment capability.

The **ACIC** provides the Australian Government's cybercrime intelligence function within the ACSC. Its role in the Centre is to discover and prioritise cybercrime threats to Australia, understand the criminal networks behind them and initiate and enhance response strategies by working closely with law enforcement, intelligence and industry security partners in Australia and internationally.

The **AFP** is the Australian Government's primary policing agency responsible for combating serious and organised crime and protecting Commonwealth interests from criminal activity in Australia and overseas. The AFP's Cybercrime Investigation teams within the ACSC provide the AFP the capability to both undertake its own targeted intelligence and to investigate and refer matters for prosecution for those believed to have committed cybercrimes of national significance.

ASIO's role is to protect the nation and its interests from threats to security through intelligence collection, assessment, and advice for Government, government agencies, and business. ASIO's cyber program is focussed on investigating and assessing the threat to Australia from malicious state-sponsored cyber activity. ASIO's contribution to the ACSC includes intelligence collection, investigations and intelligence-led outreach to business and government partners.

For more information about the ACSC, visit *https://www.acsc.gov.au*

Business

- Commercially sensitive information
- Client information
- Bulk-data containing personal information about the public
- Sensitive legal advice
- Proposed negotiating positions
- Budgets
- Marketing strategies
- Work history
- Intellectual property
- Staff information

Government

- Commercially sensitive information
- Communications between politicians
- National security information
- Policy working documents
- Bulk-data containing personal information about the public
- Proposed negotiating positions
- Sensitive legal advice

WHAT MAKES YOU A TARGET?

Home User

- Social media accounts
- Email accounts
- Banking logins
- Personal information, including photos and personal files

ICT Provider

- Client network information
- Direct access to client networks
- Network security architecture details
- Access to global corporate networks
- Customer passwords

8

ACSC CONFERENCE: THE AUSTRALIAN GOVERNMENT'S FLAGSHIP CYBER SECURITY EVENT

The ACSC Conference has grown to become one of the largest of its type in Australia. It is the flagship event for the ACSC and a high-profile demonstration of the Australian government's leadership in cyber security and commitment to industry.

The conference has seen an increasing number of delegates and sponsors each year. In 2017, there were more than 1400 attendees, 76 industry sponsors and exhibitors and over 100 speakers across eight streams.

The conference is now an established drawcard for other, more specialised cyber security events during the week. It also provides integrated training and networking opportunities as part of the official program. The 2017 ACSC Conference was a National Finalist and Territory Winner of the CIM Magazine Best Meeting or Conference.


2017
CONFERENCE
CARBON BLACK
RSA
CYBERARK

11% of the **global** information security workforce **are women**

Women in Cyber

Some estimates indicate that women comprise only 11% of the global information security workforce*.

The ACSC is proud of its representation of women represented across the organisation. While acknowledging that there is still progress to be made, the ACSC significantly outperforms the reported global averages.

- The ACSC's Leadership Group, made up of senior executives and key representatives from across partner agencies, is 50% women.
- Within ASD's Cyber and Information Security Division – which sits within the ACSC and is the largest single agency component – women make up 30% of staff. Many of the core elements of ASD's cyber security mission are led by women, including:
  - Cyber security operations and incident response
  - Cyber security tradecraft analysis
  - Strategic communications
  - Industry partnerships and accreditation, including Information Security Registered Assessors Program (IRAP)
  - Advice and assistance to government
  - Cyber security policy and international engagement, and
  - Capability development (development and integration of sophisticated technical capabilities).
- The CERT Australia and the ACIC senior executive leads to the ACSC are women; and one of the three ASD senior executives within the ACSC is a woman.

**The 2017 Global Information Security Workforce Study: Women in Cybersecurity*

WOMEN IN CYBER

30% of ASD's Cyber and Information Security Division workforce — the largest within **ACSC** — **are women**

RELOCATION OF THE ACSC FROM THE BEN CHIFLEY BUILDING

Later this year, the ACSC will start moving to a purpose designed facility. This will enable the ACSC to operate at multiple security classification levels demonstrating the Government's intent to build meaningful and effective cyber security partnerships with the private sector.

The move will lead to a new business model for cooperation across the ACSC member agencies, extending the current collocation model towards a more integrated and collaborative approach.

The state-of-the-art facility will encompass two buildings in Canberra's Brindabella Park. It will better enable the ACSC to operate on a 24/7 basis to meet Australia's cyber security requirements, and to engage with industry, academia and Government as both customers and partners.

A key priority for the ACSC will be to adapt our operational response, strategic engagement and technical capabilities to take advantage of the opportunities available at the new facility, including:

- adapting incident triage and the ACSC Watch capability
- developing a more integrated model for tracking operational events or incidents across partner agencies
- enhancing engagement with the Joint Cyber Security Centres as they are established to engage industry in cyber security collaboration with government
- streamlining the development of a cyber security incident communications capability aimed at the public
- developing business processes to ensure the smooth integration of staff with security clearances at lower classification levels.

Executive Summary

Current challenges

Cybercrime remains a pervasive threat to Australia's national and economic prosperity, with cybercrime expertise improving and tradecraft being adapted to target specific businesses. Cybercrime will continue to be an attractive option for criminals due to its ability to generate large profits with a low risk of identification and interdiction. Each successful compromise encourages further cybercrime activities.

Ransomware continues to grow as a method of extorting funds from a wide range of victims. It is one of the most prevalent financially motivated cybercrime threats worldwide and is likely to remain so due to its continuing success.

Credential-harvesting malware poses an increasing threat to Australians by facilitating the theft of credentials, such as login details and account numbers. The ACSC has observed a shift in cybercriminals' targeting and capability, specifically their development of expertise and malware to target Australia and the increased targeting of Android smartphones.

Social engineering is growing in sophistication and is likely to be increasingly employed by malicious adversaries to disguise their illicit activities as genuine. As Australian network defences harden and are therefore more resistant to cyber intrusion, social engineering provides a way to bypass security protocols that cybercriminals may not be able to overcome via technical means.

Adversaries have increased their targeting of trusted third parties, particularly service providers. These companies are highly attractive targets as they can enable secondary and tertiary access into a range of primary targets. Some Australian networks of global service providers have been compromised, and through them, so have some of their customer's networks.

Cybercriminals continued to seek access to repositories of large amounts of personally identifiable information (PII) to facilitate financial crimes and identity theft.

Security in Internet of Things (IoT) devices, such as smartphones and tablets, is not always a top priority during their creation. Their increased integration into the ecosystem introduces significant security risks.

The scale and impact of Distributed Denial of Service (DDoS) activity has set new records for volume through both traditional approaches and by exploiting newer methods such as co-opting IoT devices.

The ACSC and its international partners observed the targeting of Australian routers by malicious, sophisticated adversaries. This activity uses automated scanning to identify vulnerable routers, and subsequently extracts configuration files. Accessing a router's configuration may ultimately allow a malicious adversary to modify the router settings, enabling control of internet communications that transit the device.

Broader trends

Advanced malicious cyber activity against Australia's national and economic interests is increasing in frequency, scale, sophistication and severity. The reach and diversity of cyber adversaries are expanding, and their operations against both government and private networks are constantly evolving.

At the same time, the ACSC continues to observe malicious adversaries and criminals using rudimentary techniques and known network vulnerabilities to compromise networks that lack baseline cyber security measures. Adversaries of all kinds routinely scan the environment for vulnerabilities, leveraging them to gain and sustain access to victim networks. This opportunistic targeting is simple and cheap, and will continue as long as computers, networks and devices fail to implement baseline security.

Although our cyber defences have gradually improved, especially in government, adversaries have kept pace by adapting their tradecraft and tools to circumvent enhanced security practices. The more advanced adversaries continue to invest in their capabilities, so staying ahead of them remains an enduring challenge.

Foreign states still possess the greatest capability to compromise Australian networks. Over the last 12 months, the ACSC detected extensive state-sponsored activity against Australian government and private sector networks in support of economic, foreign policy and national security objectives.

How has the environment changed?

- The frequency, scale, sophistication and severity of cyber incidents
- More diverse and innovative attempts to compromise government and private sector networks
- The increasing number and scale of DDoS incidents
- Cybercriminal sophistication and deliberate targeting
- Foreign states increasing their level of investment in cyber capabilities

INCREASING THREATS

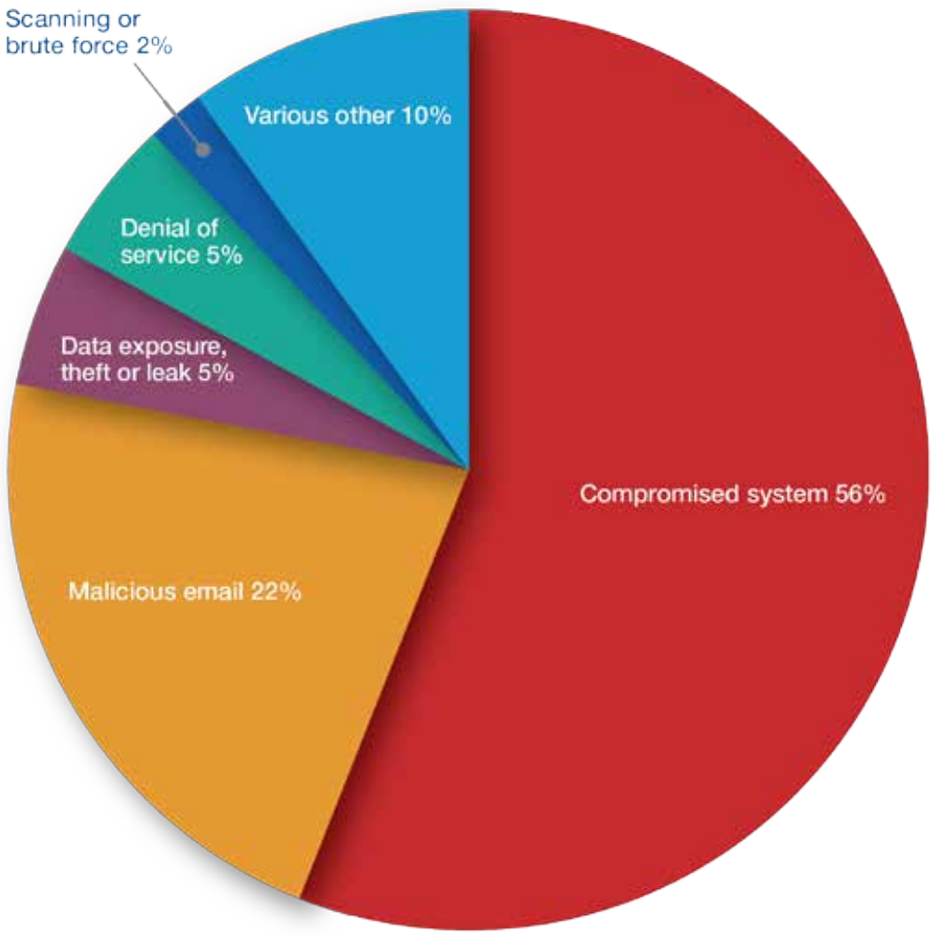


Figure 1: Top 6 private sector self-reported incident types

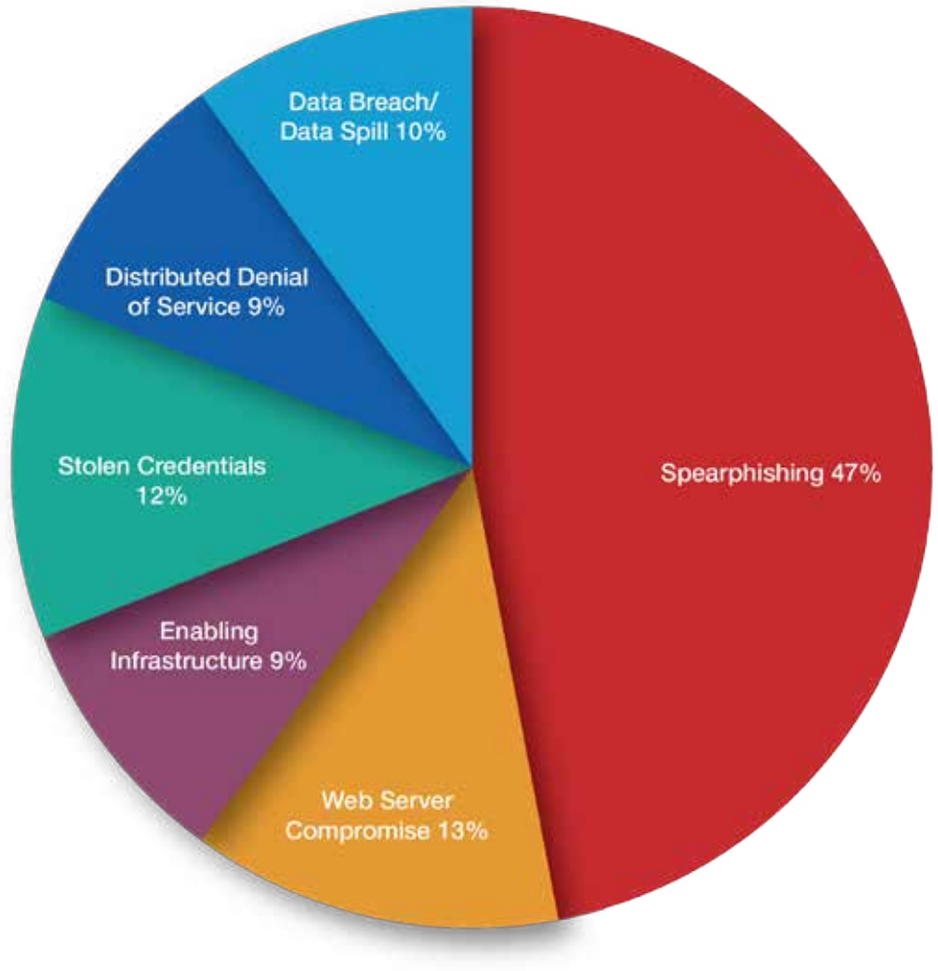


Figure 2: Top 6 government self-reported incident types

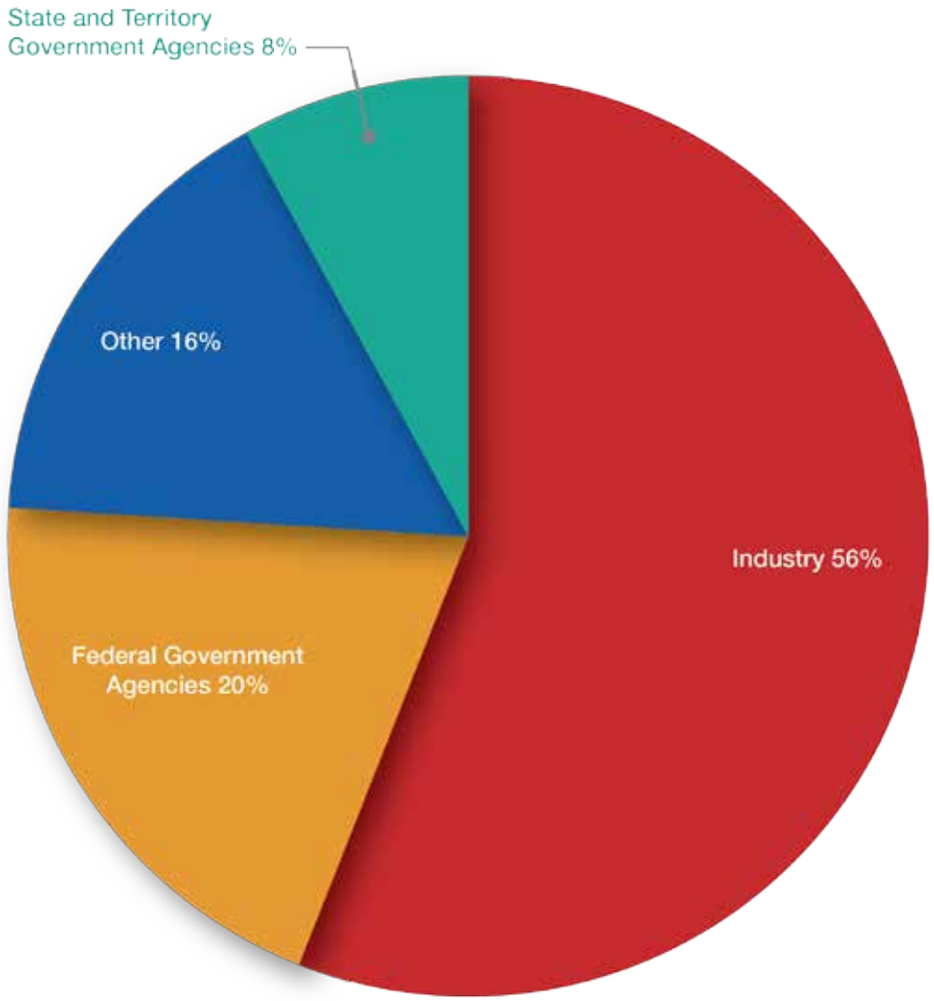


Figure 3: ACSC incident responses by victim type

OUR SOURCES

In addition to responding to reported incidents, the ACSC actively seeks to uncover cyber security threats, vulnerabilities and organisations at risk. Our detection techniques cover a range of classified and unclassified methods, and we are continually working on new technologies that will strengthen our ability to detect increasingly sophisticated malicious cyber activity. Agencies within the ACSC work closely with their international partners to obtain the latest information on emerging threats, intelligence and law enforcement actions around the globe.

The ACSC adjusts efforts to pre-empt particular threats and vulnerabilities to ensure we are well placed to detect malicious activity targeting Australia. This can include activities such as scanning for known vulnerabilities.

The ACSC makes use of a range of open source and commercially available reporting, including relationships with industry providers, vendors, news articles and blogs. Increasingly, the online community is reporting cyber incidents and events at a faster pace than traditional news sources.

WHO WE ARE WORKING WITH

The ACSC works with a wide range of Australian and international organisations to enable our protection and detection missions. These relationships include:

- threat intelligence and incident response companies
- telecommunications companies
- international law enforcement agencies
- the international CERT community
- our foreign partners.

We provide proactive mitigation advice to a range of customers, and publish information across multiple platforms, including OnSecure, the CERT portal, and the ACSC website. The ACSC effectively collates information from this broad range of sources to provide well-informed and timely responses.

The ACSC has responded to cyber security incidents impacting major government departments, large Australian organisations that own or operate critical infrastructure, small to medium enterprises and individual users. We receive cyber security incident reports from Australian Government and we also hear about cyber security incidents impacting Australian industry through CERT Australia's strong relationships. This information enables the ACSC to provide assistance where required.

RESPONDING TO INCIDENTS

Every day the ACSC triages reported cyber security incidents and adjusts its operational responses accordingly. When a cyber security incident warrants an ACSC response, an agency is assigned to lead the activity. Throughout the process, we remain closely engaged with victims about the incident. We draw on each agency's specialist knowledge and professional networks to learn about the intent behind a malicious adversary, and the methods they use to compromise their target. We also consider where else these techniques may have been used and who else could be at risk.

We treat each incident on its own merits. However, there are four key factors we use to guide our assessment of an incident:

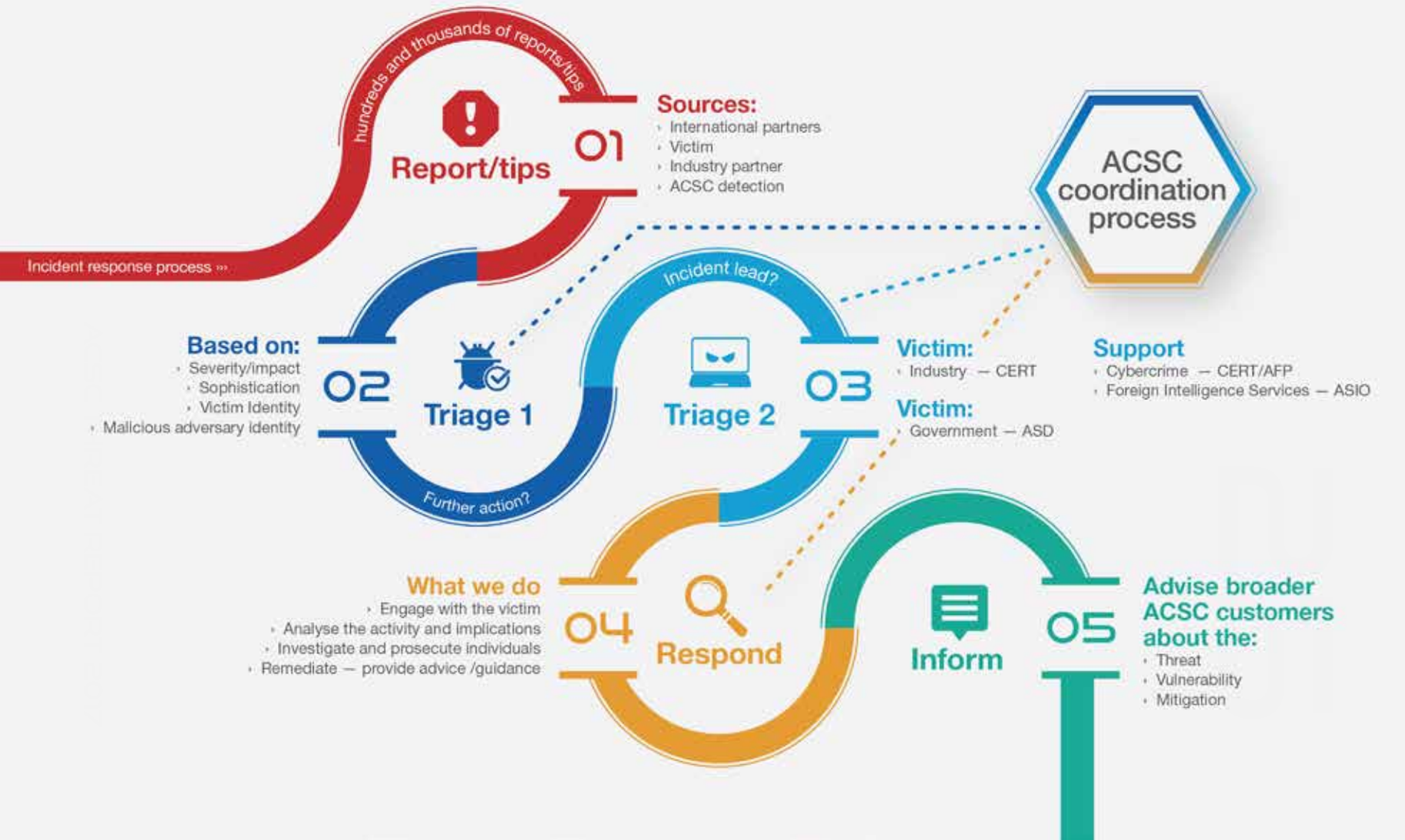
Sensitivity: Sensitivity is about who the target or victim is, the data their network holds, and why they may be of interest to a malicious cyber adversary.

Impact: Impact is defined by the tradecraft being used, what the activity enables on a network, and what security controls might prevent, or limit, potential damage.

Success: Success refers to whether there are any indications that the activity has been successful, and the extent of any potential compromise.

Adversaries: What adversary is attributed to this activity, what is their intent, and what is their level of capability?

These four factors guide the ACSC's triage process, but the greatest value comes from our staff, who use their extensive cyber security knowledge when triaging incidents to ensure the ACSC's response is both timely and appropriate.



Current Challenges

Ransomware

Ransomware continues to be a persistent threat to Australia. It is one of the most prevalent, financially motivated cyber crime threats worldwide and is likely to continue to be so with increasing frequency and variation of campaigns. The primary purpose of ransomware is direct revenue generation; it blocks access to, or encrypts, a victim's data, demanding a ransom be paid to restore access.

Ransomware targets both individuals and businesses, affecting millions of people worldwide. Adversaries develop and release new, more virulent strains of ransomware designed to be more damaging and less detectable.

Some adversaries have expanded their operations to a pseudo-franchise model, dubbed ransomware-as-a-service (RaaS) (Figure 4). RaaS provides entry to the ransomware market for anyone willing to pay, regardless of technical capability. RaaS developers write ransomware, build the infrastructure required to run a campaign and sell it through darknet markets. The infrastructure is generally sold at a low price, with a percentage of profits returned to the vendor. Purchasers (known as affiliates) are generally provided access to a darknet-based dashboard. The dashboard provides a range of capabilities, usually including ransomware customisation, as well as tracking of successful infections and ransoms paid. Affiliates use the infrastructure in conjunction with their own delivery mechanisms, such as phishing campaigns or exploit kits. This model provides the RaaS vendor with a vastly increased victim base for no additional effort.

Growth in the prevalence and sophistication of ransomware is expected to continue as barriers to entry to the cybercrime market decrease and the number of internet users increases. Ransomware campaign development has also become more sophisticated, through using advanced social engineering and making use of known Australian brands and government department identities. In 2016 and 2017, the most common ransomware variants were Cryptolocker, Torrentlocker and Cryptowall.

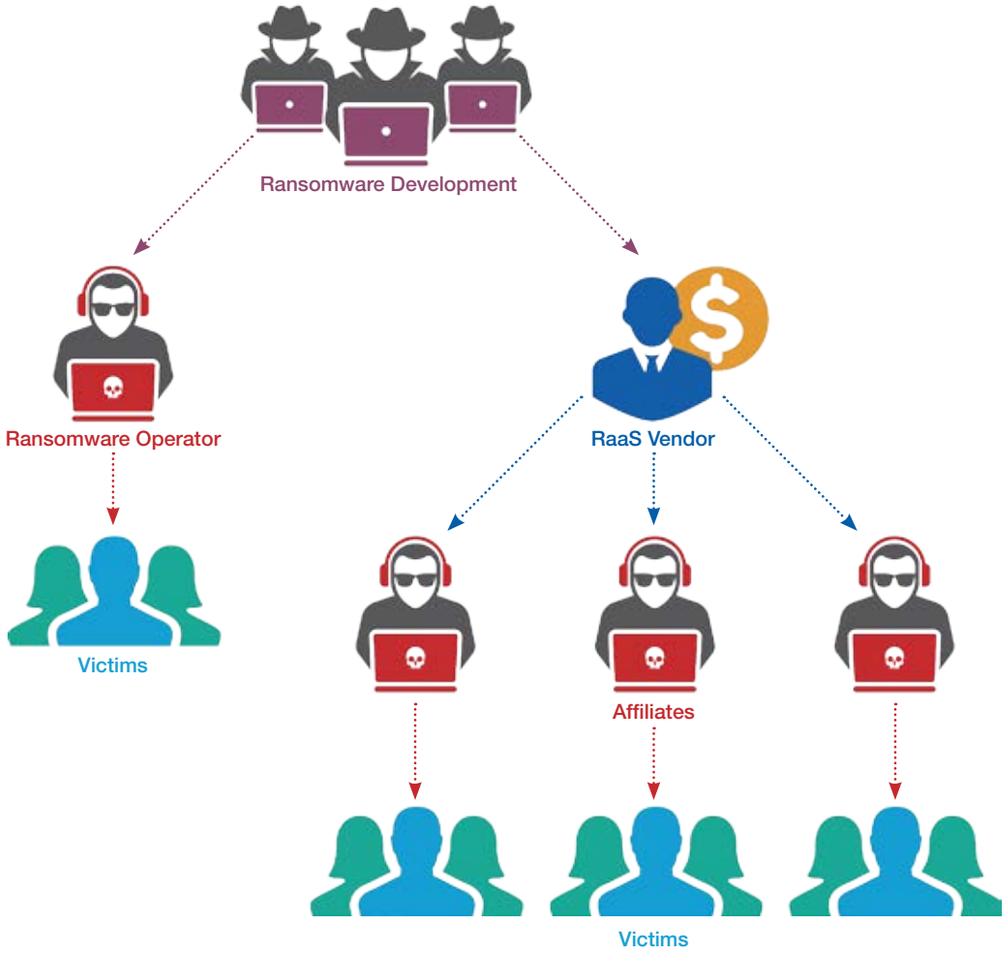


Figure 4: 'Ransomware-as-a-Service' operating model, ACIC

The most commonly reported ransomware delivery method is mass-market untargeted phishing campaigns. Large-scale, untargeted phishing campaigns are generally cheap and relatively simple to run. A fully-patched and protected device can be infected through phishing by the victim downloading a malicious attachment. The second most common form of delivery is through an exploit kit, a software tool kit, which runs on a web service and contains a variety of known exploits to infect visitors to a website with malware. Visitors are commonly infected when they click on a link in a phishing email or false advertisement (malvertisement), or when they are silently redirected from a compromised legitimate website. Exploit kits have the benefit of not requiring a person to download a file – simply visiting a compromised website while running vulnerable software is sufficient.

Notable new variants of ransomware emerging since 2016

Crysis ransomware has the ability to automatically self-propagate through a network to connected devices. Because of this, victims can be automatically reinfected through reconnecting to a compromised device.

Wanacry ransomware (also known as WannaCry, WannaCryt0r or WanaCrypt) leverages a publicly known vulnerability in Microsoft Windows. A patch for this vulnerability was released by Microsoft in March 2017, two months prior to the worldwide incident in May 2017. In May 2017, Microsoft also released further patches for Windows versions that were no longer supported. WanaCry ransomware also has the ability to self-propagate through a network.

Petya ransomware (also known as NotPetya) spread through a compromise of an M.E. Doc software update. M.E. Doc is a Ukraine-based company whose software is integrated within Ukrainian government systems. Once the update was installed, NotPetya then leveraged the same vulnerability used by the WanaCry ransomware to spread to other systems connected in the same networks.

Ransomware pays high dividends and can have very low start-up costs. Cybercriminals almost always demand ransom payment through bitcoin, with payment instructions given to the victim in a ransom message. Ransom amounts vary, but often begin at under A$1000 for individuals, with substantial increases over time. Adversaries usually demand higher ransom amounts from business victims and the amount is specifically designed to be affordable based on the size of the business. The amount can also increase over time to encourage victims to pay the ransom promptly, rather than attempting to remove the ransomware. Paying the ransom doesn't always result in data being unlocked.

Credential-harvesting malware

Credential-harvesting malware poses an increasing threat to Australian networks, in particular to the financial sector, by stealing credentials, such as login details, from the targeted network's systems. The ACSC has observed a shift in cybercriminal's targeting activities and capabilities, specifically the development of expertise and malware to target Australia and Android smartphones.

Credential-harvesting malware designed for smartphones will likely increase due to the amount of information stored on these devices, and their increased use for activities such as online banking and purchases. Similarly, ransomware which targets smartphones will likely increase in the future as people store personal information such as photos and contacts on these devices.

Credential harvesting malware

Gozi malware is one of the longest operating credential-harvesting malware campaigns. First discovered in 2007, Gozi's impact on Australian victims has increased. Gozi was originally operated by a closed group of cybercriminals who consistently upgraded the malware and added new features. Three members of the group were arrested in 2013 but the malware continues to be operated by other cybercriminal groups. Gozi represents how experienced cybercriminals can become a persistent threat to the financial sector and can be resistant to law enforcement intervention.

Mazar is a credential-harvesting malware which affects Android devices. Mazar is spread through unsolicited SMS and pop-up downloads on some websites. It creates malicious 'overlays' designed to replicate legitimate online banking logins that steal credentials. It is capable of intercepting text messages to bypass two-factor authentication.

CASE STUDY

Social engineering

As Australian network defences are becoming increasingly hardened and therefore more resistant to cyber intrusion, social engineering provides a way to bypass security protocols that cybercriminals may not be able to overcome via technical means.

Cybercriminals use social engineering techniques to manipulate human trust and elicit information in support of network exploitation efforts. Social engineering is becoming more sophisticated and is likely to be increasingly used by adversaries to disguise their illicit activities as genuine. As cyber adversaries refine their social engineering tradecraft, legitimate communications are sometimes becoming almost indistinguishable from social engineering attempts. Robust technical controls are becoming increasingly important to protect networks from this kind of malicious cyber activity.

Social engineering can range from broad phishing emails, through to targeted phishing emails, to individually tailored communications. Some of the most sophisticated social

engineering involves simultaneous approaches through different communications platforms, including phone calls. The ACSC has also identified cybercriminals using compromised accounts of networks known to their target in order to support their campaigns.

Social media has created ideal platforms for cybercriminals to obtain personal information to target victims. Malicious adversaries are able to research businesses, use false social media accounts, and compromise legitimate accounts, enabling them to impersonate business and government officials.

Mitigating the threat from malicious emails

While socially-engineered emails can be highly sophisticated, there are ways to differentiate them from legitimate emails. Advice can be found at *https://www.asd.gov.au/publications/protect/socially_engineered_email.htm*

For advice on broader malicious email mitigation strategies, visit *https://www.asd.gov.au/publications/protect/malicious_email_mitigation.htm*

The use of social engineering is particularly prominent in business email compromise (BEC), a scheme which targets businesses for financial gain. While BEC is predominantly considered to be a cyber-enabled crime, there is potential for it to include aspects of cybercrime, for example reconnaissance of a business' systems to identify how that business's transactions are authorised. BEC can take many forms but most commonly involves impersonating a senior employee to change invoice details or generate a sense of urgency to bypass anti-fraud processes. Many cases of BEC schemes rely solely on social engineering techniques and spoofed email addresses, but some also use malware to access computer systems and company information.

Over 2016-17, reports to the ACIC's Australian Cybercrime Online Reporting Network (ACORN) indicated losses of over $20 million due to business email compromise (Figure 5). This was up from $8.6 million in 2015-16, representing an increase of over 230%. This likely represents only a small percentage of total activity as both misreporting and underreporting occurs.

AUSTRALIAN INTERNET SECURITY INITIATIVE JOINS CERT AUSTRALIA AND THE ACSC

On 1 July 2017, the Australian Internet Security Initiative (AISI) transferred from the Australian Communications and Media Authority to CERT Australia. This was a fitting transfer given the cyber security data held by AISI and its alignment with CERT Australia's functions and activities.

AISI provides daily email reports to Australian internet providers identifying IP addresses on their networks observed as infected by malware or potentially vulnerable to malicious exploits. Internet providers are encouraged to use the AISI data to identify and inform affected customers about their malware infection or service vulnerability. This includes providing advice to infected customers on how they can fix the compromise or remedy the vulnerable service.

The data reported through the initiative is supported by an AISI Portal where internet providers can download malware or service vulnerability reports relating to their own networks. A diverse set of data is reported through the AISI, ranging from malware incidents affecting Android, iOS and Windows operating systems, to service vulnerabilities potentially exposing sensitive customer data or allowing devices to cause harm to other internet users. Charts containing information on AISI malware and service vulnerabilities are updated daily on the CERT website.

CASE STUDY

Business email compromise

In 2017, the ACSC observed an increase in business email compromise through targeted phishing emails. Small businesses in particular were targeted by themed phishing emails from known contractors whose systems had been compromised by malicious adversaries. The adversary would gain access to small businesses through malicious PDF files or credential phishing. Within hours of the initial network compromise, new email rules would be implemented that forwarded new emails with certain subjects such as 'invoice' to the adversary's email address. These would then be deleted from the compromised business' email. The adversary would then create new invoices for clients and contractors using the business' branding but containing different banking details. In some cases, the adversary would send out emails advising that bank details would be changing for the next invoice. In these cases, CERT Australia provided remediation advice to the affected businesses and engaged with the AFP and the ACIC in relation to the malicious adversary's activities.

In one instance, a cybercrime adversary posed as a Chief Executive Officer (CEO) and Chief Operating Officer (COO) of a large business and obtained fraudulent payments of over US$500,000. The adversary sent a spoofed email, purporting to be from the CEO (who was travelling at the time), requesting a large payment from the financial controller. A second email, purporting to be from the COO, was then sent to the financial controller. This email contained a false email trail approving the CEO's request for payment.

Not realising the request was fraudulent, the business made two payments to the cybercriminal, one for over US$200,000 and one for almost US$300,000. Both payments were made to bank accounts in overseas jurisdictions.

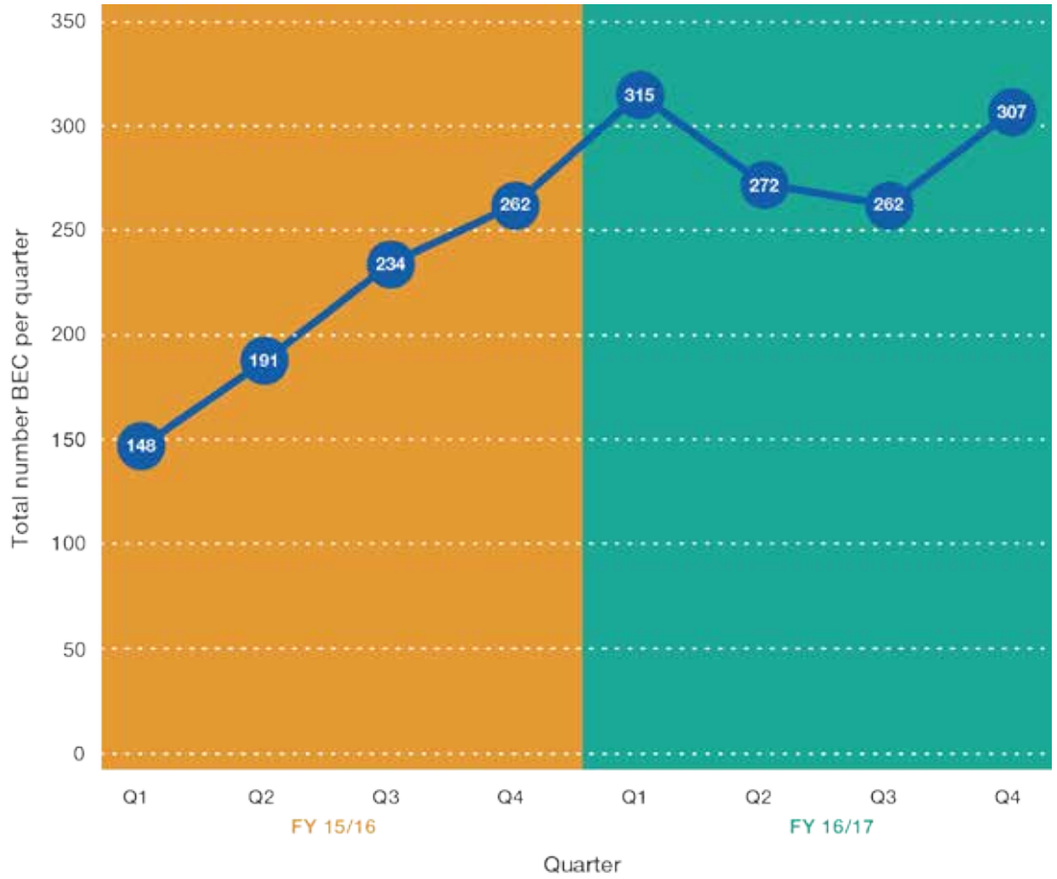


Figure 5: Business Email Compromise reports to ACORN FY 2015-16 and FY 2016-17

Threats associated with outsourcing and supply chain

Sophisticated cyber activity against third-parties – vendors that provide services to a company or agency – has increased. As it has become more difficult for adversaries to directly compromise their targets, adversaries have sought secondary or tertiary access into primary targets. Companies that provide products or services through outsourcing arrangements are highly attractive in this regard. Such providers usually have trusted relationships with their customers and are provided with extensive access.

Threats relating to outsourcing are an element of the broader threat relating to ICT supply chains, incorporating software, hardware and services, and encompass all inputs from design to delivery of an ICT product or service.

The compromise of providers can enable cyber adversaries to target and exploit customer data and networks through a range of direct and indirect means. The extent of the threat is largely dependent on the relationship between the outsourced provider and customer, in particular the extent of the provider's accesses to client networks and databases. A malicious adversary could target a provider's customer through methods including:

- exploiting the direct connectivity that a provider has with customer data and networks
- modifying the provider's software or other products with malicious content, which is then installed on customer networks
- gaining access to credentials to allow seemingly legitimate access to the target network
- engineering sophisticated spearphishing emails to deliver malware and thus compromise a target network.

Cyber security for contractors

Adversaries regularly target Australian Government information held by contractors, both classified and unclassified. Contractors can find more information on appropriately securing Australian Government information on their systems by visiting *https://www.asd.gov.au/publications/protect/cyber-security-for-contractors.htm*

Managed service providers (MSPs) are increasingly targeted as a means to compromise the networks and data of their customers including government, military and business organisations. They are a very attractive compromise target for sophisticated adversaries as they have a broad range of customers, connectivity and accesses to their customers' networks and data, and present opportunities for further network exploitation. Compromising MSPs can also be efficient tradecraft for malicious cyber adversaries. By compromising an MSP, a sophisticated cyber adversary can gain access to the data or networks of many MSP customers in one action. The ACSC has observed the compromise of Australian arms of multinational MSPs; and also observed adversaries using the compromise of the MSP to subsequently compromise the MSP's customers.

CASE STUDY

Compromise through a managed service provider

In early 2017, the ACSC became aware of the compromise of the Australian arm of a multinational construction services company. ASD and CERT Australia provided joint incident response services to the company, and through analysis were able to identify that the Australian network was compromised through their relationship with their MSP. An account associated with the MSP was used by the malicious adversary to install malware on the victim network. The account was created by the victim organisation, specifically for the service provider to log on and access the victim's network – this setup is typical of many MSP-customer relationships.

The example also highlights the risk that companies can be compromised through their service provider, without either the company or provider knowing. It also demonstrates the types of risks that organisations face when they outsource certain activities, or when they outsource with little consideration to security. When you enable other organisations access to your network, your network is exposed to their security posture – you are effectively increasing your own risk. And when you don't know the risks associated with a connected network, it is much more difficult to mitigate them.

The ACSC recommends building effective cyber security strategies – such as the Essential Eight – into contracts to protect organisations when outsourcing. Key security controls should be applied to both the customer and providers networks – with tailored security controls in place. Organisations also need to consider what to do once risk is realised, noting that realisation of risk often has significant impacts for the victim network.

ACSC RESPONSE TO REPORTED COMPROMISES OF GLOBAL MANAGED SERVICE PROVIDERS (CLOUDHOPPER)

The compromise of the global networks of several managed service providers (MSP) was reported in 2017. Using the specialist skills and relationships of all ACSC partner agencies, the ACSC has been responding to these global compromises here in Australia.

Given the potential scale of this threat to government and industry, the ACSC undertook a range of activities involving all partner agencies. We adjusted our detection posture to ensure we have the best possible visibility of this activity in Australia. We armed stakeholders – particularly those with an ability to detect and protect themselves and others from the threat – with the information they needed to investigate their own networks for any evidence associated with this activity. We reached out to the Australian arms of the impacted MSPs, ensuring that they were aware of the potential threat to their networks and to their customers. Some MSP were ready to respond and are actively managing their own internal response, others have sought assistance from commercial incident response companies, and others are working with the ACSC to investigate their networks.

ASD worked with government agencies to ensure they were alert to the risk, and able to detect and mitigate against it. The ACSC hosted briefings for Commonwealth departments and agencies and ACSC representatives travelled to all state and territory capitals for similar briefings with state and territory government staff.

Recognising the global implications of these compromises, the ACSC worked with partners around the world to understand the threat and to support the interests of Australian companies with infrastructure and other interests located overseas.

Within three hours, CERT Australia provided technical guidance to 144 partner companies that they considered could have been impacted. This was followed by a debrief workshop at the Brisbane Joint Cyber Security Centre shortly after.

The ACSC used the technical expertise and its international relationships to stay up-to-date with the tradecraft and malware being used in these compromises. Through this approach, the ACSC provided a comprehensive national response to the threat. The ACSC worked with partners to improve their overall cyber security readiness. The ACSC's response to the MSP compromise threat is ongoing.

Questions for Managed Service Providers

Organisations may choose to outsource their ICT services to Managed Service Providers. Prior to engaging their services, organisations are encouraged to confirm the security of their services. ASD has developed a set of practical questions to ask Managed Service Providers, the document is available at *https://asd.gov.au/publications/protect/questions-for-service-providers.htm*

HOW TO MANAGE RISK AND EXPOSURE

The level of segregation or integration between your network and your MSP will significantly impact how organisations manage their risk exposure. Some risk exposures are provided in the table below. Organisations should consider their risk profile on a case-by-case basis.

Relationship	Characterised by	Risk
Embedded MSP staff	Complete network segregation. MSP staff are embedded in organisations within networks, providing direct network support for the customer. There is no network connectivity to the MSP.	Low
Bastion hosts	Usually a single standalone host located in the customer network that the MSP would use to connect into the customer's network. Typically located in front of a network firewall and open to the internet.	High
Hosted network	No network segregation between the MSP and customer networks. The MSP has full access to the customer's network.	Extreme

Personally identifiable information

Malicious cybercriminals continued to seek access to repositories of large amounts of personally identifiable information (PII). Government and commercial bulk data repositories provide a single point of storage for valuable information on large numbers of Australians.

Criminals regularly seek to acquire PII to commit financial crimes and identity theft. Basic information, such as name, birth date and address, is often enough for criminals to impersonate victims. Cybercriminals may also try to extort money from organisations and individuals by threatening to release PII. Terrorists and hacktivists have publicly disclosed PII in order to embarrass, intimidate or threaten individuals, government and commercial organisations in 'hack and release' operations.

In 2017, US company Equifax reported that the PII of approximately 143 million customers had been accessed through an unauthorised cyber security incident. Information accessed included name, social security numbers, birth dates, addresses and in some instances, drivers licence details – more than enough to facilitate identity theft activities.

Malicious use of leaked tools

The public release of computer network exploitation (CNE) tools by groups such as the Shadow Brokers will improve the capabilities of malicious cyber adversaries. Less capable adversaries are likely to adopt these tools and use them on systems that remain vulnerable due to ineffective patching or updating. More capable adversaries may incorporate the tools and knowledge gained into their existing malware development efforts.

Cyber adversaries have demonstrated the ability to quickly use zero-day vulnerabilities – vulnerabilities in software unknown to the vendor. The ACSC has seen cyber adversaries modify them to be effective against current systems and circumvent some of the available patches. The knowledge gained from the release will probably lead to the development of new tools and exploits to compromise the next generations of systems.

Implementing timely patching and system-hardening regimes, and upgrading unsupported operating systems will mitigate most of the risk. Unfortunately, in many cases, patching and mitigation of these vulnerabilities are applied inconsistently.

The Shadow Brokers have stated in their public communications that further information may be released, which may include additional exploits.

CASE STUDY

Inadvertent sensitive data exposure by suppliers online

CERT Australia continues to respond to incidents where sensitive supplier data has been exposed. The reason for the data exposure is often not malicious, but rather due to technical error. A number of technologies have been involved including File Transfer Protocol (FTP) servers, Network Attached Storage (NAS) devices, and Amazon S3 buckets. During these investigations, it was discovered that the majority of the incidents involved the exposure of sensitive data relating to the supplier's customers. Data exposed has included customer names, credentials for internal systems, and network diagrams. The impact of exposure of such sensitive data can be critical as it can enable a malicious adversary to see the internal workings of a customer's network and potentially gain unauthorised access.

In these incidents, CERT Australia notified the suppliers so they could determine the source of the data exposure and fix the issue. Once the data was no longer accessible, CERT Australia worked with the suppliers to determine the impact of having the data exposure, which organisations were affected, and what led to the exposure. Customers were provided with information on the issue and appropriate remediation actions.

Applying patches and hardening systems

Applying patches to operating systems, applications and devices is critical to ensuring the security of systems. Guidance on assessing the risk posed to organisations if patches are not applied in a timely manner can be found at *https://www.asd.gov.au/publications/protect/assessing_security_vulnerabilities_and_patches.htm*

Advice on hardening various operating systems and software packages can be found at *https://www.asd.gov.au/publications/index.htm*

Protecting against router scanning

The ACSC has undertaken a number of activities in response to this router scanning, including:

- directly engaging with victims who had their router configuration files stolen
- proactively engaging with critical sectors (including critical national infrastructure)
- updating technical guidance and intelligence assessments – including issuing public advice via the ACSC website
- engaging with industry partners.

Given the ongoing nature of this activity and the potential for harm, the ACSC undertook proactive scanning of the Australian IP space to identify vulnerable routers and engaged with organisations to provide tailored mitigation advice. The ACSC has previously published advice to mitigate this threat. Since October 2016, the ACSC has published advice on its website on how to mitigate this threat.

Router scanning

Throughout 2017, the ACSC and our international partners continued to observe the targeting of routers, including Australian routers, by malicious, sophisticated threat adversaries. This activity centres on automated scanning to identify vulnerable routers, and the subsequent extraction of configuration files. A configuration file is data that stores various settings, including security settings and passwords. Accessing a router's configuration file may ultimately allow a malicious adversary to modify the router settings, enabling control of internet communications on that device. While the ACSC has not yet observed activity beyond exfiltration of the router configuration file in Australia, a number of international partners have reported instances of this occurring overseas.

The adversaries appear to be leveraging routers that have Simple Network Management Protocol (SNMP) exposed to the Internet. By default, routers typically have SNMP exposed to assist with router installation and network setup; however best practice remains disabling SNMP once a router is installed.

Distributed Denial of Service threats

Distributed Denial of Service activity will remain a threat to internet-connected systems for the foreseeable future. The means and mechanisms may change, but it will remain an enduring threat with demonstrated utility for state, criminal and issue motivated groups.

In October 2016, the 1200 Gbps DDoS activity directed at Domain Name Service (DNS) provider Dyn set records for size, and demonstrated a weak point in major internet services. An outage at Dyn made many popular web services dependent on Dyn for DNS – including Twitter and Reddit – unavailable for many users. Though the impact was not as severe in Australia as it was in US, some Australian websites did experience performance issues as a result.

Australian systems may be affected by DDoS activity occurring outside Australia as DDoS threats not only affect a given website or service, but can also affect related systems through interdependencies. Understanding these interdependencies is core to risk management. Some DDoS activities, such as those directed against Dyn, will continue to cause collateral damage on related systems. In the absence of specific, proportional targeting, these effects may be widespread.

Managing the DDoS risk

DDoS capabilities will continue to evolve in size and sophistication, but will not become an insurmountable threat. DDoS activities can be disrupted at several points and a coalition of stakeholders may contribute to mitigating the threat. More information can be found at *https://www.asd.gov.au/publications/protect/preparing-for-responding-to-ddos-activities.htm*

Internet of Things (IoT)

An increasing number of consumer devices are now being developed with the capabilty to connect to the internet to receive instructions and transmit data back to online services and personal applications. Referred to as the Internet of Things (IoT), these devices range from simple sensors and CCTV cameras to whitegoods, lightbulbs, medical aids, household devices, and internet-facing industrial control systems.

Home automation is accelerating the introduction of a diverse range of internet-connected consumer products. These devices are then being linked to other online services

Top security tips for personal device use

Compromises of personal devices, such as smartphones, tablets and laptops, can have significant productivity, financial and emotional impacts. For further information on the top security tips to secure personal devices and protect your information, visit *https://www.asd.gov.au/publications/protect/personal-device-security.htm*

CASE STUDY

Mirai

Mirai is an example of malware that is comparatively unsophisticated; the source code is readily available for use by adversaries at the lowest levels of sophistication. Mirai malware turns Internet of Things devices into 'bots' to be used by adversaries for malicious purposes such as DDoS. Mirai operates by scanning the internet for a suite of devices with known default credentials, including DVRs, printers and home internet routers. It uses those credentials to install itself onto the device, and then scans the internet for new vulnerable devices to infect. Despite its relative simplicity, Mirai has been used to implement some of the largest DDoS incidents seen to date.

On 20 September 2016, the Mirai botnet launched a DDoS attack against OVH, a major web hosting company based in France. A DDoS attack was also launched against the website of an independent IT security journalist, Brian Krebs, forcing his website offline despite it being protected by one of the leading DDoS protection services, Akamai. Regardless of its relative simplicity, this attack by Mirai was considered one of the largest DDoS attacks ever seen.

which are connecting them in novel ways. For example, it is within the reach of consumers to have their light bulbs flash if it is forecast to rain, if their team wins, or if they are mentioned on social media.

IoT devices are created for automation and to improve efficiency, however, security in these devices is not always a top priority during the design process. A lack of standardisation and the absence of any agreed security baseline means the proliferation of these devices is introducing potential for significant security risks. Additionally, connecting devices that can change the real-world environment (such as medical devices, cars, airconditioners, fridges and door locks) through the manipulation of an online service also increases the potential impact of a compromise.

We have already seen the impact of poor security in IoT devices. The previously mentioned DDoS activity directed at Dyn used infected IoT devices such as printers, IP cameras and baby monitors, as the infrastructure for the activity. The IoT devices

were infected by a self-propagated worm which continuously scanned for unsecured IoT devices. These devices then directed tens of millions of requests to the Dyn servers rendering them unable to perform their normal services.

Prevention as an investment

Prevention is better than a cure. The initial cost of implementing robust cyber security mitigation and incident management strategies, such as ASD's Essential Eight, may seem high for some organisations, however, it represents an important investment, reducing long term costs and risk. Investing in a solid baseline of network security will help organisations avoid having to spend even more when faced with a network compromise.

Having well defined system processes, such as network segregation, administrative privilege restrictions, and system logging, is crucial. Similarly, maintaining a secure and robust network involves more than performing routine system maintenance and relying on the latest software and applications for network security. Investing in trained personnel will prove more beneficial than investing in software and applications that existing personnel may not be able to support. Senior management should build this interest and awareness into the organisation's culture. Having the resources and processes in place will ensure that the organisation is prepared for when a cyber incident occurs.

Cyber insurance

Cyber insurance is rapidly gaining popularity in Australia. Paying for cyber insurance is not a substitute for investing in appropriate cyber security measures, such as implementing ASD's Essential Eight.

Even if a cyber security incident is covered by the cyber insurance policy, an insurance payout may not be able to repair the damage caused by activities, such as stolen intellectual property and the compromise of personal information. Understanding a cyber insurance policy will assist organisations to ensure that they comply with the condition of coverage.

In 2017, the risk of cyber compromise is assessed as high for Australian organisations. The Essential Eight significantly reduces risk for almost all types of cyber incidents. Australia cannot afford to be victim to the types of malicious cyber activity we see occurring globally.

ASD'S WORLD-LEADING CYBER SECURITY ADVICE: THE STRATEGIES TO MITIGATE CYBER SECURITY INCIDENTS

First released in 2010, ASD's Strategies to Mitigate Cyber Security Incidents is the result of our distilled expertise and has evolved as cyber adversaries, tradecraft and threats have evolved. The strategies are informed by ASD's unique visibility of cyber security incidents, vulnerabilities and adversary techniques and what we learn through responding to a range of cyber security compromises. We also consult widely with a range of industry and government partners.

Updated earlier this year, the Strategies to Mitigate Cyber Security Incidents is a prioritised list of practical actions Australian organisations can take to make their networks the hardest to compromise in the world. It provides succinct, specific, prioritised guidance to address the broad range of cyber threats faced by governments and businesses alike.

Building on the Top 4, the Essential Eight are so effective at mitigating target cyber intrusions and ransomware that ASD considers them to be the cyber security baseline for all organisations. Effective implementation of the Essential Eight mitigates most common incidents, including:

- targeted cyber intrusions
- ransomware
- malicious insiders
- business email compromise
- threats to industrial control systems
- adversaries who have destructive intent.

Implementing the Essential Eight is not simply a 'tick-a-box' compliance exercise. Instead, the guidance can be tailored to meet an organisation's specific risk and resource profile. It provides organisations with a principles-based approach to building a defence-in-depth security posture. Organisations need to perform a risk assessment, implement the Essential Eight actions as a baseline, and then select other relevant actions based on the risks to their individual business and overall needs.

In every compromise ASD has investigated in the past several years, correct implementation of the Essential Eight would have effectively prevented, or minimised the extent of, compromise to the victim network. Investing in the Essential Eight is critical to effectively protecting your network from the widest range of security threats – from sophisticated cyber espionage to cybercrime.

Practical implementation guidance is available on the ASD website at *https://www.asd.gov.au/infosec/mitigationstrategies.htm*

You can now self-assess how well your organisation has implemented the Essential Eight with ASD's new maturity model. The Maturity Model is a handy tool for self assessment, providing succinct and specific guidance to address the broad range of cyber threats faced by governments and businesses alike. This is intended for cyber security professionals to assess the maturity of their implementation of the Essential Eight mitigation strategies.

The Maturity Model is applicable to the full spectrum of organisations, from those facing standard risks through to organisations constantly targeted by highly skilled adversaries, or otherwise operating in a high risk environment. The Maturity Model can be found on the ASD website: *https://www.asd.gov.au/publications/protect/essential-eight-maturity-model.htm*

WHAT ARE THE ESSENTIAL EIGHT ACTIONS TO MITIGATE CYBER SECURITY INCIDENTS?

Broader Trends

Cybercrime

Cybercrime remains a pervasive threat to Australia's national interests and economic prosperity. Australia's relative wealth and high use of technology, including social media, online banking and government services, make it an attractive target for cybercrime syndicates. High profile cybercrime successes and lucrative financial gains ensure the persistence of the cybercrime threat.

Cybercriminals are targeting Australian victims by using technically-advanced methods as well as simple defrauding tactics.

DEFINITION

Cybercrime

The ACSC defines cybercrime as crimes directed at computing or other ICT, such as unauthorised access to, modification or impairment of electronic communication or data. This does not include technology-enabled crimes where computers or ICT are an integral part of an offence, such as online fraud, identity theft and the distribution of child exploitation material.

Some cybercriminals are becoming increasingly sophisticated and ambitious, targeting businesses directly by seeking access through internet-connected software. Cybercriminals have demonstrated their ability to obfuscate their identities, conceal their communication, distance their identities from illicit profits, and use infrastructure that is resistant to compromise.

Despite this increasing sophistication and technical ability, cybercriminals are also continuing to use simple targeting methods and tools to compromise victims. This is likely due to their ongoing success, low start-up costs and the high dividends produced. The success of simple compromise tools is demonstrated by cybercriminals' continued use of phishing to deliver ransomware and credential-harvesting malware.

Cybercrime incidents commonly receive public attention when they cause damage to businesses, infrastructure

CASE STUDY

Cashout of cybercrime

The AFP continues to focus on key criminal services and enablers within the cybercrime business model, including 'cashout' strategies and services designed to transfer illicit funds from Australia to overseas locations. This has included a specific project between the AFP, AUSTRAC, the ACIC and the Australian Border Force with the aim of identifying methodology and disrupting money-muling as a key enabler of cybercrime in Australia. This initiative has identified various methods of transferring funds that are used to facilitate the cashout of cybercrime proceeds.

In one particular investigation, the AFP identified a United Kingdom (UK) national who had opened bank accounts with multiple Australia-based financial institutions shortly after arriving in Australia. After returning to the UK, this individual received A$711,000 into one of those accounts as a result of funds diverted from an Australian company that had been compromised by malware. The matter was referred to the City of London Police and the offender arrested. He was found guilty and sentenced to two years and eight months in prison.

AFP ASSESSMENT CENTRE

The AFP has a team within the ACSC responsible for evaluating cyber incidents reported to ACSC agencies. This team is responsible for the review and assessment of referrals to the ACSC that originate from the private sector, online crime reporting portals as well as international and domestic partners. An assessment for further investigation is based on a number of considerations including the needs and expectations of the AFP's clients, partners and stakeholders, the incident type and impact on Australian society and the resources required. The assessment can result in the matter being referred to AFP Cybercrime Operations, domestic and international law enforcement or intelligence partners for investigation or reference.

or governments. This has occurred recently through business disruption caused by ransomware encrypting critical files. However, smaller incidents, such as monetary losses, can have significant financial and psychological impact on individual victims and small business.

The ACSC's efforts, led by the ACIC and the AFP, to identify cybercriminals and their illicit activities is assisted by the continued emphasis the adversaries place on their reputation. Cybercriminals almost always use consistent aliases through which they communicate and conduct their business. These aliases are not often changed as their reputation is linked to them. This means activities, communications and any identifying information they reveal can be more readily tracked and attributed to a particular person. This can provide insights into the diversity of the adversaries's activities, the size of their operations, and any possible associates.

The growth of online communication networks, forums and darknet marketplaces has also eased entry to the cybercrime market and introduced the notion of cybercrime as a service that can be purchased. Goods and services available include infrastructure, malware deployment and development, communication services, and cashout services. The availability of these reduces the technological knowledge required to obfuscate one's identity or obtain profits through cybercrime.

Cyber espionage

Australia continues to be a target of persistent and sophisticated cyber espionage directed by foreign intelligence services – and will remain so for the foreseeable future. There are multiple drivers for cyber espionage against Australia, but it is most commonly observed where Australia has a prominent role in contested international issues or where a foreign state's security or economic interests are perceived to be affected.

The ACSC's knowledge of cyber adversaries who target Australia for espionage purposes has continued to grow. State-based adversaries have been observed using cyber exploitation capabilities against Australian systems in attempts to satisfy a range of intelligence requirements. This targeting does not only include Australian government networks. Private enterprises engaged in activities or industries of interests to foreign states are also targeted.

Foreign investment in the Australian private sector is creating new motivations and opportunities for adversaries to conduct cyber espionage against Australian interests. Businesses that are the subject of, or involved in, foreign investment face a greater risk of being targeted as the foreign investor seeks sensitive information that would provide a commercial advantage.

Cyber espionage operations can be conducted for other reasons than to extract information of intelligence value from the victim network. Some adversaries compromise vulnerable Australian networks for the purpose of using them as infrastructure to conduct

ACSC RESPONDS TO WANACRY IN MAY 2017

Although it had limited impact on Australia, WanaCry was one of the most significant ransomware incidents experienced globally. Pre-emptive mitigation advice from the ACSC and other security organisations had been taken up broadly across Australia, but WanaCry infections still impacted a number of small businesses. The ACSC is aware of 14 affected entities in all – and the impacts were limited.

ASD and CERT Australia proactively produced relevant alerts from the point they became aware of the vulnerability that WanaCry later exploited, including:

- August 2016: an advisory relating to the vulnerability in network devices following the public release by Shadow Brokers
- January 2017: publication of mitigation advice until patches were available
- February 2017: release of the Essential Eight – which would have mitigated the vulnerabilities exploited for WanaCry
- March 2017: a broadcast to Government highlighting the release of vendor patches.

With news of WanaCry's serious impact emerging from the UK, the ACSC was able to provide initial technical advice, conduct escalation procedures, and begin the call-out for ASD and CERT technical support. The ACSC quickly confirmed the technical mechanism that WanaCry used to propagate and publicly released the first set of written mitigation advice. The ACSC emailed this advice to all Government IT contacts. CERT and ASD provided advisories through their customer portals, and the ACORN website was updated to include a link to the ACSC advice.

CERT led the ACSC operational response to WanaCry, channelling public messaging through the Stay Smart Online portal as well as using a range of social media platforms. CERT, ACIC and ASD also undertook a joint effort to look for Australian victims. ASD contacted a number of organisations that were potentially vulnerable, and checked for evidence of WanaCry across government networks. CERT engaged with international partners and key industry bodies, with the initial focus on the Australian health sector (as that sector had been heavily impacted in the UK). The AFP contacted confirmed ransomware victims to prepare for any law enforcement follow-up.

Parliamentary briefings

In February 2017, at the request of the Prime Minister, and in response to evidence of foreign interference in the US Presidential election, ACSC agencies provided a classified briefing to political party leaders on the cyber threat to the electoral process.

The briefing was led by the Hon Dan Tehan MP, Minister Assisting the Prime Minister for Cyber Security, the Director of ASD, the Special Advisor on Cyber Security and the ACSC Coordinator, with representatives from the AFP, CERT Australia and ASIO also attending. The ACSC briefed senior representatives of all political parties on the cyber threat landscape and measures needed to protect information in Australia and when travelling overseas. The briefing also presented advice on how to mitigate and respond to malicious cyber security incidents, including how best to report incidents.

This followed extensive work ASD had already undertaken with the Australian Electoral Commission in the lead-up to the 2017 Federal Election, including:

- conducting a technical review of the new Senate voting system
- providing tools for the AEC to conduct website vulnerability scanning
- preparing the AEC for a cyber incident with a tailored threat briefing and proactive advice.

Since the briefing, ASD's support for the electoral process has continued with ongoing discussions on designing security into online voting systems, our participation in cyber security briefings to all state Electoral Commissioners and participation in a workshop in May 2017 run by the Electoral Commission of Australia and NZ (ECANZ) on online electoral voting.

operations against other targets. The use of victims as infrastructure in this way means that even networks that hold no information of interest to foreign states are potential targets.

Overall, the ACSC still assesses that our visibility across the range of malicious cyber activity conducted by sophisticated actors remains limited. The true scale of cyber espionage activity against Australian interests may never be known. Keeping pace with this evolution will increasingly challenge network defences as more states invest in their cyber capabilities, and at greater levels.

Cyber attack

Australia has not been subjected to malicious cyber activity that would constitute an official cyber attack. Although Australians and Australian interests are routinely targeted for compromise, no adversary has sought to disrupt or degrade Australian networks, or misuse stolen data to achieve the serious compromise of national security, stability or economic prosperity that would be considered to be a cyber attack.

The ACSC continues to assess that a cyber attack against Australia would most likely be aimed at high value targets such as critical infrastructure, government networks or military capabilities. However, the trend towards states interfering in the affairs of others using cyber

CASE STUDY

Compromise of an Australian company with national security links

In November 2016, the ACSC became aware that a malicious cyber adversary had successfully compromised the network of a small Australian company with contracting links to national security projects. ACSC analysis confirmed that the adversary had sustained access to the network for an extended period of time and had stolen a significant amount of data. The adversary remained active on the network at the time.

Analysis showed that the adversary gained access to the victim network by exploiting an internet-facing server, then using administrative credentials to move laterally within the network, where they were able to install multiple webshells – a script that can be uploaded to a webserver to enable remote administration of the machine – throughout the network to gain and maintain further access.

DEFENCE INDUSTRY – A PRIORITY TARGET

Defence contractors and companies involved in the design, manufacture and maintenance of defence capabilities continue to be targeted by state cyber programs. Cyber adversaries often target the networks of defence-affiliated organisations, such as commercial contractors. This targeting seeks to access information that would be difficult to obtain from more secure government networks, or to exploit trusted network relationships to facilitate access to, or targeting of, more secure networks.

Recognising this industry-specific targeting, the ACSC (CERT Australia, ASD and ASIO) collaborated with the Australian Government Security and Vetting Service and the Centre for Defence Industry Capability to provide seven Defence Industry Security and Cyber Awareness Forums across Australia. The ACSC provided an analysis of contextual cyber security threats affecting Australia's defence industry, and preventative strategies and resources to raise awareness of the threat to over 150 businesses in the sector. Establishing this dialogue builds on the relationship the ACSC and Australian Government have with the defence industry to strengthen the sector's cyber security awareness and posture over time.

DEFINITION

Cyber attack

The Australian government defines cyber attack as a deliberate act through cyberspace to manipulate, disrupt, deny, degrade or destroy computers or networks, or the information resident on them, with the effect of seriously compromising national security, stability or prosperity.

Relatively unsophisticated cyber activity – including website defacement, spearphishing, social media hijacking – is a common occurrence that is often described as 'cyber attack'. The use of the term cyber attack to encompass low-level activity complicates a mature appreciation of cyber security risk and vulnerability and removes it as a meaningful threshold for policymakers.

means illustrates that malicious cyber activity can take many forms, and will not always be immediately apparent. Events continue to highlight how cyber capabilities can be employed in ways that can impact national security and prosperity, or embarrass governments and political adversaries.

Cyber terrorism

The ACSC considers the risk of terrorist organisations using a cyber attack to impact Australian interests as low. Terrorist groups lack the technical sophistication to threaten Australia's security using cyber means. Over the longer term, there is potential for such groups to develop the necessary capabilities, but this would require a change in focus and deliberate recruiting and training efforts. Despite promises and inflated claims of cyber prowess, terrorist groups use of offensive cyber capabilities has been limited. In the meantime, we should continue to expect terrorist groups using basic methods to make propaganda wins, such as defacing websites and hacking social media accounts.

Threat to Government

The ACSC has observed fewer major compromises of Australian government networks, but this doesn't necessarily represent a reduction in targeting. Government networks were regularly targeted by the breadth of adversaries, including cybercriminals, issue-motivated groups and individuals, and state-sponsored adversaries. As government defences gradually improve, cyber adversaries will increasingly look to identify softer targets to gain access to government information and networks. Advanced cyber adversaries are also using increasingly sophisticated tools, meaning that some compromise attempts could go undetected.

No federal or state government network is exempt from malicious cyber activity. Foreign states continue to possess the greatest intent and capability to compromise Australian government networks. Cybercriminals continued to pose an ongoing threat to government-held information, although much of it is opportunistic, rather than specific effort to compromise a given network. Nevertheless, relatively inexpensive and accessible cyber tools can achieve significant disruptive effects and embarrassment.

WORKING WITH GOVERNMENT

Between 1 July 2016 and 30 June 2017, ASD – who takes the leads within the ACSC on incidents impacting government – responded to 671 cyber security incidents considered serious enough to warrant operational responses.

The security of government networks and information is not only measured by how many cyber security incidents occur, it is measured by the type of incidents, their scale and the impact they have on national security and economic prosperity. As cyber security awareness has increased, and government organisations have improved their ability to respond to lower level cyber security incidents on their own, the number of incidents requiring an operational response has decreased. We can expect to see this trend to continue.

Australian government organisations are required to report cyber security incidents to improve the ACSC's understanding of the threat and to assist other organisations facing these threats.

CYBER SECURITY MASTERCLASSES

The Australian Government recognises that organisations with strong support for cyber security initiatives at the senior leadership level are far more resilient than those without senior leadership support. Regular, proactive discussions at the most senior levels build resilience and result in better preparation and responses to cyber threats.

To ensure Australian Government senior leaders are supportive of cyber security within their areas of responsibility, CERT Australia, in collaboration with the Department of Defence, Department of Industry and Department of Prime Minister and Cabinet, has developed a series of masterclasses for Australian Government Ministers and senior government executives on the fundamentals of cyber security.

The Cyber Security Masterclasses are presented by leading senior government experts and give participants a deeper understanding of the current issues in cyber security. They are designed to explain complex terminology in simple terms and outline the varying roles and responsibilities for cyber security within the Australian Government. Information is also provided on threats, impacts, the importance of having measures in place to limit the harm from cyber security incidents, who to contact in a crisis and how to talk about issues to staff and the broader Australian public.

CERTIFIED CLOUD

ASD has been providing cloud computing security advice and assistance to both cloud service providers and tenants, including Australian Government agencies, since 2011 *(https://www.asd.gov.au/infosec/cloudsecurity.htm)*. ASD also certifies cloud services as appropriately secure for Australian Government use.

Achieving ASD Certification is difficult with only some providers meeting the Australian Government physical, personnel and information security requirements (see the ASD Certified Cloud Services List (CCSL) *https://www.asd.gov.au/infosec/irap/certified_clouds.htm).*

ASD uses its Information Security Registered Assessors Program (IRAP) and the Attorney General's Department Security Construction and Equipment Committee (SCEC) when conducting security risk mitigation activities. Only when the residual risk is identified, mitigated or effectively remediated does ASD award certification. ASD certified the first public cloud service for UNCLASSIFIED DLM material in 2015. At the ACSC Conference 2017, ASD announced the certification of the first cloud services to meet PROTECTED security requirements. Sliced Tech, Vault Systems and Macquarie Telecom are Australian companies with PROTECTED community cloud offerings for the Australian Government. ASD continues to work with Australian and global cloud providers to make secure business and development decisions in order to meet the technology and security needs of the Australian Government. While protecting Australian Government information this work is also securing the information of the global cloud consumer.

WORKING WITH THE PRIVATE SECTOR

During 2016-17, CERT Australia – who takes the lead within the ACSC on incidents impacting the private sector – responded to 734 cyber incidents affecting private sector systems of national interest and critical infrastructure providers.

Following the release of the 2016 Australian Cyber Security Strategy, CERT Australia has expanded its capacity to work with Australian businesses through the sharing of threat indicators, security advice and incident reporting. With this expansion, CERT Australia has enhanced industry engagement, with more than 580 businesses having partnered with CERT Australia by the end of 2016–17. CERT Australia proactively reaches out to industry, hosting various events across Australia, as well as responding to thousands of automated cyber related reports with more than 700 requiring dedicated technical assistance and analysis by CERT Australia staff.

Threat to the Australian private sector

The Australian private sector continues to be targeted by malicious activity ranging from low impact incidents such as website vandalism, through to high impact intrusions that result in the loss of valuable intellectual property. Of particular note was the 11% increase in non-traditional sectors, reflecting the expanded scope of targets for cybercriminals and adversaries (Figure 6).

Cyber espionage and cybercrime remain the primary threats to the Australian private sector, affecting Australia's competitive advantage, particularly in the specialist and profitable area of research and development. Cyber espionage poses the most advanced threat, and while it is generally associated with the theft of intellectual property, cyber espionage may also include the theft of other commercially sensitive information such as company negotiation strategies or business plans.

The vast majority of reported cyber incidents affecting the Australian private sector were criminally motivated, typically for financial gain. Malicious emails continued to be a common vector for compromising private sector networks. Targeted socially-engineered spearphishing emails, sometimes combined with phone calls, were regularly used to gain access to corporate networks. Malicious cyber adversaries make

Through automated detection and notification processes, CERT Australia provided

6456 automated responses to industry.

Private sector targets

Cyber espionage activity is likely to target Australian industries where:

- Australia has particular technology or research strengths
- foreign states have identified a specific technology gap
- a particular economic or military benefit exists
- foreign states lack the capability to manufacture or develop the technology indigenously
- research, development and manufacturing costs are prohibitive
- an organisation holds bulk personally identifiable information
- a foreign entity is seeking to invest or purchase within that sector.

Of incidents impacting industry that the ACSC responded to,

58% were self-reported by industry and

42% were detected by the ACSC

use of publicly available industry information such as annual reports, shareholder updates and media releases to craft their malicious cyber activities, and have used sophisticated exploits and implants to evade detection.

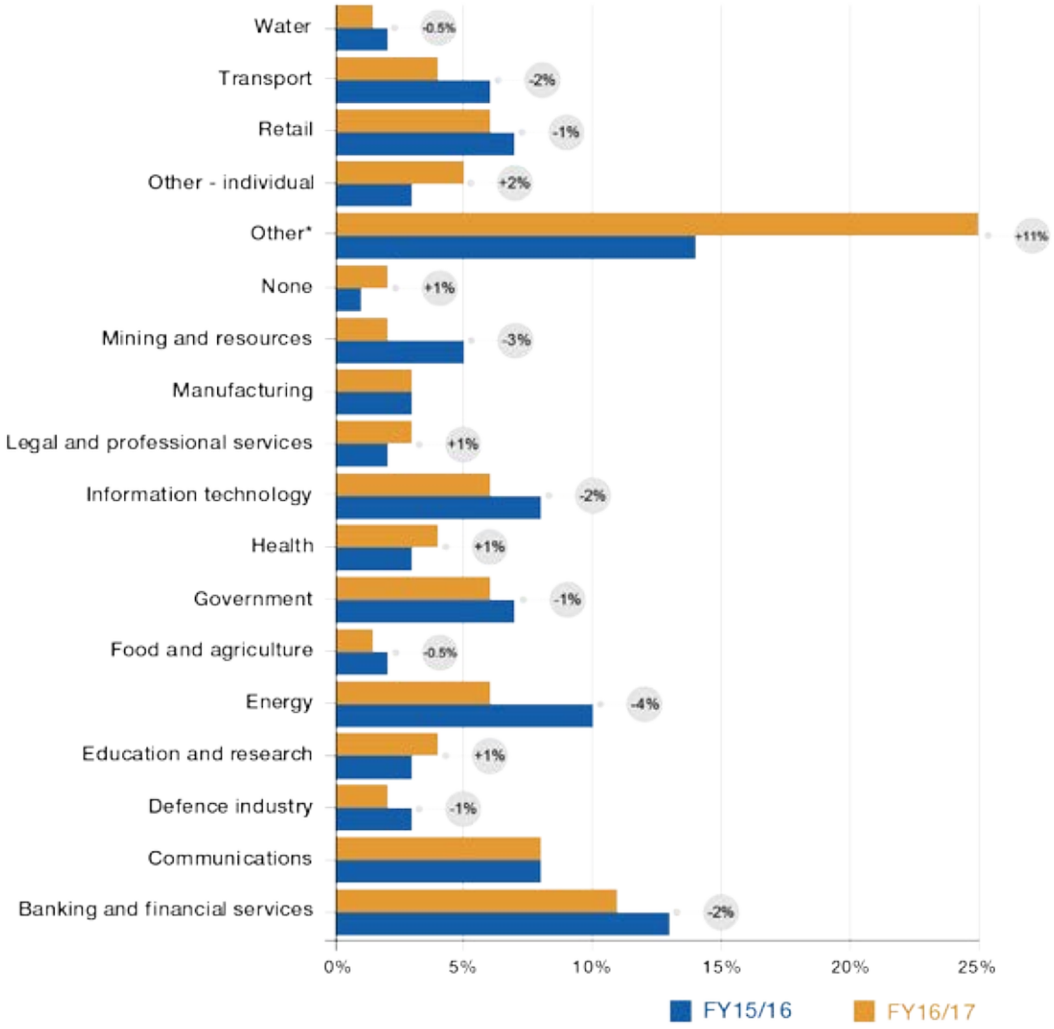


Figure 6: Private sector incident responses by sector

*CERT Australia has had an increase in voluntary reporting from sectors that have not been traditionally targeted, such as the accommodation, automotive and hospitality sectors. This shows the expanding scope of targets for adversaries and cybercriminals.

JOINT CYBER SECURITY CENTRES

The Joint Cyber Security Centre (JCSC) program, led by CERT Australia, is establishing centres in major capital cities that bring together business, government and academia to share cyber security information.

The JCSCs will enhance cyber security information sharing nationally, and provide a direct link between partners and the ACSC. The first JCSC in Brisbane was launched in February 2017, and the Melbourne, Sydney and Perth centres will become operational before the end of 2017, with Adelaide to follow in early 2018. In the lead up to the centres becoming operational, CERT Australia is engaging closely with key industry and government stakeholders to design all elements of the centres, from the national governance arrangements through to their activities.

The reach of the centres will be enhanced by the development of a related JCSC information sharing portal. CERT Australia is working with Data61 to deliver a number of workshops to Commonwealth and industry stakeholders to inform the design and functionality of the online portal and how it can best support two-way sharing of cyber security information between government and business.

Since the Brisbane JCSC was launched, it has partnered with more than 35 organisations who are participating in a program of activities. To date, 14 activities have been held. These activities have ranged from threat sharing roundtables through to targeted workshops on topics such as automated threat sharing, technical recruitment and risk management. These activities are interactive sessions where attendees can share organisational approaches to the topics being discussed in a trusted environment. Brisbane JCSC partners play an active role in proposing activities moving forward and identifying emerging trends that require attention through the JCSCs.

INTERNATIONAL CYBER SECURITY CAPACITY BUILDING

The Asia-Pacific Computer Emergency Response Team (APCERT) is a grouping of leading and national CERTs and Computer Security Incident Response Teams dedicated to the protection of national infrastructure in the Asia-Pacific. APCERT has an operational focus to help create a safe and reliable cyberspace in the Asia-Pacific region through global collaboration. CERT Australia currently chairs the APCERT Steering Committee, as well as the Policy, Procedures and Governance Working Group, focusing on increased information sharing, training and capacity development within APCERT members. The collaborative community of APCERT has expanded with stronger partnerships both in the Asia-Pacific region and beyond.

MAJOR EVENTS AND CYBER SECURITY

High profile events are attractive targets for malicious cyber actors. Adversary's motives will vary: some will seek to cause nuisance or embarrassment; criminally-motivated groups may seek to steal information from which they can profit; while some groups may want to raise their profile and use disruption to promote their agenda. Examples of disruptions could include:

- a successful DDoS or the execution of cryptolocker-style ransomware that disables key system, such as those responsible for logistics or presentations
- unauthorised access to official social media accounts and websites to draw attention to themselves, their causes or to inflict reputational harm
- using an event website to infect visitors to the site
- criminal targeting to extort the event organisers, such as gaining access to ticket sales systems or credit card information
- gaining access to internal systems and publicly releasing sensitive or embarrassing data, such as internal communications.

In addition to business-as-usual engagement, CERT Australia also engages with industry in preparation for major events. CERT Australia hosted an information exchange for critical infrastructure and systems of national interest involved with the 2018 Commonwealth Games (the Games). During the information exchange participants collaborated and shared information to ensure they are better prepared for the Games. Events such as these, facilitated by CERT Australia, demonstrate the trusted environment that has been built to allow industry competitors to sit next to each other and openly share information.

CERT Australia is also partnered with the Gold Coast Commonwealth Games Corporation, which was created to deliver the Commonwealth Games in 2018. This corporation is not a CERT partner in the traditional sense, as CERT Australia has engaged with them on a time-limited basis in order to provide support, options and advice in regards to ICT security issues that relate to a mass gathering of this type. The Gold Coast Commonwealth Games Corporation is a private company that is funded by the Queensland state government, the Gold Coast City Council, as well as Commonwealth Games sponsors.

Threat to financial institutions

Cybercriminals continued to pose a significant threat to financial institutions globally, but have yet to severely affect Australian institutions. Criminal activity is generally opportunity-based and the relative cyber security maturity of Australian financial institutions means there are more attractive and vulnerable targets in developing countries.

Cybercrime conducted by criminal and state-sponsored cyber adversaries remains a persistent threat to Australian financial institutions. Criminal groups continue to conduct malicious cyber activity such as deploying malware on a network to steal online banking credentials or conducting large, multi-stage intrusions to facilitate larger scale theft.

The global financial system is likely to face challenges from a growing volume of increasingly sophisticated malicious activity. Foreign state and criminal groups are demonstrating the capabilities and operational tradecraft to conduct major intrusions into financial institutions. The adverse effects of these actions on second parties and on confidence in system security will probably have wide ranging repercussions.

Threat to Australian academic institutions

Targeting of the networks of Australian universities continues to increase. Universities are an attractive target given their research across a range of fields and the intellectual property this research is likely to generate. Additionally, state-sponsored cyber adversaries may use university networks as infrastructure due to their reliability and high and varied traffic, thus allowing adversaries to 'hide in the noise'.

Further information

The Australian Government Information Security Manual (ISM)

The Australian Government Information Security Manual (ISM) assists in the protection of official government information that is processed, stored or communicated by Australian government systems, and is available at: *https://www.asd.gov.au/infosec/ism/*

Strategies to Mitigate Cyber Security Incidents

ASD's Strategies to Mitigate Targeted Cyber Intrusions, first published in 2010, focuses on mitigating targeted cyber intrusions by foreign states. Updated strategies were released in 2017, renamed to Strategies to Mitigate Cyber Security Incidents, tailoring prioritisation and providing additional controls that will make the mitigation strategies also relevant to current and emerging issues such as ransomware, business email compromise, destructive malware and industrial control systems. The strategies document can be found at: *https://www.asd.gov.au/infosec/mitigationstrategies.htm*

Stay Smart Online

Stay Smart Online is a CERT Australia initiative that provides simple, easy to understand advice and resources on how to protect yourself online as well as up-to-date information on the latest online threats and how to respond. More information is available at: *https://www.staysmartonline.gov.au*

Contact details

Australian government customers, businesses or other private sector organisations with questions regarding this advice should contact the ACSC by calling 1300 CYBER1 (1300 292 371) or by visiting *https://www.acsc.gov.au/contact.html*