Australian Government

Australian Cyber Security Centre

ACSC

AUSTRALIAN CYBER SECURITY CENTRE

2016

THREAT REPORT

Contents

Foreword

With more and more high profile cyber security incidents being made public, awareness of the importance of cyber security continues to steadily increase. However, while an ongoing dialogue is good for Australia, the level of public discussion and understanding would benefit from more informed and considered perspectives. In order to have a mature discussion in 2016, it is particularly important that we get the language right - calling every incident a 'hack' or 'attack' is not helpful for a proportionate understanding of the range of threats and only promotes sensationalism. And treating every adversary as though they are all equally sophisticated and motivated detracts from a balanced perspective of risk and vulnerability.

This is the second Australian Cyber Security Centre (ACSC) Threat Report. It continues to reflect the experience, focus, and mandates of the ACSC's member organisations. This report provides an insight into what the Centre has been seeing, learning, and responding to, focusing on specific areas of change or new knowledge obtained. But we at the ACSC are not just focused on the problem. Importantly, this document also contains mitigation and remediation advice to assist organisations to prevent, and respond to, cyber threats. The current hype associated with the proliferation of 'threat intelligence' can be a distraction from what really matters: the motivation to allocate effort and resources to improving your cyber security posture by implementing technical controls. If you are relying on threat intelligence to respond to threats already discovered, it is too late for you and your organisation.

In cyber security, prevention is always better than a cure. This report should be read in conjunction with the latest advice from the ACSC (available on the ASD website as well as advisories posted on the CERT Australia website) to assist organisations to prevent and respond to the cyber threat - particularly ASD's *Strategies to Mitigate Targeted Cyber Intrusions*. This guidance is regularly reviewed and updated, informed by visibility of threats and experience performing incident response, vulnerability assessments and penetration testing. ASD's *Strategies to Mitigate Targeted Cyber Intrusions* have undergone significant revision in 2016 and an update will be released later this year.

Clive Lines
Coordinator, ACSC

About the Australian Cyber Security Centre

The ACSC co-locates key operational elements of the Government's cyber security capabilities in one facility to enable a more complete understanding of sophisticated cyber threats, facilitate faster and more effective responses to significant cyber incidents, and foster better 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), the Defence Intelligence Organisation (DIO), the Australian Security Intelligence Organisation (ASIO), Computer Emergency Response Team (CERT) Australia, the Australian Criminal Intelligence Commission (ACIC), and the Australian Federal Police (AFP).

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.

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

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.

CERT Australia is the Government contact point 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.

Australia's Cyber Security Strategy – announced by Prime Minister Turnbull in April 2016 – and the *2016 Defence White Paper* are major initiatives that forecast significant investment in the Government's cyber capability. The ACSC worked closely with the Department of the Prime Minister and Cabinet to develop the Cyber Security Strategy and will play a key role in delivering many of its signature initiatives.

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 with the capability to undertake targeted intelligence and to investigate and refer matters for prosecution for those believed to have committed cybercrimes of national significance. The AFP is also the ACSC's conduit for State and Territory law enforcement.

The ACSC's key areas of collaboration are:

- triaging and responding to significant cyber security incidents affecting national security or economic prosperity;
- identifying, analysing, and conducting research into sophisticated malicious cyber activity targeting Australia;
- creating shared situational awareness of the cyber threat by developing alerts, warning and mitigation advice, and producing intelligence;
- working closely with government organisations, critical infrastructure owners and operators, and key industry partners and sectors to reduce security risk and limit the threat to Australia's most important networks and systems; and
- developing relationships with key international partners.

For more information about the ACSC, visit *https://www.acsc.gov.au.* To provide feedback or otherwise contact the ACSC about this report, please contact 1300 CYBER1 or use other details available at: *https://www.acsc.gov.au/contact.htm*

Scope of malicious cyber activity – a high level overview

Cyber attack

'Cyber attack' is a term that is frequently used by media, academics and foreign governments to describe the gamut of malicious activity including common occurrences such as Distributed Denial of Service (DDoS), website defacement, spear phishing, social media hijacking, cybercrime, and the theft of personal data. The term 'cyber attack' is well-entrenched within the information security community, where it is used to broadly describe malicious activity against a computer network or system.

The broad adoption of the term has seen it often used in a sensationalist way – similar to 'cyber war', 'cyber terrorism' and 'cyber weapons' – with the term 'attack' generating an emotive response and a disproportionate sense of threat. The use of the term 'cyber attack' to encompass common cyber threats complicates an advanced appreciation of the spectrum of cyber security risk, vulnerability, and consequences; blurs the understanding of potential 'red lines' in cyberspace; and undermines the development and application of proportionate nation state responses.

If a nation says it has been subjected to an 'attack', this is weighted with tremendous significance. As such,

DEFINITION

The Australian Government has defined **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 economic prosperity.

This definition was developed in 2011 after extensive policy and legal consultation. It was subsequently used to underpin the provisions of the ANZUS Treaty that allow Australia and the US to consult each other in the event of a cyber attack on either party.

the Australian Government's definition of cyber attack can be at odds with what the information security community, the public and the media envisage cyber attacks to be. A recent example is the disruption to the Australian Bureau of Statistics (ABS) 2016 online Census. On 9 August 2016, as a precaution to ensure the security of census data already submitted, the ABS and its service provider IBM temporarily disabled access to the Census website after experiencing multiple DDoS incidents. However, this incident was initially described in some media reporting as being the result of a "foreign cyber attack" – a description that led to a heightened sense of threat and risk, increased concerns from the public about the security of their personal information, and triggered media speculation about nation state motivations, tradecraft, and the possibility of further 'attacks'.

Australia treats cyber attacks as extremely serious and provocative events. Fortunately, Australia still has not been subjected to malicious cyber activity that could constitute a cyber attack as defined on the previous page. Contrary to speculation, this is not simply a matter of failed detection; the effects of a cyber attack could not possibly have gone unnoticed. However, the threat of a cyber attack being conducted against Australian government, infrastructure, industry or other networks has grown following a series of high-profile disruptive or destructive incidents in other countries over the last five years.

DEFINITION

Cyber adversary is an all encompassing term that describes an individual or organisation (including an agency of a nation state) that conducts malicious cyber activity.

The ACSC has previously assessed that cyber attacks against Australia would most likely occur against high-value targets such as critical infrastructure, government networks or military capabilities during periods of very high tension or an escalation to conflict. Although this remains broadly accurate, the nature and targets of recent incidents overseas – combined with a growing understanding of adversaries' capabilities and intentions – highlight the breadth of potential targets and different ways cyber capabilities can be employed by adversaries seeking to achieve damaging or destructive effects outside conflict.

Behaviour by a number of countries is demonstrating a willingness to use disruptive and destructive cyber operations to seriously impede or embarrass organisations and governments – equating to foreign interference or coercion. For example, state-sponsored cyber adversaries have been publicly linked to causing deliberate damage to commercial entities to achieve strategic, political or economic goals – or a combination thereof – during increased tensions or a dispute with another state.

Some of these events have occurred outside conflict, and have set precedents for how states may seek to use cyber operations to generate effects that could have a potentially significant impact. Where coercion, economic damage or embarrassment is the goal,

the potential targets of cyber attack may include major industries, critical infrastructure, political entities, the media, the financial sector and other sectors considered important to Australia's economy and identity.

A range of states now have the capability to conduct cyber attacks against Australian government and industry networks. However, in the absence of a shift in intent – which could occur relatively quickly – a cyber attack against Australian government or private networks by another state is unlikely within the next five years.

The absence of effective repercussions following past cyber attacks internationally will embolden some states to continue developing and using cyber capabilities as a coercive tool. A continued lack of international consensus on proportionate and appropriate responses to offensive cyber activity makes the threshold for response ambiguous, raising the risks of miscalculation.

Cyber espionage

Australia continues to be a target of persistent and sophisticated cyber espionage. The cyber threat to Australia is not limited by geography; adversaries with even a transitory intelligence requirement will target Australian individuals and organisations regardless of physical location.

With a high level of collaboration and knowledge sharing between the ACSC's member organisations and other partners, our knowledge of adversaries who target Australia continues to grow – particularly for sophisticated adversaries that target government networks and key industry sectors.

More and more foreign states have acquired or are in the process of acquiring cyber espionage capabilities. The ACSC is aware of diverse state-based adversaries attempting cyber espionage against Australian systems to satisfy

Attribution of malicious cyber activity is often portrayed as contentious in contemporary media and academic discussion. Attribution beyond a reasonable doubt in a timely manner is portrayed as difficult – if not impossible – due to the absence of readily identifiable evidence and the use of denial and deception tactics by many adversaries. There are also differing perspectives on the need for attribution.

For the Australian Government, attribution of malicious activity is necessary to enable a range of response options, as well as informing intelligence collection and assessment and undertaking proactive security measures. Depending on the seriousness and nature of an incident, the Government has developed the capability to attribute malicious cyber activity in a timely manner to several levels of granularity – ranging from the broad category of adversary through to specific state and individuals – through the combined efforts of the intelligence community, law enforcement, foreign partners, and other relationships.

strategic, operational and commercial intelligence requirements. But the number of cyber security incidents across the breadth of Australian non-government networks either detected or reported is highly likely to be a fraction of the total.

Cybercrime

Cybercrime remains a pervasive threat to Australia's national interests and prosperity. Australia's relative wealth and high use of technology such as social media, online banking and government services make it an attractive target for serious and organised criminal syndicates. Lucrative financial gains by serious and organised crime syndicates ensure the persistence of the cybercrime threat. Ransomware, credential-harvesting malware and DDoS extortion continue as the predominant cybercrime threats in 2016.

The extent of cybercrime is a significant concern. High levels of misreporting and under-reporting make it difficult to accurately assess the prevalence and impact of cybercrime. While it is very difficult to establish an accurate figure, the actual costs of cybercrime at the systemic level include the costs of immediate responses, system remediation costs, and flow-on costs to government and support programs that assist cybercrime victims. The direct and indirect costs to victims include damage to personal identity and reputation, loss of business or employment opportunities and the impact on emotional and psychological wellbeing.

The global cybercrime market

The global cybercrime market is a low-risk, high-return criminal enterprise, with goods and services in strong supply and demand. It can be highly lucrative, and commodities are easily accessible through online marketplaces and forums. Anyone aiming to make an illicit profit can purchase infrastructure, delivery mechanisms, coding services, antivirus checking services, exploit kits, communication services, and 'cash out' and money transfer services. Most elements of this criminal economy and their global business operations exist alongside the legitimate online activity of governments, businesses and individuals. The challenge lies in detecting the constantly evolving illicit activity, and determining its motivation, impact and mitigation strategies.

Cyber terrorism

Terrorist groups that seek to harm Western interests currently pose a low cyber threat. Apart from demonstrating a savvy understanding of social media and exploiting the internet for propaganda purposes, terrorist cyber capabilities generally remain rudimentary and show few signs of improving significantly in the near future. They will continue to focus on DDoS activities, hijacking social media accounts, defacing websites, the hack and release of personal information (see Page 28) and compromising poorly-secured internet-connected services. It is unlikely terrorists will be able to compromise a secure network and generate a significant disruptive or destructive effect for at least the next two to three years.

Cyberspace will continue to present a target rich environment. With intent and investment, terrorist groups could potentially develop more sophisticated cyber capabilities. However, at this point in time, terrorist groups are more likely to embarrass governments, impose financial costs, and achieve propaganda victories by compromising and affecting poorly secured networks.

Threat to government

Australian government networks are regularly targeted by the full breadth of cyber adversaries. While foreign states represent the greatest level of threat, cybercriminals pose a threat to government-held information and provision of services through both targeted and inadvertent compromises of government networks with ransomware. Hacktivists will continue to use low-sophistication cyber capabilities – website defacement, the hack and release of personal or embarrassing information, DDoS activities and the hijacking of social media accounts – to generate attention and support for their cause. As such, issue-motivated groups pose only a limited threat to government networks, with possible effects including availability issues and embarrassment. However, some hacktivists intend to cause more serious disruption and may be able to exploit poor security to have a greater impact.

As the Prime Minister acknowledged during the launch of *Australia's Cyber Security Strategy* on 21 April, the ACSC has worked with government organisations to understand and respond to significant compromises of government networks, including a cyber intrusion on the Bureau of Meteorology's network (see below) and the Department of Parliamentary Services (which pre-dates the timeframe of this report).

Between 1 January 2015 and 30 June 2016, ASD, as part of the ACSC, responded to 1095 cyber security incidents on government systems which were considered serious enough to warrant operational responses.

As cyber security awareness has increased, and government organisations have improved their ability to respond to their own lower level cyber security incidents, the number of incidents requiring an operational response has decreased. We can expect to see this trend continue.

The security of government networks and information is not only measured by how many cyber security incidents occur – it is about the type of incidents, their scale and the impact they have on national security and economic prosperity.

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.

Bureau of Meteorology

In 2015, ASD detected suspicious activity from two computers on the Bureau of Meteorology's network. On investigation, ASD identified the presence of particular Remote Access Tool (RAT) malware popular with state-sponsored cyber adversaries, amongst other malware associated with cybercrime. The RAT had also been used to compromise other Australian government networks.

ASD identified evidence of the adversary searching for and copying an unknown quantity of documents from the Bureau's network. This information is likely to have been stolen by the adversary.

ASD recovered a password dumping utility used by the adversary and identified the malicious use of at least one legitimate domain administrator account. ASD identified at least six further hosts on the Bureau's network that the adversary attempted to access, including domain controllers and file servers. The presence of password dumping utilities and complete access by the adversary to domain controllers suggested all passwords on the Bureau's network were already compromised at the time of the investigation. ASD also identified evidence suggesting the use of network scanning and time stamp modification tools, used to analyse the network architecture and assist with hiding the adversary's tools on hosts.

In this instance, the ACSC attributed the primary compromise to a foreign intelligence service, however, security controls in place were insufficient to protect the network from more common threats associated with cybercrime. CryptoLocker ransomware found on the network represented the most significant threat to the Bureau's data retention and continuity of operations.

The implementation of security controls outlined in *ASD's Strategies to Mitigate Targeted Cyber Intrusions* publication will significantly improve the security posture of the Bureau's corporate network. The ACSC continues to work with the Bureau of Meteorology to implement a number of further, specific recommendations to mitigate future compromise.

CASE STUDY

Persistent

The ACSC undertook a major incident response, investigation and remediation of a government network compromised by a foreign state. ASD identified that the adversary had gained initial access to the network using malicious Microsoft Office macros – small programs executed by Microsoft Office applications to automate routine tasks. On advice from ASD, the government agency implemented technical controls to mitigate the threat of malicious Microsoft Office macros on the network.

Since that time, the same adversary has repeatedly attempted to regain access to the government network, incrementally evolving their tradecraft. The adversary displayed the ability to use knowledge from the previous intrusion to target specific users, vulnerabilities and systems. For example, the adversary sent a spear phishing email to a staff member from the account of a legitimate user from another foreign organisation with which the staff member had prior communication. The adversary provided advice to the staff member on how to circumvent security controls to enable Microsoft Office macros. The adversary referred accurately to the department's ICT service desk by acronym and had hardcoded the user's username, the domain and the IP address of their computer in the malicious Microsoft Office document.

This activity confirmed that the foreign state has an ongoing intelligence requirement against the government department and has most likely not regained access since ASD's remediation work. The later spear phishing activity demonstrates knowledge of the network, including that Microsoft Office macros had been disabled following the previous compromise.

Threat to the private sector

Australian industry is persistently targeted by a broad range of malicious cyber activity, risking the profitability, competitiveness and reputation of Australian businesses. The spectrum of malicious cyber activity ranges from online vandalism and cybercrime through to the theft of commercially sensitive intellectual property and negotiation strategies.

The ongoing theft of intellectual property from Australian companies continues to pose significant challenges to the future competitiveness of Australia's economy. In particular, cyber espionage impedes Australia's competitive advantage in exclusive and profitable areas of research and development – including intellectual property generated within our universities, public and private research firms and government sectors – and provides this advantage to foreign competitors.

The ACSC's visibility of cyber security incidents affecting industry and critical infrastructure networks is heavily reliant on voluntary self-reporting. Some companies may be hesitant to report incidents to the government due to concerns the disclosure may adversely affect their reputation or create legal or commercial liabilities. For example, in some cases victim organisations have sought legal advice before reporting an incident. Many cyber security incidents across the private sector are undetected or unreported. Increased reporting of cyber security incidents by the private sector would subsequently increase the ACSC's knowledge of cyber adversaries who target Australian industry and critical infrastructure, and the

Reports help the ACSC to develop a better understanding of the threat environment and will assist other organisations who are also at risk.

Cyber security incident reports are also used in aggregate for developing new defensive policies, procedures, techniques and training measures to help prevent future incidents.

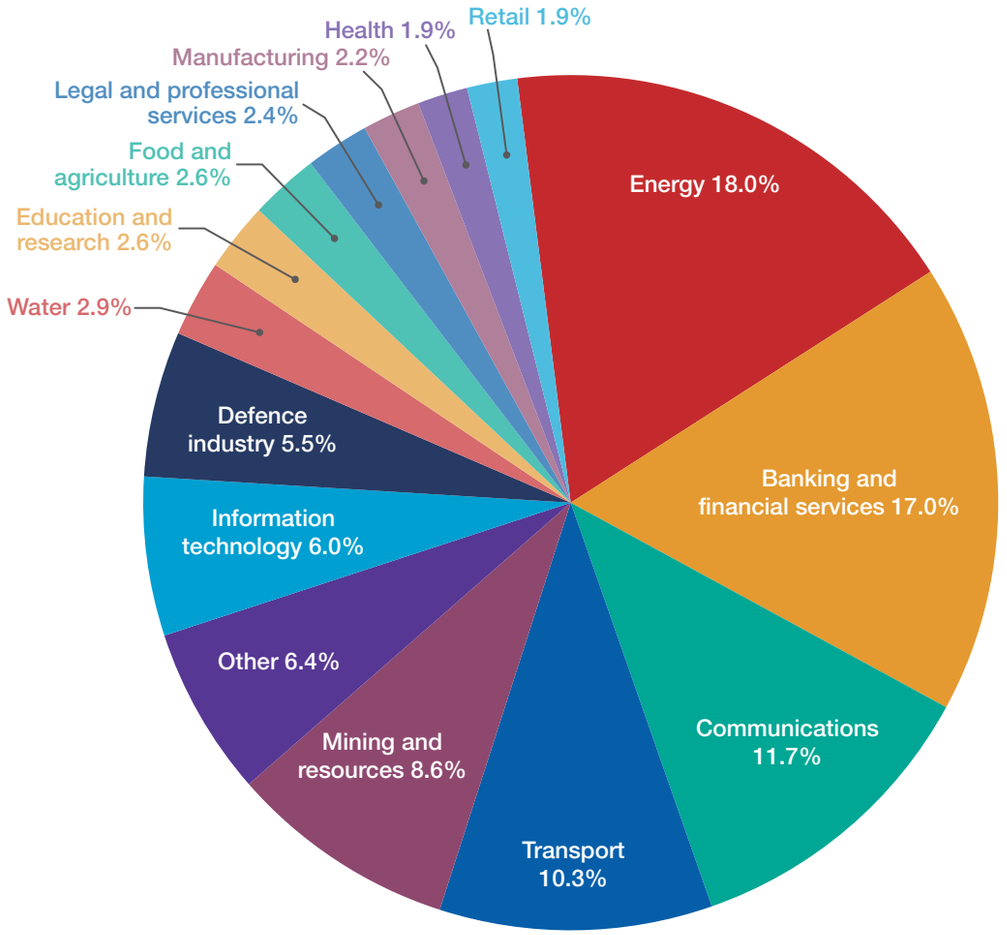
methods they employ. This knowledge would further enable the development of cyber security advice and mitigation strategies.

The ACSC is making a dedicated effort to engage industry on cyber threats and associated mitigation strategies through a process of sustained engagement. However, the private sector's ability and willingness to recognise the extent of the cyber threat and to implement mitigation strategies varies considerably across and within sectors. Generally, companies that have been extensively targeted or compromised are more likely to view the business risks associated with the cyber threat as sufficient to warrant investment in cyber security. Those without direct experience of being targeted or a victim may not be aware of the potential economic harm malicious cyber activity can cause their businesses, do not understand the value of the data they hold, and cannot conceive why they would be targeted.

Between July 2015 and June 2016, CERT Australia responded to 14,804 cyber security incidents affecting Australian businesses, 418 of which involved systems of national interest (SNI) and critical infrastructure (CI). The incidents affecting SNI and CI are broken down by sector on the following page. CERT Australia relies heavily on the voluntary self-reporting of cyber security incidents from a wide variety of sources throughout Australia and internationally and therefore does not have a complete view of incidents impacting Australian industry.

Engaging with the private sector

- The ACSC has provided advice and assistance to the private sector to deal with cyber security incidents, including serious network compromises.
- Exploitation techniques the government learns through investigating cyber security incidents contribute to public advice from ACSC member organisations. Indicators of compromise are shared with industry through partnership with CERT Australia.
- In 2015-16, CERT Australia participated in 15 different cyber security exercises. Exercises provide valuable insight into how industry can best respond to cyber security incidents.
- CERT Australia provides businesses with unique and sensitive information through sector specific, regional and national information exchange programs.
- The ACSC will be relocated to a new facility that allows unclassified and classified collaborative work spaces.
- The ACSC will co-design regional hubs - Joint Cyber Security Centres – with the private sector to share information and advice that organisations can use to take practical steps to improve security.



In CERT Australia's experience, the energy and communications sectors had the highest number of compromised systems, the banking and financial services and communications sectors had the highest incidence of DDoS activity, and the energy and mining/resources sectors had the highest number of malicious emails being received.

CASE STUDY

In July 2015, CERT Australia advised a financial services provider of a compromised domain controller on their network which was communicating with malicious domains. At the time of notification, it was believed this host had been compromised for at least a year.

CERT Australia forensically analysed a disk image of the compromised domain controller (provided by the business). This analysis revealed the presence of three different versions of a malware variant capable of the extraction of sensitive files and other malicious activities including keystroke logging and enabling access to other areas of the network, as well as the presence of additional tools capable of extracting user credentials.

Following this analysis, CERT liaised with the business to help them recover from the incident and mitigate any future incidents. This included providing a full list of practical recommendations, such as mandated password resets on all accounts, implementing the 'Top 4' of ASD's *Strategies to Mitigate Targeted Cyber Intrusions*, and creating an incident response plan which would bolster the business's cyber security posture.

Threat to critical infrastructure

Internet connectivity and Information and Communications Technology (ICT) are increasingly employed to improve the management of systems supporting critical infrastructure, enabling a wide range of functions that would not be possible on an isolated network. However, critical infrastructure is also a target of a range of cyber adversaries seeking to achieve a disruptive or destructive effect. Despite the many benefits internet and ICT connectivity provide, administrators of critical infrastructure need to remain alert to, and protect against, adversaries seeking to interfere with networks supporting critical infrastructure.

Industrial control systems (ICS) support the automation and management of physical components used in production and distribution for critical infrastructure networks, and underpin the delivery of essential services to the Australian population. The prevalence of ICS technologies in critical infrastructure – and the evolution towards greater connectivity and dependence – presents opportunities for sophisticated adversaries. For example, with adequate access, knowledge and capabilities, a sophisticated adversary could modify ICS systems to achieve a disruptive effect on critical infrastructure. These effects could include manipulating the production and supply of energy and power, the creation of outages, damage to industrial systems, and manipulation or theft of information utilised by infrastructure owners and operators.

DEFINITION

Critical infrastructure is defined as those physical facilities, supply chains, information technologies and communication networks which – if destroyed, degraded or rendered unavailable for an extended period – would significantly impact on the social or economic wellbeing of the nation, or affect Australia's ability to conduct national defence and ensure national security. Critical infrastructure can include services that provide food, water, defence, transportation, energy, communications, public health, banking and finance.

Establishing a strong cyber security posture, increasing awareness of potential vulnerabilities and implementing effective security measures are vital to deter and prevent similar incidents against Australian critical infrastructure.

Network segmentation and segregation help to prevent adversaries from spreading throughout an organisation's network, especially protecting systems never designed to have a presence online, such as power controls and circuit breakers. Segmenting and segregating networks into security zones, limiting user access to systems and data, and denying unrequired network connectivity between all computer devices will make it significantly more difficult for adversaries to locate and gain access to an organisation's most sensitive information and critical system controls. Organisations with critically sensitive information might choose to store and access it using air-gapped workstations and servers that are not accessible from the internet. Security patches and other data can be transferred to and from air gapped workstations and servers in accordance with a robust media transfer policy and process.

The December 2015 Ukraine power outages highlight the vulnerabilities of critical infrastructure to sophisticated adversaries. In a well-planned and highly coordinated operation, an adversary successfully compromised and affected the systems supporting three power control centres, taking down 30 substations and leaving over 225,000 Ukrainians without power for several hours. The adversary also delayed restoration efforts by disabling control systems, disrupting communications and preventing automated system recovery. These effects were the result of over six months of planning and involved a range of activities, including compromise through spear phishing, the theft of user credentials through key loggers, and data exfiltration.

CASE STUDY

Critical Infrastructure

The ACSC was notified of a cyber intrusion on the corporate network of an Australian critical infrastructure owner and operator. CERT Australia led the ACSC's incident response, working alongside the AFP and ASD to determine the extent of the compromise and the identity of the responsible actor.

Working onsite with the victim, the AFP identified a significant amount of data had been stolen from the network, including sensitive information relating to the organisation's physical security and layout. The ACSC's investigation revealed the actor used legitimate credentials belonging to a staff member and a contractor of the organisation during the compromise. The actor was able to escalate their privilege to administrator level, enabling further compromise.

With significant assistance from the ACSC – including ongoing remediation assistance and advice to improve the organisation's ICT security posture – the organisation has taken measures to prevent the incident from reoccurring. The AFP identified an off-shore suspect and liaised with foreign law enforcement which led to a successful arrest.

Trends in targeting and exploitation techniques

Spear phishing

Spear phishing – emails containing a malicious link or file attachment – remains a popular exploitation technique for many cyber adversaries, with methods used becoming more convincing and difficult to spot. As such, spear phishing emails continue to be a common exploitation technique used in the compromise of Australian industry networks.

DEFINITION

Social engineering employs psychological manipulation and deceit to establish trust and elicit information. In cyberspace it is commonly observed in spear phishing, and increasingly in exploitation attempts through social media. Used proficiently, social engineering can enable adversaries to bypass security measures they were unable to overcome via technical means.

Adversaries are targeting industry personnel in order to gain access to corporate networks; individuals with a large amount of personal or corporate information online make it easier for adversaries to target that individual or their organisation. Adversaries also make use of publicly available industry information such as annual reports, shareholder updates and media releases to craft their spear phishing emails, and use sophisticated malware to evade detection.

The ACSC is aware of an increase in the prevalence of socially engineered emails designed to elicit company information, including organisational structures. In many instances, this information is not commercially sensitive; however, it probably provided insights into business processes, employee details, and other information that could later be used to craft spear phishing emails.

Adversaries are improving their social engineering techniques, including by carefully crafting and customising their attempts to appeal to a target by use of an individual's personal and professional circumstances and their social networks. In this way targets of spear phishing emails are duped into opening malicious attachments and links.

CASE STUDY

Spear phishing

A company contacted CERT Australia for assistance in mitigating sophisticated spear phishing. A malicious email with an attached, password-protected zip archive had been sent to a company manager. The email appeared to be from a familiar contact – a contractor overseas – that was working on a joint project. The email used the contractor's signature block, was addressed to the manager by name and contained details of relevant work projects. The sender's email address was a Gmail address created by the adversary that contained the contractor's full name. Believing the email was legitimate, the manager forwarded it for action with the adversary copied in. When the email triggered an alert and was blocked, a request was made – also copying in the adversary – to release the email from quarantine.

The malicious email was not released and the IT manager contacted CERT Australia for assistance. Analysis revealed that the attached zip archive contained a Windows screensaver file that would have appeared on the system as a PDF file. When opened, it would have dropped a malicious executable and added a Microsoft update-themed shortcut to the system's start-up folder to establish a persistent presence. The malicious executable would have sent encrypted beacons containing details of the infected system. It was a first-stage implant that could have been used to upload additional files and to execute commands on the infected host system.

With assistance from CERT Australia, the company worked to improve the integrity of its networks and systems to establish an improved IT security posture.

Sophisticated social engineering is decreasing a user's ability to distinguish between legitimate emails and malicious cyber activity, and robust technical controls will become increasingly important as a security measure.

Ransomware

The ACSC is aware that individuals and businesses continue to be infected with ransomware via malicious emails and websites. These campaigns are constantly evolving and highly successful. They target a broad range of sectors including government, resources, business, educational institutions and home users. At a recent Regional Information Exchange hosted by CERT Australia, almost all of the attendees noted they were still being targeted and/or affected by ransomware campaigns. Almost all were delivered via email, however CERT Australia is also aware of some web-based exploit kits which are used to deliver them. Phishing emails also use attachments to deliver their ransomware, such as malicious macros in Microsoft Office files which contain instructions on how to enable and run macros.

Ransomware encrypts the files on a computer (including network fileshares and attached external storage devices) then directs the victim to a webpage with instructions on how to pay a ransom in bitcoin to unlock the files. The ransom has typically ranged from $500 - $3000 in bitcoins; however businesses have been hit with more targeted ransoms of tens of thousands of dollars. CERT Australia has also been informed of some cases where cybercriminals increased their ransom price depending on the value of the information and its availability, for example, if no backups were in place then the ransom would increase.

In the past, victims have attempted to recover from ransomware activity using methods that are ill-advised or unreliable. For example, some victims sought to recover by following instructions to pay a ransom, while others resorted to using stolen keys from the adversary's servers. Other legitimate ways have been to restore from offline backups or using shadow copies from Microsoft restore points. Even if no data is lost, the impact can still be detrimental for organisations; it can take a long time to restore from backup, assuming there were adequate backups at all.

ASD, in collaboration with domestic and international partners, developed its *Malicious Email Mitigation Strategies* publication (updated July 2016) to provide strategies for mitigating the security risk posed by malicious emails.

The *Malicious Email Mitigation Strategies* publication can be found at: *http://www.asd.gov.au/publications/protect/malicious_email_mitigation.htm*

Organisations should consider their unique business requirements and risk environment when deciding which mitigation strategies to implement. Furthermore, before any mitigation strategy is implemented, comprehensive testing should be undertaken to minimise any unintended disruptions to business.

CASE STUDY

Ransomware

In 2016, a staff member from a government organisation clicked on an Australia Post-themed email which infected their workstation with Cryptolocker. At that time, the staff member's workstation was simply re-imaged.

Three months later, ICT staff realised that thousands of files needed for legal proceedings stored on a file server had also been encrypted by the ransomware.

Due to the amount of time that had elapsed, the backups contained encrypted copies of the files, and it was far too late to pay the ransom. However, the organisation managed to recover important information that was held elsewhere throughout the agency in data repositories such as databases.

The ransomware itself, the email addresses used to deliver it and the malicious domains hosting the malware are changed rapidly by cybercriminals which frustrates and renders ineffective attempts to defend against these threats by simply blocking them. They often closely resemble the expected legitimate email addresses, webpages, and domains to encourage the victim to click the link and download the ransomware. The ransom emails often contain a threat of further fines or fees to pressure the recipient into taking action, and the ransom typically doubles after 24 hours if not paid. In some cases, files are progressively deleted until the ransom is paid.

For up to date ransomware alerts and mitigations, Australian organisations should use the OnSecure portal (government), or refer to CERT Australia's regular advisories (private sector).

DEFINITION

Watering holes – where adversaries compromise a legitimate website in order to deliver malware to any visitor or subset of visitors – are often designed to take advantage of vulnerabilities in software like Adobe Flash. Visiting infected web sites is often the only user action required.

Web-seeding techniques

State-sponsored cyber adversaries and cybercriminals have continued to use strategic web compromises to target users. By compromising web sites frequently visited by targets, adversaries are able to exploit targets without overt communication, such as spear phishing emails. Strategic web compromises have proven effective for thematic campaigns, such as targeting foreign policy and defence organisations via the compromise of think tanks and media organisations, but pose an equal threat to all users.

Malicious advertising (Malvertising): growing, effective and targeted

Malvertising allows an adversary to target a specific audience by exploiting online advertisement networks used by popular websites that visitors trust. By using the advertisement network's profiling of website visitors, an adversary can focus on specific target groups such as government departments, military personnel or senior business executives. Typically, either malicious code is inserted into an ad being presented to users in the course of their normal browsing or a benign ad is used to redirect the user to somewhere that will download malicious code automatically. Importantly, adversaries can make their ads, and themselves, appear legitimate by serving up non-malicious ads to the vast majority of users, using legitimate companies' domains for the redirects and by swapping out non-malicious ads for malicious ones for only a limited period of time. As such, malvertising requires no victim interaction, targets historically vulnerable software (such as Adobe Flash plugins), and is difficult to detect. Cyber adversaries – predominantly cybercriminals – will continue to misuse advertising networks to exploit victims' browsers and deliver malware. Furthermore, the combination of malvertising with

Adobe Flash

The ACSC has identified increased exploitation of vulnerabilities found in Adobe Flash. Cyber adversaries will use these vulnerabilities to enable compromised websites (watering hole techniques) and malvertising to host crimeware tools.

In a recent investigation the ACSC identified a number of Australian business websites, regularly visited by government staff members, being used as watering holes. The websites had been compromised to host Adobe Flash exploits. Government staff had a genuine need to access the websites and did not have to authorise nor knowingly download any files for the exploit to run.

The ACSC recommends reviewing business requirements for the use of Adobe Flash.

CASE STUDY

Defending against strategic web compromises

On 26 May 2016, ASD identified suspected malicious files present on a government network. The files had been downloaded when several staff members visited a legitimate website, which was compromised to redirect users to another compromised server containing the malicious files.

Analysis confirmed the malicious files were Flash files which enumerated browser details, encrypted them and passed them on to a server. The Flash file then injected JavaScript into the user's browser which then attempted to obtain the respective public IP addresses.

ASD determined that this activity was likely opportunistic in nature and not a targeted or persistent threat to the government network. Although users from another government network had visited the same compromised website, that particular network had Flash blocking implemented at its gateway which prevented the malicious Flash file from penetrating the network. Consequently, the affected government agency was provided with advice on Flash blocking and removing or modifying browser functionality in order to protect is network from this type of malicious activity.

CASE STUDY

Various Canberra based websites hosting exploit kit

On 4 August 2016, the ACSC became aware that websites of various Canberra based businesses - some of which were located in close proximity to government departments - were hosting an exploit kit redirect which forms the first step in a process to compromise visitors. Subsequent analysis indicated that the exploit kit redirect was part of the Neutrino Exploit Kit which is used to gain access to victim hosts in order to drop malware.

The ACSC determined that the activity was most likely opportunistic in nature and was not targeted at any particular government department's network. The ACSC contacted the owners of the websites hosting the exploit kit redirect and provided detection and remediation guidance. Based on feedback received, a number of Wordpress site owners were able to identify and remediate the exploit kit redirect.

the use of exploit kits, normally used by cybercriminals, could allow many foreign states to blend in with cybercrime activity and help to obfuscate their intent.

Real-time bidding (RTB) is a method used by advertisers to deliver their ads quickly to a specific audience, but the use of RTB could also limit the exposure of adversaries' tools and techniques by only distributing their malware to specific audiences. Ad networks profile website visitors, acquiring the user's general location from a database of geo-located IP addresses and inferring user interests through tracking cookies. This information is provided to potential advertisers to bid, in real-time, for ad space attached to the website. Cyber adversaries can see this profiling information and have often created a fake enterprise to serve as a middleman to place bids on these ads. If successful, the designated ad loads immediately, complete with a malicious redirect to exploit servers. The redirect is active for only a few minutes and then discontinued, returning the "legitimate business" page so that no one is alerted to the malicious activity.

Secondary targeting

There has been an increase in the detection of cyber adversaries attempting to gain access to enabling targets – targets of seemingly limited value but which share a trust relationship with a higher value target organisation. It is imperative that organisations understand that they might be targeted solely based on their connections with other organisations – the real target of these adversaries.

Cyber adversaries have been observed using compromised mail servers to send spear phishing emails from legitimate accounts to peer organisations, increasing the likelihood of recipients acting upon them. Adversaries have also been observed scanning for connections from less-protected targets to higher value targets.

Avoiding detection

Sophisticated adversaries persistently and aggressively attempt to compromise Australian networks, and are constantly improving their tradecraft to defeat security controls and remain undetected once compromise is successful. Adversaries have increasingly employed robust, standard encryption algorithms, which hinders detection of malware communications and investigation of their activities. In a typical targeted intrusion, the ACSC has observed adversaries using archive files, such as zip and RAR, to compress and encrypt a copy of an organisation's sensitive information. Adversaries then exfiltrate this information using network protocols and ports allowed by the organisation's gateway firewall or obtain legitimate remote access account credentials, with the aim of defeating network-based monitoring.

PowerShell

The ACSC has observed an increase of systems being exploited using PowerShell. PowerShell is a powerful shell scripting language developed by Microsoft, enabling network administrators to fully control Microsoft Windows systems easily. PowerShell allows automation of a wide variety of tasks, and it can be run locally or across the network. Activities performed from the PowerShell environment bypass many security protections and leave virtually no residual artefacts on the system, thus making any compromise more difficult to identify as well as making any forensic investigation more difficult to perform.

ASD has published a maturity framework document to assist government organisations in taking incremental steps towards securing PowerShell across their environment. It can be found at: *http://www.asd.gov.au/publications/protect/securing-powershell.htm*

The ACSC has also observed sophisticated adversaries using 'in-memory' malware – malicious programs that are never written to a disk – to minimise forensic evidence, hinder detection, and bypass security controls. These adversaries have also increased

their use of low-cost, anonymous commercial services that are easily replaced – including virtual private networks, virtual private servers, cloud hosting services, and dynamic domain name services.

Rapid integration

Sophisticated adversaries have demonstrated an ongoing ability to rapidly integrate new information and opportunities – including publicly released exploits – into their operations in attempts to gain access to systems before patches are released and applied. For example, the ACSC observed leaked exploits associated with the public disclosure of Italian security firm Hacking Team's source code being used by known adversaries within days.

The ACSC emphasises the importance of applying patches to applications, operating systems and devices and considers it as one of the most effective security practices organisations can perform. It is essential that security vulnerabilities are patched as quickly as possible after vulnerabilities are identified and reported by vendors, independent third parties, system owners or users. ASD's *Assessing Security Vulnerabilities and Applying Patches* publication has been developed to provide advice on assessing security vulnerabilities in order to determine the security risk posed to organisations if patches are not applied in a timely manner. It can be found at: *http://www.asd.gov.au/publications/protect/assessing_security_vulnerabilities_and_patches.htm*

Targeting bulk personal and personnel information

Australian networks that hold bulk personally identifiable information (PII) have been, and will continue to be, targeted by cyber adversaries. Organisations should carefully consider how much PII they really need to collect, how they protect it, who they share it with, and the expectations of individuals who are entrusting their PII. Individuals should also consider how much information an online service needs to know about them and minimise the amount shared.

The theft of PII is a key trend that shows no signs of abating. Foreign states, hacktivists, terrorists and cybercriminals have sought to gain access to PII from poorly secured systems in the private sector. The aggregation of a large amount of PII from many people in one location is highly attractive to adversaries, who previously would have had to compile or compromise a number of different sources to find the same amount of information.

Criminals have sought PII to commit financial crime and identity theft. Even basic information – a name and address – is often enough to impersonate victims. Cybercriminals may also try to extort money from organisations by threatening to release the compromised information.

Terrorists and hacktivists hack and release PII in order to embarrass, intimidate or threaten individuals and organisations. ISIL sympathisers have published details of alleged Western government and military personnel, including a small number of Australians, as 'hit lists' while encouraging radicalised individuals to harass or attack them. Some Government employees had used work email addresses for personal business, meaning they could be easily identified and singled out. Often databases are released without context, but ISIL-affiliated individuals have enriched basic PII with information from social media to provide fuller profiles of the targets. Concerns over the vulnerability of individuals' personal information and the potential threat of an attack provided ISIL with valuable propaganda for comparably little effort.

Payroll software compromise

In late 2015, a payroll system utilised by a number of Australian based companies was compromised and the personal data of employees was obtained. The actors used the stolen information, including tax file numbers, to lodge fraudulent tax returns. The incident resulted in considerable financial and reputational damage to the companies impacted by the compromise.

CASE STUDY

Targeted disclosures

Recent compromises and targeted disclosures of information from high-profile entities – including the US Democratic National Committee and World Anti-Doping Administration – demonstrate how cyber capabilities can be used by adversaries to influence, coerce or embarrass a target. While the theft and targeted disclosures of sensitive information is not a new threat, the employment of the tactic in such a brazen manner against high profile entities has almost certainly lowered the threshold of adversaries seeking to conduct such acts.

Damage caused by targeted disclosures can be increased when adversaries seed false information amongst real documents. While this disinformation can be corrected, doing so can be labour intensive and untimely, and there are likely to always be enduring questions about the legitimacy of data, irrespective of claims about its fabrication.

State and non-state adversaries – including hacktivists and terrorist sympathisers – are likely to continue efforts to compromise and release sensitive information.

Credential harvesting campaigns

The ACSC has become aware of a recent round of credential harvesting emails targeting Australian government organisations. The harvesting emails direct the user to access a document via Google Drive, and by clicking on a "View Document" link, the user is then directed to a webpage where credentials are requested and thereby harvested by the adversary. Emails are then sent from the compromised user's account to contacts contained in the compromised user's address book, meaning the malicious emails will appear to be coming from legitimate and trusted sources.

The ACSC advises users to abstain from using corporate credentials on public websites. Where this has occurred, users should reset any corporate passphrase currently matching a private use passphrase, and then reset the private passphrase as well.

Cybercrime targeting customers of online banking

Malware known as Dyre (or Dyreza) and Dridex featured in malware campaigns targeting Australia's online banking portals throughout 2015. While Dyre activity appears to have significantly reduced in late 2015, Dridex appears to remain active in 2016.

Dridex is delivered via spam email with malicious attachments, monitors for activity related to online banking and then steals information and credentials. Dyre enables the redirection of a victim's authentication credentials from their bank's site to the criminal. Although victims think they are interacting securely with the online banking site, their traffic is actively intercepted by the malware. Dyre was also distributed through spam emails with a malicious attachment. Customers of financial institutions in English speaking countries comprised the largest target set, with the malware targeting over 200 banks worldwide, including at least 36 in Australia.

Dyre: Targeting customers of Australia-based companies

Examination of a sample of Dyre malware identified that the list of targets included several Australian banks. Additionally, some Australian-based superannuation management platforms were identified in the target list. Dyre reportedly had significant impact upon retail and business banking systems in Australia. A further list of Dyre targets contained 50 Australia-based companies.

Microsoft Office macro security

Adversaries are increasingly using Microsoft Office macros – small programs executed by Microsoft Office applications such as Microsoft Word, Excel or PowerPoint – to circumvent security controls that prevent users from running untrusted applications. Microsoft Office macros can contain malicious code resulting in a targeted cyber intrusion yielding unauthorised access to sensitive information.

A Microsoft Office macro can contain a series of commands to perform a variety of activities, including malicious activities to exfiltrate sensitive information. If not setup correctly, Microsoft Office macros can automatically execute when the documents are opened, without users ever receiving a security warning.

The ACSC has seen an increasing number of attempts to compromise organisations using social engineering techniques and malicious Microsoft Office macros. The use of these malicious Microsoft Office macros can range from cybercrime to more sophisticated exploitation attempts.

ASD has released the *Microsoft Office Macro Security* publication to introduce approaches that can be applied by organisations to secure systems against malicious Microsoft Office macros while balancing both their business and security requirements. It can be found at: *http://www.asd.gov.au/publications/protect/ms-office-macro-security.htm*

DDoS extortion

DDoS extortion against Australian businesses, including some of Australia's largest financial institutions, has increased. DDoS extortion occurs when a cyber adversary threatens to launch DDoS activities against an organisation unless a fee is paid. These threats can be accompanied by a small-scale DDoS activity – or temporary larger activity – to demonstrate capability.

International serious and organised criminal syndicates have raised DDoS extortion threats against small, medium and large businesses in Australia. Over a three month period, CERT Australia received 15 reports of this activity from different companies.

The DDoS extortion threats begin with an email that informs the victim of a low-level DDoS underway against their website. The email demands a ransom be paid in bitcoin, backed by the threat of a larger DDoS being launched. Multiple ransom demands are made of the individual business and each demand gives 24 hours to pay. However, in instances the ACIC is aware of, further DDoS activity has not followed after these demands were not met. This pattern of activity indicates a reliance on the threat of DDoS activity to scare organisations into paying. Larger organisations targeted in Australia have not reported a significant effect on their ability to conduct business. However, if DDoS extortion threats are repeated against large corporate entities, there could be an increasing threat to profitability.

What does a 'typical' compromise look like?

Based on compromises responded to by the ACSC, many adversaries broadly follow the same approach when compromising a network despite each threat group employing unique tradecraft.

Initial foothold:

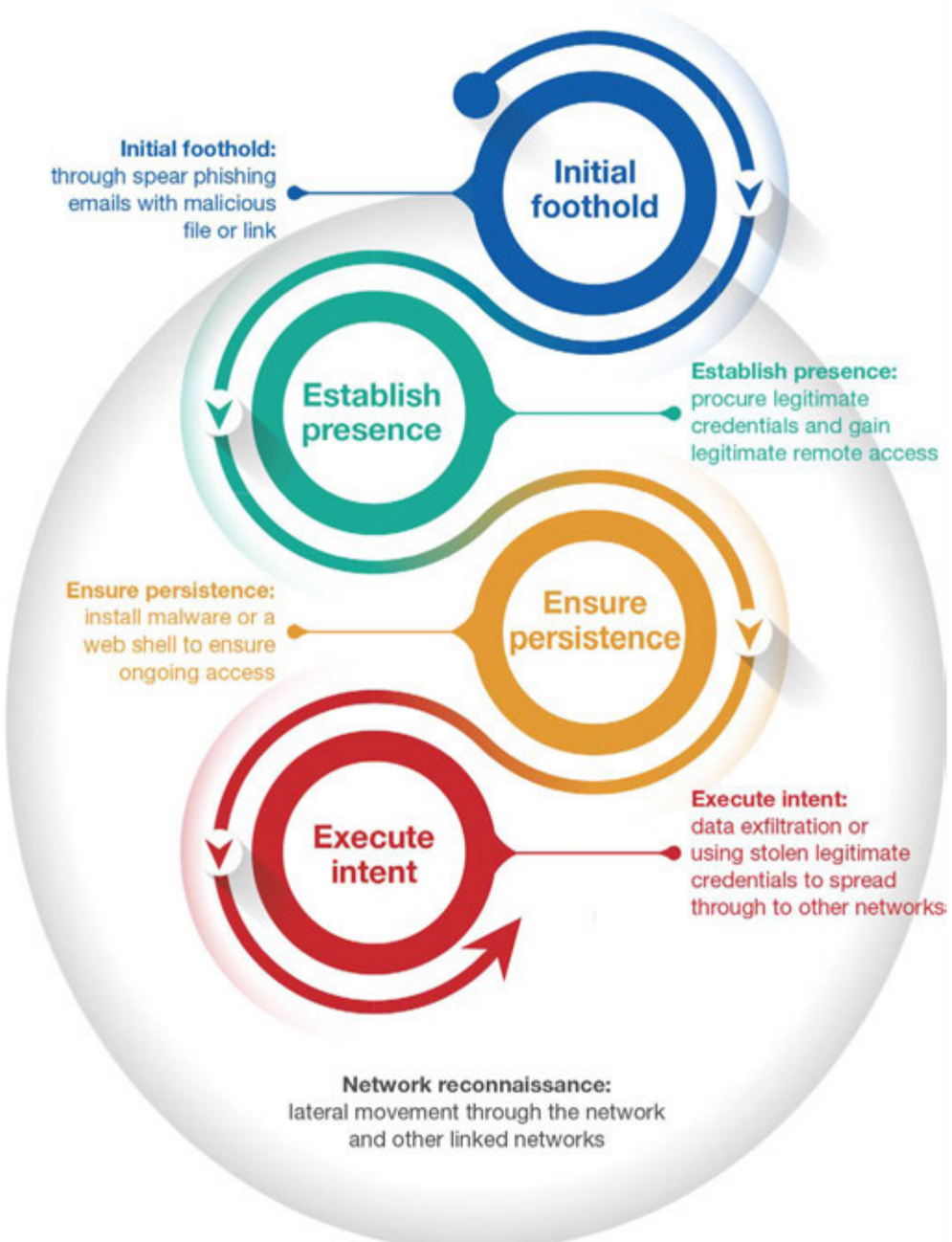
An adversary sends a spear phishing email to their target, relying on trust already established between users as they repurpose genuine emails or contacts to ensure success. When the user opens the malicious attachment or link in the spear phishing email, malware is executed on the user's workstation creating an entry into the network.

Another method used to gain initial access is the compromise – either targeted or opportunistic – of vulnerable internet-facing services. Most exploited services have involved publicly-known vulnerabilities with patches available from application and operating system vendors.

Network reconnaissance is continually performed by the adversary once they have access to the network. Moving laterally, the adversary will study the network infrastructure, search for domain administration credentials and possibly propagate through other linked networks. Adversaries will typically build-up knowledge of the compromised network that rivals, and sometimes exceeds, the organisation's own administrators. In some cases, ASD has observed adversaries actively monitoring administrators to identify upcoming changes within the environment or to determine if the compromise has been detected. As an example, an adversary will regularly access the network to gain updated user credentials, thus avoiding losing access because of password changes.

Establish presence:

Once in the network, the adversary will attempt to procure legitimate user credentials with the goal of gaining legitimate remote administrative access.



Adversaries will typically obtain legitimate privileged credentials by dumping them from administrator workstations, domain controllers, or other key hosts within the network. After legitimate credentials are obtained, the adversary will transition from malware-dependant tradecraft to the use of Virtual Private Network (VPN), Virtual Desktop Infrastructure (VDI), or other corporate remote-access solutions combined with software native to the organisation.

Ensure persistence:

In the types of compromises responded to by the ACSC, adversaries typically want to establish persistence. To do this, adversaries strive to install malware or a web shell to ensure ongoing access should their legitimate accesses cease to function. Malware is typically configured with a limited “beacon rate” to minimise network traffic and evade network defenders. However, web shells are increasingly being used as they generate zero network traffic and are difficult to detect unless the adversary is actively interacting with them.

Execute intent:

Once persistent access is gained, the adversary will execute their intent. This intent could be anything from data exfiltration to enabling lateral movement to the real targeted organisation, exploiting circle of trust relationships between the organisations.

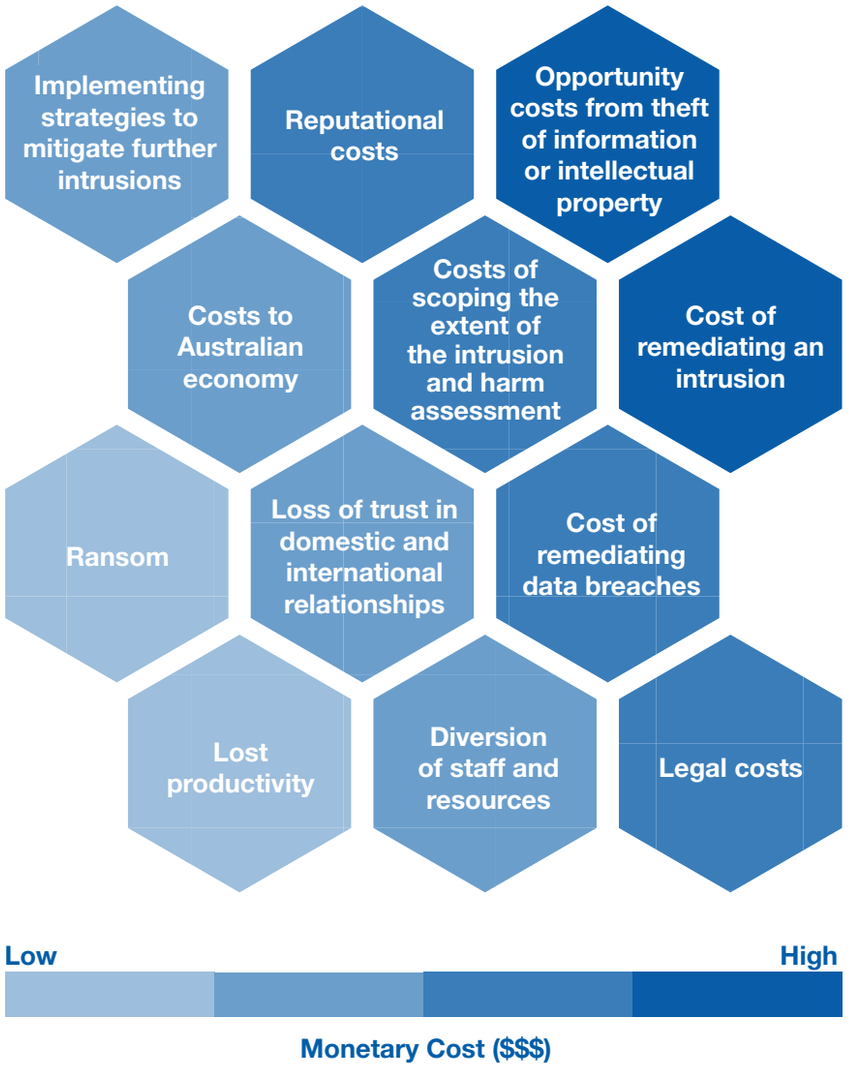
The ACSC has observed adversaries compromise Microsoft Outlook Web Application (OWA) servers and utilising web shells for network persistence. OWA is a full-featured, web-based email client where users can remotely access their emails, contacts, tasks and folders through a secure connection from anywhere with internet access. OWA servers are often both external and internal facing, so they are well-positioned to be used as data collection points for network traffic such as user login details. OWA servers can be used to host web shells as well as to provide a channel for network exploitation disguising as legitimate network activities.

The cost of compromise

No organisation is immune from the risk of compromise. While the upfront costs of implementing robust cyber security mitigation and incident management strategies may seem high, senior management should consider the associated costs that could be incurred if a serious compromise occurs on their network. In the event of a network compromise, not only will organisations be faced with the cost of implementing these strategies to prevent further compromise, they will also incur both higher direct and indirect costs associated with remediation.

There are a number of direct and indirect costs associated with a compromise, including:

- Resources to investigate the extent of the intrusion, understanding the harm, and the immediate remediation of the intrusion (for example by cyber security specialists).
- Reactive implementation strategies to mitigate further intrusions – this is more expensive to do in response to an incident, as timeframes are more compressed compared to implementing these strategies proactively.
- Lost productivity and income, and the costs of diverting staff and resources from other business to deal with a compromise.
- Loss of revenue associated with the theft of information, such as intellectual property, or information about Australia's negotiating position.
- Broader costs to the Australian economy where information is stolen from networks, e.g. personal information used to conduct fraud.
- Reputational costs, including negative social and news media exposure and the trust of your customers, for example in the case of disruption to the availability of online services.



- Costs associated with breaching privacy legislation, or remediating data breaches of financial information.
- Legal costs when impacted third parties may sue for negligence or breach of contract.
- Loss of trust by partners (government or industry), harming domestic and international relationships critical to the organisation.

Preparing for and responding to cyber security incidents

In cyber security, prevention is better than a cure. However, in the ACSC's experience providing incident response, relatively few organisations sufficiently planned or prepared for a significant cyber security incident. The effective management of an incident can greatly decrease the severity, scope, amount of damage and therefore cost of a cyber security incident.

Planning and Preparation

- Have monitoring in place to assess your environment for cyber security threats.
- Have processes in place to detect when an incident may have occurred.
- Assign primary responsibility for incident response in your organisation.
- Have an up-to-date and regularly tested incident response plan and business continuity plan.
- Have up-to-date documentation such as System Security Plans and Standard Operating Procedures.
- Maintain a current security risk management plan for information security systems.
- Know if agreements with contracted IT service providers have arrangements in place for incident response, and understand what type of support you can expect.
- Identify your critical systems.
- Identify key stakeholders including communications and legal.

Responding

- How easily and quickly can you access resources key to mitigating an incident? (For example, system managers, technical experts, Internet Service Provider, system logs and physical system infrastructure.)
- Have an up-to-date after hours contact list for key personnel and external stakeholders.
- Have the ability to identify and isolate an affected workstation or server.

Reporting

- Understand your legislative requirements and obligations for incident reporting.
- Have procedures in place to provide information and reporting to relevant parties during an incident.
- Be familiar with the Cyber Security Incident Reporting process to the ACSC (available on the ACSC's website). Early reporting of significant cyber security incidents to the ACSC will enable the triage, mitigation and containment of the threat, if required. Reporting cyber security incidents also assists the ACSC in developing an understanding of the threat picture for Australian information system networks, and subsequently, enables the delivery of comprehensive cyber security advice relevant to such networks.

The ACSC commonly finds that poor logging records, or a poor understanding of the layout of a network, can impede the ACSC's ability to assist a victim organisation and result in more time and resources being required to remediate the compromise.

Further, the AFP has observed numerous examples of companies not testing what is being logged or retained by analytic agents on their network, resulting in redundant information being compiled. Analytic solutions are important to establish baseline activity in order to detect anomalies and should be regularly tested.

Further information

Strategies to Mitigate Targeted Cyber Intrusions

ASD's *Strategies to Mitigate Targeted Cyber Intrusions*, first published in 2010, focuses on mitigating targeted cyber intrusions by foreign states. The strategies will be revised in 2016 and renamed, tailoring prioritisation and providing additional controls that will make the mitigation strategies also relevant to current and emerging issues such as ransomware and other destructive malware, malicious insiders, and industrial control systems. Once finalised, a list of changes and guidance to implement the mitigation strategies will be available on ASD's website.

The current version of the strategies can be found at: *http://www.asd.gov.au/infosec/mitigationstrategies.htm*

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: *http://www.asd.gov.au/infosec/ism/index.htm*

CERT Australia publications

CERT Australia's public website contains useful information for Australian businesses in relation to mitigating cyber security incidents.

CERT publishes advisories for public consumption that provide detailed and time sensitive information on mitigation strategies and action that can be taken in regard to things such as security flaws or product-specific vulnerabilities.

CERT's website also hosts the 2015 ACSC Survey: *Major Australian Businesses* and CERT's *Cyber Crime and Security Survey,* which provides an understanding of the cyber security posture and attitudes across Australian organisations.

More information can be found at: *https://www.cert.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 *http://www.acsc.gov.au/contact*