Australian Government
Australian Cyber Security Centre

ACSC

AUSTRALIAN CYBER SECURITY CENTRE

2015

THREAT REPORT

Contents

The Australian Cyber Security Centre Threat Report 2015

Foreword

The cyber threat to Australian organisations is undeniable, unrelenting and continues to grow. If an organisation is connected to the internet, it is vulnerable. The incidents in the public eye are just the tip of the iceberg.

Australia must be vigilant and proactive in its approach to cyber security, investing resources to meet the challenges of a complex cyber environment.

Compromise is expensive. It can include financial losses, damage to reputation, loss of intellectual property and disruption to business. Australia cannot afford this.

This is the first unclassified Australian Cyber Security Centre (ACSC) Threat Report. All ACSC partner agencies have contributed to provide information tailored for Australian organisations about the threats their networks face from cyber espionage, cyber attacks and cybercrime. It also contains mitigation and remediation information to assist organisations to prevent, and respond to, the threat.

To combat the threats detailed in this report and reduce the risk of compromise, organisations must move now to implement cyber security measures to make Australia a harder target, increase the confidence of Australians when they are online, and maximise the benefits of the internet for Australian organisations.

Ultimately, this will see organisations and their users taking greater responsibility for the security of their networks and information. The ACSC has been established to help in this process.

The information in this report is designed to assist the achievement of a more cyber secure Australia. Your feedback is welcome.

About the ACSC

The ACSC brings cyber security capabilities from across government together in one location. It is a hub where the private and public sector can collaborate and share information to combat serious cyber security threats. ACSC partner agencies include:

Australian Crime Commission (ACC)

Australian Federal Police (AFP)

Australian Security Intelligence Organisation (ASIO)

Australian Signals Directorate (ASD)

Computer Emergency Response Team (CERT) Australia

Defence Intelligence Organisation (DIO).

For more information about the ACSC, visit acsc.gov.au.

To provide feedback or otherwise contact the ACSC about this Report please use the details available at acsc.gov.au/contact.html.

Introduction

The number, type and sophistication of cyber security threats to Australia and Australians are increasing. Due to the varied nature of motivations for cyber adversaries targeting Australian organisations, organisations could be a target for malicious activities even if they do not think the information held on their networks is valuable, or that their business would be of interest to cyber adversaries.

This first unclassified report by the ACSC describes the range of cyber adversaries targeting Australian networks, explains their motivations, the malicious activities they are conducting and their impact, and provides specific examples of activity targeting Australian networks during 2014. This report also offers mitigation advice on how organisations can defend against these activities.

The ACSC's ability to detect and defend against sophisticated cyber threats continues to improve. But cyber adversaries are constantly improving their tradecraft in their attempts to defeat our network defences and exploit the new technologies we embrace.

There are gaps in our understanding of the extent and nature of malicious activity, particularly against the business sector. The ACSC is reaching out to industry to build partnerships to improve our collective understanding. Future iterations of the Threat Report will benefit from these partnerships and help to close gaps in our knowledge.

The Australian Threat Environment

Australian government and businesses increasingly rely on the internet to deliver products and services. This comes with risks – Australian networks and their users are vulnerable to malicious cyber activity such as cyber espionage, cyber attack and cybercrime.

Australia's information and communications technology (ICT) security community, academia and decision makers in government and business need to:

- keep pace with developments
- identify new vulnerabilities
- advise Australian organisations on how to mitigate emerging threats.

Internet subscribers in Australia

At the end of December 2014 there were:

- more than **12.6 million** internet subscribers in Australia
- **21 million** subscribers to mobile services with an internet connection. [1]

Cyber adversaries targeting Australia

What is a cyber adversary?

A cyber adversary is an individual or organisation (including an agency of a nation state) that conducts cyber espionage, crime or attack.

Cyber adversaries are aggressive and persistent in their efforts to compromise Australian networks and information. They are constantly improving their tradecraft in an attempt to defeat our network defences and exploit new technologies.

Australia is an innovative country with a globally important resources sector. We are a regional leader with global interests and important partnerships. This makes Australia a target-rich environment for cyber adversaries.

There are a range of cyber adversaries motivated to target Australian networks.

Foreign state-sponsored adversaries

Foreign state-sponsored adversaries, including nation-states, seek economic, foreign policy, defence and security information for strategic advantage. Such adversaries have traditionally possessed the most advanced and sophisticated tools to conduct their activities, sometimes maintaining access to an organisation's network for years at a time to steal the information they require. These adversaries are most frequently identified as Advanced Persistent Threats (APT).

Serious and Organised Criminals

Financially motivated criminals that exploit and access systems for financial gain are a substantial threat to Australia. Transnational serious and organised cybercrime syndicates are of most concern, specifically those which develop, share, sell and use sophisticated tools and techniques to access networks and systems impacting Australia's interests.

[1] Australian Bureau of Statistics, *Internet activity Australia, December 2014*, 2015, abs.gov.au/ausstats/abs@.nsf/mf/8153.0/

Issue motivated groups and individuals with personal grievances

Hacktivists and individuals causing nuisance, attempting to draw attention to themselves and their causes, while usually less capable and sophisticated, are still able to cause disruption to Australian government and businesses.

Cyber espionage

> ***What is cyber espionage?***
>
> Cyber espionage is offensive activity designed to covertly collect information from a user's computer network for intelligence purposes.

Cyber espionage can have a significant impact on Australia's national security and economic prosperity. Foreign state-sponsored adversaries are targeting the networks of the Australian government (including state and territory), industry and individuals to satisfy requirements for economic, foreign policy, defence and security information, and gain advantage over Australia.

Australia is an attractive target for cyber espionage due to our:

- resource wealth
- range of commercial interests in Australia and internationally
- expertise in certain fields of scientific research, manufacturing and technology
- particular bilateral relationships and alliances
- prominent role in the Indo-Pacific region.

Significant compromises can also cause economic harm, damage Australia's reputation and undermine international and domestic confidence in Australian network security.

An increasing number of countries are developing cyber espionage capabilities as this type of activity offers high returns with relatively low cost and risk. Many countries will continue to deny they have a cyber espionage program, however, as more cyber security firms publicise these activities, it is becoming more difficult for adversaries to plausibly deny their capabilities.

The ACSC is aware that cyber espionage adversaries target industry networks in addition to government networks to acquire desired information. Cyber adversaries will target the weakest link; if the network security of their primary target is robust, they will move to secondary targeting of other networks that may hold the same information but are easier to compromise.

The cyber espionage threat to Australia continues to evolve and expand. The ACSC is aware of foreign state-sponsored adversaries using malicious software typically used by cybercriminals. In some cases, their activity appears to be financially motivated cybercrime, making it difficult for the victim to identify the true adversary, assess how much damage has resulted from the activity and remediate the damage.

Cyber espionage does not always happen in isolation, with cyber espionage activities efforts sometimes combined with other means of collection. As such, organisations need to work within their own organisations to consider how cyber defences are integrated with other security measures as part of a broader security posture.

Cyber espionage against Australian Government networks

The ACSC sees daily cyber espionage activity targeting Australian Government networks.

Australian Government agencies that have implemented ASD's Top 4 *Strategies to Mitigate Targeted Cyber Intrusions* and a selection of the remaining strategies based on internal risk assessments, are improving their protection against cyber espionage activities.[2] In addition, they are reducing the consequences of these activities to Australia's national security and economic prosperity.

While the overall number of cyber security incidents increased in 2014, the number of confirmed significant compromises of federal Australian Government networks has decreased since 2012. Improving network security forces cyber adversaries to either develop their capability or find alternative targets.

Cyber espionage against Australian businesses

Australian businesses are increasingly being identified as targets of cyber espionage. The theft of intellectual property or commercially sensitive information can:

- seriously impair reputations, profitability and ability to compete in the global economy
- limit business opportunities and reduce a company's economic competitiveness
- undermine a company's business model and viability.

Targeting of systems of national interest and critical infrastructure

> ***What are systems of national interest and critical infrastructure?***
>
> **Systems of national interest** are those systems that, if rendered unavailable or otherwise compromised, could result in significant impacts on Australia's economic prosperity, international competitiveness, public safety, social wellbeing or national defence and security.
>
> **Critical infrastructure** is a subset of systems of national interest.

Australia's systems of national interest and critical infrastructure are vulnerable to malicious cyber activity. In 2014, CERT Australia responded to 11,073 cyber security incidents affecting Australian businesses, 153 of which involved systems of national interest, critical infrastructure and government.

In 2014, the top five non-government sectors assisted by CERT Australia in relation to cyber security incidents were: energy, banking and financial services, communications, defence industry, and transport.

The ACSC relies primarily on voluntary self-reporting for information about cyber security incidents affecting these networks. Some sectors have not yet invested heavily in cyber security, and therefore may not understand the level of risk or potential economic harm to their business. Furthermore, some businesses may be hesitant to report incidents due to the perceived impact or harm to their reputation.

The ACSC is working to forge stronger relationships with Australian businesses to better assess cyber security practices and support improved cyber security.

[2] Access ASD's Top 4 Strategies to Mitigate Targeted Cyber Intrusions at asd.gov.au/infosec/mitigationstrategies.htm

Cyber attack

What is a cyber attack?

A cyber attack is a deliberate act through cyber space to manipulate, destruct, deny, degrade or destroy computers or networks, or the information resident in them, with the effect, in cyber space or the physical world, of seriously compromising national security, stability or prosperity.

The ACSC treats cyber attacks as extremely serious and provocative events. Destructive cyber attacks could be considered equivalent to an armed attack, and therefore, an act of war.

Australia has not yet been subjected to any activities that could be considered a cyber attack. A destructive cyber attack against Australian networks or critical infrastructure – that would seriously compromise national security, stability or prosperity – is unlikely outside a period of significant heightened tension or escalation to conflict with another country.

Due to some overlap in the tools and techniques used in cyber attack and cyber espionage, efforts by organisations to improve network resilience and better protect their networks from cyber espionage will reduce the effectiveness of cyber attacks that target Australia.

As the technological and financial barriers to developing an effective attack capability diminish, Australia faces the threat of a more diverse set of state and non-state-based cyber attacks in the future. Although some non-state adversaries – such as terrorist and issue-motivated groups – have expressed intent to conduct cyber attacks, they will probably continue to use disruption and vandalism to gain publicity and further their causes.

Cybercrime

What is cybercrime?

In Australia, cybercrime refers to criminal acts involving the use of computers or other ICT, or targeted against computers or other ICT.

Pure cybercrime: Crimes directed at computers or other ICT such as unauthorised access to, modification of or impairment of electronic communications or data.

Technology-enabled crime: Crimes where computers or ICT are an integral part of an offence, such as online fraud, online identity theft and the online distribution of child exploitation material.

Cybercrime affects individuals, businesses and governments. Australia's relative wealth and high use of technology – including social media, email and online banking and government services – make it an attractive target for organised criminal syndicates. Misreporting and under-reporting of cybercrime make it difficult to assess the prevalence and impact of offences.

Although it is difficult to establish an accurate figure for the cost of cybercrime in Australia, an October 2013 industry estimate put the cost over the previous 12 months at A$1 billion.[3] This is likely to be an underestimation as it is based on adult individuals affected and does not include the cost to business and government.

[3] Symantec, *2013 Norton Report: Total Cost of Cybercrime in Australia amounts to A$1.06 billion*, 13 October 2013, symantec.com/about/news/resources/press_kits/detail.jsp?pkid=norton-report-2013

There are direct and indirect costs to cybercrime victims including:

- damage to personal identity and reputation
- loss of business or employment opportunities
- impact on emotional and psychological wellbeing of individual victims.

The actual costs of cybercrime at the systemic level encompass the:

- financial losses from fraud
- costs of immediate responses
- system remediation costs
- flow-on costs to government support programs that assist cybercrime victims.

The complexity, sophistication and impact of cybercrime evolves as technology evolves, making it difficult to track the technological advancements of cyber criminals. Furthermore, the complexity and sophistication of malware used for cybercrime now rivals the capabilities of some state-sponsored adversaries. As mentioned previously, foreign state-sponsored adversaries are using malicious software typically used for financially motivated cybercrime to mask their identities and activities.

The ACSC assesses that cybercrime activity will continue to increase over the next five years. Organised crime groups are using sophisticated malware to improve their success, and avoid detection, in gaining unauthorised access to computer systems. Previously considered a niche capability, malware used for cybercrime is now readily available through the online criminal marketplace, often with ongoing technical support, making it accessible to people with minimal ICT knowledge.

Disruption

The disruption of services or networks can affect Australian government and businesses. Hacktivists and individuals causing nuisance favour activities such as denial of service, web defacement and electronic graffiti to disrupt business and government activities. These activities are frequently opportunistic in nature rather than targeted, taking advantage of a victim's poor cyber security posture.

Issue-motivated groups can be particularly active around high profile events that attract significant media attention, as these often result in the disruption gaining maximum visibility. The capabilities of adversaries conducting these activities, while not as sophisticated as that of foreign state-sponsored adversaries, can still be very effective in achieving their limited aims.

Hacktivism and denial of service activities are explained later in the report.

Cyber security incidents reported to ACSC agencies

What is a cyber security incident?

A cyber security incident is any activity that may threaten the security of a system or its information. A compromise is an incident where the security of a system or its information was successfully harmed. Examples of compromises include the extraction of information from a computer network, defacement of a website, or degradation in the reliability of an online service.

Attempts to compromise government, business and other networks of national importance are regularly identified by, or reported to, the ACSC. Cyber adversaries are constantly adapting their techniques in an attempt to breach security and compromise Australian networks.

ACSC partner agencies continued to compile separate statistics until the ACSC was officially opened in November 2014. Consequently the following cyber security incident response statistics for 2014 have been presented separately in this publication.

ASD is predominantly responsible for responding to cyber security incidents involving Australian Government networks and other networks of national importance; consequently, ASD statistics may reflect this bias. The 2014 ASD statistics reflect cyber security incidents that were triaged through the former Cyber Security Operations Centre.

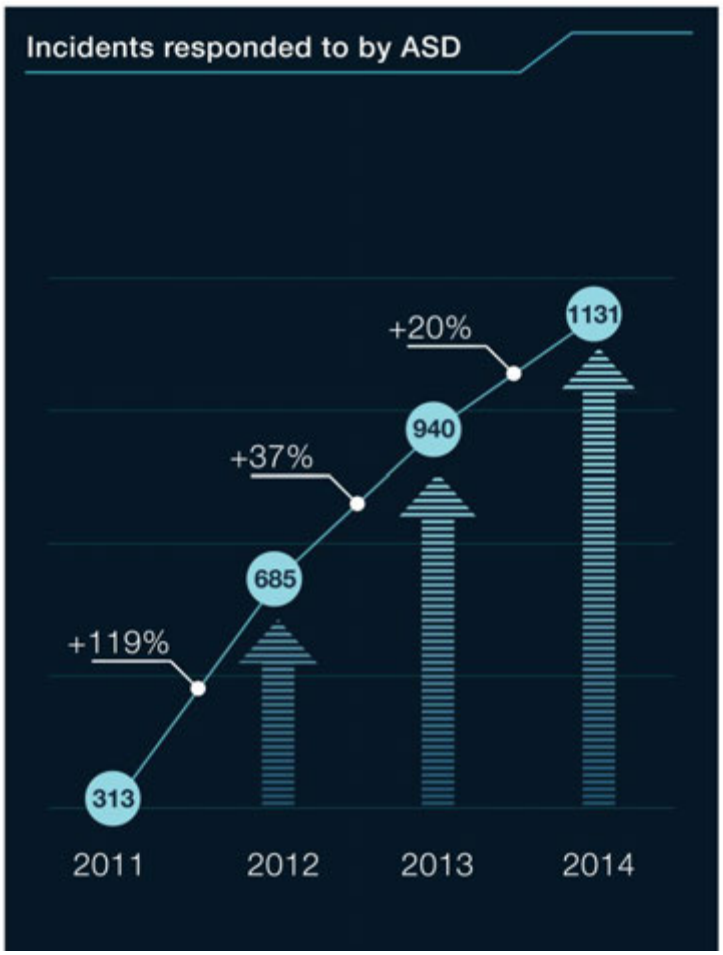

Figure 1: Cyber security incident responses by ASD

CERT Australia is predominantly responsible for responding to cyber security incidents involving Australian businesses and systems of national interest, including critical infrastructure operators; CERT Australia statistics may reflect this bias.

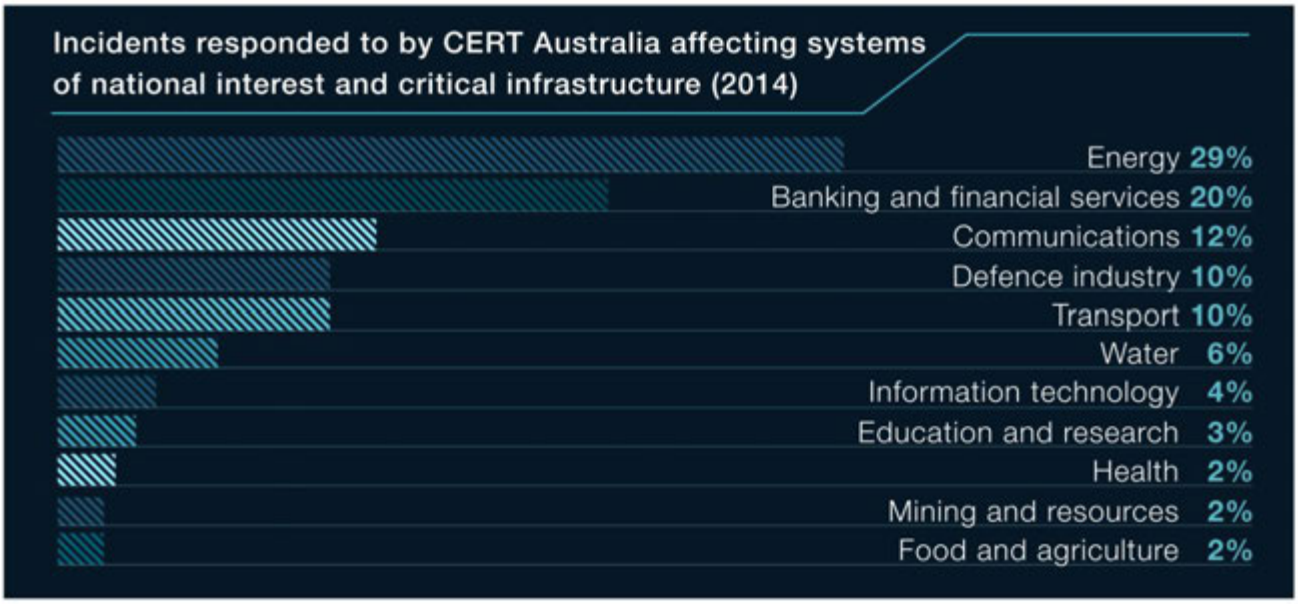

Figure 2: Incidents responded to by CERT Australia affecting systems of national interest and critical infrastructure in 2014

Activity Targeting Australian Networks

Cyber intrusions

What is a cyber intrusion?

A cyber intrusion, also referred to as unauthorised access or hacking, occurs when someone gains access to a computer or device without the owner's permission.

Foreign state-sponsored actors conduct targeted cyber intrusions, seeking information about Australia's business dealings, intellectual property, scientific data and government policy decisions. These activities can give them a diplomatic, political, military or economic advantage over Australia.

Adversaries that conduct intrusions for cybercrime purposes gain unauthorised access to computers, networks and devices to illicitly obtain funds. This can involve extortion as well as extracting usernames, passwords and other information to undertake theft and fraud.

Cyber adversaries exploit security vulnerabilities in a targeted computer or network to gain access, and frequently use social engineering techniques such as carefully crafted emails to entice a user to click on a link or open an attachment. These techniques, also known as spear phishing, remained a prevalent method used to target Australian organisations in cyber intrusions during 2014. The sophistication of these emails continues to grow, making them more difficult to detect.

Case study: Spear phishing

Organisations with poor cyber security are particularly susceptible to compromises resulting from socially engineered emails.

An employee at an Australian business received an email that appeared to have been sent from another business with which they dealt regularly. However, the email had been sent from an unfamiliar webmail account. Although the recipient of the email was suspicious and attempted to check the legitimacy of the email, they opened an email attachment without waiting for a response.

The attachment was an executable (.exe) file masked as a MS Excel file. Consequently, the network was compromised, and it is believed that intellectual property, personnel records, business development proposals and project information may have been stolen.

The compromise could have been prevented if application whitelisting had been adequately implemented on the network, including on the laptop that the employee was using when the attachment was opened.

Remote Access Tools

A Remote Access Tool (RAT) is an administration tool that allows someone to access a computer from a remote location. While RATs have legitimate purposes, they can also be associated with malicious activity. In 2014, the ACSC observed RATs being used in targeted cyber intrusions.

Case study: RAT

In 2014, the ACSC received a report from an Australian state government agency that had discovered a compromise of one of its servers when performing an annual penetration test.

An ACSC investigation confirmed the presence of Java ServerPage RAT (jRAT) on four servers. This had allowed remote administrator-level access to the servers and confidential files stored on them. The default administrator credentials had not been changed after a recent software upgrade. To remediate, the servers were removed from the network and rebuilt.

Watering-hole techniques

What is a watering-hole?

A watering-hole is a compromised legitimate website, frequented by a cyber adversary's intended targets. Malware placed on the website is intended to compromise the computers of visitors to the site.

The use of watering-hole techniques by cyber adversaries targeting Australian networks continues to grow. Taking full advantage of a user's trust in a website, the watering-hole technique provides an effective method for exploitation.

In 2014, the ACSC noted incidents involving watering-hole exploitation of websites regularly visited by Australian government employees. These incidents were mitigated successfully, as the malware was attempting to exploit a vulnerability to which the visitor was not exposed. It is important to understand however that this type of activity is no longer opportunistic; it is now an activity targeting Australian government and business.

During 2014, CERT Australia handled more than 8,100 incidents involving compromised websites. Websites can often be compromised due to poor maintenance or security configuration. Cyber adversaries often target these websites to distribute malware, host phishing websites or build denial of service botnets.

While these issues are relatively easy to remedy from a technical perspective, the potential impact to the website owner and visitors can be significant. In many cases, the owner of the website was not aware of the compromise until they were notified or the website had been blacklisted by a security organisation. A blacklisted website can experience a significant drop in regular traffic and therefore a drop in revenue.

Case study: Watering-hole

In October 2014, CERT Australia issued an advisory warning of watering-hole activity specifically targeting organisations in the energy sector. The advisory listed websites that had likely been compromised, and encouraged clients to report any suspicious activity. CERT Australia clients were able to use the information provided to successfully detect and block communications to watering-hole sites.

Malware

> ***What is malware?***
>
> Malware is MALicious softWARE designed to facilitate unauthorised access to a system, or cause damage or disruption to a system.

In 2014, malware, including ransomware, was the predominant cybercrime threat in Australia. It is a persistent threat because new malware types are developed and released regularly, and antivirus software cannot detect all new variants. Some malware remains dormant on a system for a period of time, circumventing security and running undetected until achieving its objectives.

The Australian Communications and Media Authority (ACMA) operates the Australian Internet Security Initiative (AISI) program. The AISI provides participants with daily notifications of IP addresses on their networks observed as potentially vulnerable to malicious exploits or infected by malware.[4]

Between 17 October 2014 and 14 January 2015, the AISI reported over 15,000 malware compromises daily to Australian Internet Service Providers (ISPs) for them to action.[5]

Data collected by the AISI between April and December 2014 indicates the three malware variants most frequently detected on Australian IP ranges were:

- Zeus
- ZeroAccess
- Conficker.

Zeus

Discovered in July 2007, Zeus is a Trojan that steals banking details through keylogging and form-grabbing. It is spread through drive-by downloads and socially engineered emails. Zeus GameOver is a variant of this Trojan.

In June 2014, approximately 1 million computers worldwide were thought to be infected with Zeus GameOver, causing an estimated loss of US$100m.

> **Case Study: Zeus GameOver takedown**
>
> In 2014, the AFP assisted in operational activity led by the US Federal Bureau of Investigation (FBI), which resulted in the takedown of Zeus GameOver infrastructure. The US obtained civil and criminal orders authorising measures to sever communication between the infected computers and redirect them from criminal servers to government controlled servers. Additionally, these orders authorised the FBI to identify victim IP addresses and provide this victim information to international CERTs, ISPs and other private sector organisations to assist victims in removing the malware from their computers.
>
> Evgeniy Bogachev, the leader of a cybercrime group based in Russia and the Ukraine, was responsible for developing and operating Zeus GameOver, as well as a type of ransomware named CryptoLocker.

[4] The 140 AISI participants include ISPs, educational institutions and other Internet providers

[5] Australian Communications and Media Authority, *AISI malware statistics*, 2014 www.acma.gov.au/Industry/Internet/e-Security/Australian-Internet-Security-Initiative/australian-internet-security-initiative

Case Study: Zeus GameOver takedown (continued) The takedown of Zeus GameOver demonstrates that international collaboration across government and industry can successfully disrupt serious and organised cybercrime activity.[6]

ZeroAccess

ZeroAccess is another type of malware used for financially motivated cybercrime. ZeroAccess causes computers that are infected to generate 'clicks' on advertisements to receive commission from the advertising companies (also known as 'click fraud'). These companies are not usually aware that the click activities are not legitimate. Infection by this malware is typically through drive-by downloads and socially-engineered emails. While ZeroAccess is currently used for click fraud and bitcoin mining, the threat arises from its ability to undertake any activity desired by its controller. The large network of ZeroAccess botnets can be used as the delivery mechanism for any other desired activities that may pose significant risks to Australian interests.

Case Study: ZeroAccess

ZeroAccess is highly commercialised and highly profitable malware with a 'pay-per-install' incentive that has contributed to its growth. The amount paid is based on the country in which the installation occurs, with installations on Australian computers earning US$75. According to AISI data, ZeroAccess malware compromised an average of 4,000 devices per day between October and December 2014.

ZeroAccess targets a range of devices, and uses an advanced method of self-protection by disabling any security tool trying to detect and remove it. In 2014, it affected Point of Sale systems in 60 Australian Pizza Hut outlets. During these incidents, stores were unable to serve customers for up to two hours. In some cases, stores were offline for an entire day while computers were re-imaged.

Despite law enforcement interdiction, ZeroAccess remains resilient to disruption due to the complexity of its network. It continues to be a threat in Australia, through bitcoin mining and click fraud, and it has the potential to be used for other types of cybercrime activity.[7] [8] [9]

Conficker

First detected in November 2008, Conficker is a worm that targets Microsoft Windows operating systems, using vulnerabilities to gain privileged access to a network. Although security patches to address these vulnerabilities have existed for years, many computers remain vulnerable and infected.

[6] GameOver Zeus Botnet Disrupted – Collaborative Effort Among International Partners fbi.gov/news/stories/2014/june/gameover-zeus-botnet-disrupted/

[7] Sophos, *Sophos Technical Paper: The ZeroAccess Botnet – Mining and Fraud for Massive Financial Gain*, 2012 sophos.com/en-us/why-sophos/our-people/technical-papers/zeroaccess.aspx

[8] Australian Communications and Media Authority, *AISI malware statistics*, 2014 acma.gov.au/Industry/Internet/e-Security/Australian-Internet-Security-Initiative/australian-internet-security-initiative

[9] Tech Worm, *Pizza Hut Australia Point of Sales hit with ZeroAccess rootkit malware for over a year*, 2014 techworm.net/2014/11/pizza-hut-australia-point-sales-hit-zeroaccess-rootkit-malware-year.html

Ransomware

> ***What is ransomware?***
>
> Ransomware refers to extortion through the use of malware that typically locks a computer's content and requires victims to pay a ransom to regain access. It can also be accompanied by a threat that the computer has been locked as a result of illegal or questionable conduct by the victim.

Ransomware campaigns against computers in Australia and overseas are increasing. There are a variety of campaign methodologies and themes, but most types of ransomware encrypt files on a computer so that they cannot be accessed until a ransom has been paid. Some types of ransomware will also activate the webcam to try to convince the user that their computer is under real-time surveillance. This may be reinforced by an accompanying message (frequently purporting to be from a law enforcement or government agency) claiming that the computer has been used for illegal activity and demanding payment of a fine.

In July 2014, a number of ACSC partner agencies issued alerts notifying their customers of an aggressive encrypting ransomware campaign. The campaign was targeting government and non-government organisations through phishing emails with links to a website hosting a .zip file containing malicious executable content.

In separate activity during 2014, it was discovered that CryptoWall 2.0 ransomware was using 'malvertising' to infect computers visiting popular Australian websites. These malvertisements exploited Adobe Flash vulnerabilities in web browsers to covertly install CryptoWall 2.0 on the computers of visitors to these websites. The ransomware then encrypted the hard drive and disabled access until the victim paid a fee for the decryption key.[10] It is important to note that the websites themselves were not compromised. Rather, it was the advertising network connected to the websites which did not have sufficient screening detection against advertisements originating from malicious sources.

Many large organisations and some members of the community were able to remove the ransomware infections by restoring computers and data from a backup. However, organisations that had not performed a recent backup experienced much greater disruption (the ACSC was aware of one organisation that had not performed a network backup in the previous 12 months). Some organisations found that, despite restoration from backup, roaming profiles were continuing to execute the malware and re-compromising their networks.

[10] Proofpoint, *Malware in Ad Networks Infects Visitors and Jeopardizes Brands*, 22 October 2014 admin.proofpoint.com/threatinsight/posts/malware-in-ad-networks-infects-visitors-and-jeopardizes-brands.php

Case study: TorrentLocker

TorrentLocker was first identified as a new variant of ransomware in February 2014. Masquerading as CryptoLocker, it initially only targeted Australia but by the end of the year had been observed targeting a total of 13 countries. Australian victims received a ransom message specifying the ransom fee, and demanding that they purchase bitcoins from specified Australian websites and send the payment to the address provided. The ransom amount ranged from A$500 to A$600.

TorrentLocker used the branding of trusted and well-known Australian corporations as part of its social engineering techniques.

Misappropriation of business names and counterfeiting of legitimate brands harms the reputation of these businesses and impacts customer loyalty. Businesses need to invest time and resources to inform customers about scams that exploit their identity, and then incur further costs to improve security.

One prominent Australian corporate victim, whose brand has been exploited, estimates that its response to TorrentLocker, including monitoring, takedown actions against malicious domains, and brand protection, has so far cost A$185,000.

The ACC estimated in December 2014, that approximately 16,000 victims had been affected and paid a cumulative ransom of approximately A$8 million. The numbers of those systems that were infected without a ransom being paid are much higher, and a cost may be associated with each infection for the subsequent system repairs.[11] [12]

Distributed Denial of Service

What is a Denial of Service (DoS)?

A DoS is an attempt by a cyber adversary to prevent legitimate access to online services (typically a website), by consuming the amount of available bandwidth or the processing capacity of the computer hosting the online service. A DoS can also occur unintentionally through misconfiguration or a sudden and unexpected surge in legitimate usage. When multiple computers are used to conduct these activities, such as through the use of a botnet, it is referred to as Distributed Denial of Service (DDoS).

The impact of DDoS activities can be amplified when they are bounced off other internet services. Cyber adversaries are now using infrastructure that can turn small requests into large responses (some up to 500 times larger), meaning that even relatively small botnets can cause significant problems for Australian organisations.

The number of DDoS activities identified by or reported to the ACSC during 2014 remained steady compared to 2013. The ACSC assesses that DDoS activities will remain a threat to Australian networks and organisations, particularly from issue-motivated groups and individuals demanding attention. Cyber adversaries are increasingly finding ways to monetise activities that were previously considered to be solely nuisance value.

[11] iSIGHT Partners, *Analysis of 'TorrentLocker' – A New Strain of Ransomware Using Components of Cryptolocker and CyrptoWall*, 2014 isightpartners.com/2014/08/analysis-torrentlocker-new-strain-malware-using-components-cryptolocker-cryptowall/

[12] Australian Crime Commission, *Organised Crime in Australia 2015*, 2015 crimecommission.gov.au/sites/default/files/FINAL-ACC-OCA2015-180515.pdf

A growing trend observed by the ACSC is DDoS extortion, where an adversary will threaten to launch DDoS activity against an organisation unless a fee is paid. These threats can be accompanied by a small-scale DDoS activity to demonstrate intent.

The ACSC advises Australian organisations not to respond to threats. There is no way to determine if the threat is credible, or to guarantee that the DDoS will not occur if the fee is paid.

The ACSC has recently updated its advice on DDoS, including information on preparing for and responding to such activities, see asd.gov.au/publications/protect/preparing-for-responding-to-ddos-activities.htm.

Case study: DDoS

A major Australian organisation was the victim of a sustained DDoS targeting its main website. An issue-motivated group purporting to oppose the work of this organisation claimed responsibility for the activity. The group had exploited poorly configured domain name system (DNS) infrastructure to conduct the activity.

CERT Australia provided advice to the organisation on how to protect itself from a DDoS activity, and analysed logs of the activity. As a result of the analysis, CERT Australia identified DNS servers utilised in the activity, and contacted the system owners to help them improve the configuration so that those systems would not be used in further DDoS activity.

Hacktivism

What is hacktivism?

Malicious cyber activity conducted by issue-motivated groups or individuals for the purpose of promoting a particular cause or targeting a particular person or organisation associated with an issue or cause.

Another type of malicious activity occasionally observed in Australia is issue-motivated hacking, also referred to as hacktivism. Hacktivists use cyberspace to sustain political debate and engage in protest. This can include electronic graffiti such as offensive propaganda postings on social media platforms and defacement of web pages, unauthorised computer intrusions and other acts of digital tampering. This type of activity can cause disruption for affected organisations.

Over the past two years, the AFP has disrupted activities and arrested individuals involved in the compromise and defacement of government websites and theft of personal and corporate data holdings. While cyber adversaries can operate from anywhere, arrests can be a significant deterrent to hackers in Australia.

Mitigation advice

Mitigating cyber intrusions

Key publications such as the *Australian Government Information Security Manual* (ISM) and the *Strategies to Mitigate Targeted Cyber Intrusions* are regularly updated to reflect the increasing sophistication of cyber adversaries targeting Australian networks. When implemented as a package, the Top 4 *Strategies to Mitigate Targeted Cyber Intrusions* can mitigate at least 85% of targeted cyber intrusions responded to by the ACSC. See both asd.gov.au/infosec/ism/index.htm and asd.gov.au/infosec/mitigationstrategies.htm.

Mitigating watering-hole techniques

Education will not necessarily prevent a user from visiting a legitimate website that has been temporarily compromised as part of a watering-hole attack. Visiting such a website might compromise a user's computer without any obvious indications of the compromise.

It is essential that organisations implement technical measures to defend against this type of activity. In addition to implementing the Top 4 *Strategies to Mitigate Targeted Cyber Intrusions*, organisations should consider introducing additional technical measures such as:

- Strategy 5: User application configuration hardening
- Strategy 6: Automated dynamic analysis
- Strategy 7: Operating system generic exploit mitigation
- Strategy 18: Web content filtering.

Organisations should also ensure that their own websites and web applications cannot be compromised and used as watering-holes.

Mitigation strategies for malware

The ACSC recommends Australian government and businesses defend against malware infections by implementing the *Strategies to Mitigate Targeted Cyber Intrusions*, with particular attention to the Top 4 strategies. In addition:

- educating staff about cyber security can assist in preventing and identifying an initial system infection
- using up-to-date antivirus software configured to perform internet-based reputation checking can help detect malware if it does make its way onto the system
- disabling AutoRun and AutoPlay features may help to prevent malware from propagating through a network via removable media.

Mitigation strategies for ransomware

Avoid paying a ransom if you experience this type of infection, as this perpetuates the incentive for the cyber adversary to continue their activities. Data loss can be minimised by taking the appropriate steps to prevent this type of infection from occurring in the first place.

The ACSC recommends the following to avoid falling victim to ransomware:

- implement the Top 4 *Strategies to Mitigate Targeted Cyber Intrusions*
- block executable files from entering a corporate network through email or web downloads
- inspect compressed file formats for executable content
- create regular offline backups, including backups of peripheral data storage devices.

If you do experience a cyber security incident involving encrypting ransomware, the ACSC offers the following remediation advice:

- identify any compromised workstations and remove them from the network
- block known indicators to prevent an immediate re-compromise, check for profile-resident malware and clean profiles
- restore from backup.

Key Cyber Security Alerts

Heartbleed

In April 2014, Heartbleed, a serious vulnerability in OpenSSL's implementation of the TLS/SSL Heartbeat extension, was publicly disclosed. OpenSSL is commonly used in Apache software running on Linux/Unix web servers, and other Linux/Unix services. Exploitation of this vulnerability causes the memory contents to leak, allowing a cyber adversary to gain access to private keys, usernames, passwords and protected content that could facilitate further cyber activities. The vulnerability also allows cyber adversaries to repeatedly access the data by sending a series of commands to vulnerable servers. Within four hours of the vulnerability becoming public, adversaries were taking full advantage of it, much faster than vendors were able to create and release patches.

OpenSSL released a patch for the Heartbleed vulnerability the day it was publicly disclosed. Organisations using a vulnerable version of OpenSSL were advised to upgrade their OpenSSL, install a new certificate and revoke old certificates.

A problem associated with the vulnerability was that users of affected web servers had to wait for instructions from the organisations *prior* to changing their passwords. Changing passwords before the servers were patched and old certificate revoked would still expose the users to exploitation. Communicating this message and ensuring that users adhered to the specific instructions presented a challenge.

In April 2015, 12 months after Heartbleed was first publicised, it was revealed that an estimated 84% of Australian businesses had yet to fully remediate this vulnerability.[13]

The ACSC urges Australian organisations to check that they are not affected by Heartbleed, and take appropriate action as required.

Case study: Heartbleed

After Heartbleed was publicised, the ACSC saw numerous adversaries conduct testing against a range of systems in Australia.

During an investigation by the AFP in May 2014, analysis of an alleged offender's computer showed that they made over 360 attempts to access data exploiting Heartbleed. The offender targeted remote access servers in an effort to extract usernames and passwords, in an attempt to gain access to more sensitive data.

Victims that had implemented intrusion detection/prevention systems were able to mitigate the activity. The alleged offender was charged with several counts of attempted unauthorised access to twelve Australian servers.

[13] The Register, *Most top corporates still Heartbleeding over the Internet*, 2015 theregister.co.uk/2015/04/08/still_bleeding_one_year_laterheartbleed_2015_research/

Bash / Shellshock

In September 2014, an extreme risk vulnerability in the Bash shell was made public. Bash is the default shell on Linux and Apple OS X systems used to execute command lines and scripts. It is widely present in the firmware of common devices such as routers and wireless access points. The vulnerability affects UNIX based platforms, including Apple Mac. This vulnerability can be exploited to remotely execute arbitrary code, potentially permitting full system control for cyber adversaries. The vulnerability allows malicious commands to be included, which can then download and run malicious programs.

Patches for this vulnerability are available for download; however, this vulnerability may still be present in third party applications and programs that are embedded in the systems. Vendors must first upgrade the firmware of their appliances and programs for the systems to be considered fully patched.

End of Support for Windows XP and MS Office 2003

In April 2014, Microsoft ended support for Windows XP and Microsoft Office 2003. Organisations still using this software are urged to review the threat and risk assessments for their ICT environments and implement additional controls to reduce their risk exposure.

The ACSC has produced tailored advice for organisations using Windows XP and MS Office 2003, highlighting which *Strategies to Mitigate Targeted Cyber Intrusions* can offer additional security improvements until they upgrade their standard operating environment. This advice is available at asd.gov.au/publications/protect/win_xp_office_2003_end_support.htm.

Microsoft Active Directory Group Policy Preferences Vulnerability

In July 2014, the ACSC notified Australian Government customers of a vulnerability associated with Microsoft Active Directory Group Policy (CVE-2014-1812).

Several months prior to this, Microsoft had released a patch to prevent easy privilege escalation by a cyber adversary. The patch prevented a cyber adversary from creating new local accounts with passwords but did not remove existing vulnerable local accounts from systems or existing group policies.

If the vulnerability is not fully mitigated, a cyber adversary can move laterally across a network. They are able to obtain clear text credentials of local administrator accounts. As such, this vulnerability presents a high level of risk for Australian Government agencies in particular, and other organisations valuable to cyber adversaries.

The ACSC recommends organisations ensure that this vulnerability is patched, or that this feature not be used to store credentials in group policy preferences.

Cloud Computing Security

What is cloud computing?

Cloud computing is a service model that enables network access to a shared pool of computing resources such as data storage, servers, software applications and other ICT services.

There are three types of cloud service offerings: Infrastructure as a Service (IaaS); Platform as a Service (PaaS); Software as a Service (SaaS). Any of these services can be provided through community, hybrid, private or public cloud models.[14]

Cloud computing can be a cost-effective option for providing information technology services, delivering a superior service and greater security in some circumstances. Many Australian public and private sector organisations are already using cloud services to enable their business, a trend that is certain to continue.

Cloud services are subject to similar threat vectors as traditional ICT service models, and can introduce additional cyber security threats to an organisation's information. In June 2014, a company was put out of business when a cyber adversary used the company's legitimate cloud login credentials to irretrievably delete company data from the Cloud Service Provider (CSP).[15]

It is essential that organisations conduct comprehensive risk assessments to identify and manage jurisdictional, governance, privacy, technical and security risks. Some points to consider include but are not limited to:

- Where your data may reside (onshore versus offshore), and therefore whether that data is subject to a foreign government's lawful access, as well as jurisdictional laws. Foreign-owned CSPs operating in Australia may also be subject to a foreign government's lawful access. Major cloud service providers acknowledge that they have to disclose customer data in response to legally binding requests, and may not be able to notify customers beforehand.
- Storing information in multiple disparate locations and allowing more people to access it can increase the opportunities for information and networks to be compromised.
- The multi-tenancy nature of cloud computing (ie hosting multiple customers on the same infrastructure), increases the likelihood of unauthorised access or network compromise. Proof-of-concept exploits have been developed to circumvent virtualisation software that underpins cloud computing technologies.
- Some security measures that were previously visible to and controlled by an organisation will become the responsibility of the CSP. However, organisations must still consider the security of virtualised environments, including implementation of the Top 4 *Strategies to Mitigate Targeted Cyber Intrusions*.

[14] NIST Special Publication 800-145: *NIST Definition of Cloud Computing* csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

[15] Threat post, *Hacker puts hosting service Code Spaces out of Business*, 9 June 2014

Mitigation strategies for risks associated with cloud computing

Although mitigating the risks associated with cloud computing is a responsibility shared between the tenant and the CSP, organisations are ultimately responsible for protecting their information. While cloud computing may be a daunting prospect for some organisations, many of the risks can be mitigated through mechanisms such as the contract with the CSP and specific security measures.

The ACSC has updated its cloud computing security advice for both tenants and CSPs, including identified risks and mitigation advice for managing these risks. The *Australian Government ISM* has also been updated to include information and controls on Outsourced Cloud Services. These publications are complemented by ASD's new *Certified Cloud Services List,* a list of CSPs that have been assessed and certified against security and governance requirements.

Refer to the following for further information about cloud computing:

- Australian Government ISM asd.gov.au/infosec/ism/index.htm
- *Certified Cloud Services List* asd.gov.au/infosec/irap/certified_clouds.htm
- ACSC Protect publications: *Cloud Computing Security for Tenants*; *Cloud Computing Security for Providers* asd.gov.au/infosec/cloudsecurity.htm.

For assistance with legal and financial considerations for contracts, visit the Australian Department of Finance website at finance.gov.au/cloud/.

Incident Reporting

Australian organisations are urged to report cyber security incidents to the ACSC by following the links on the ACSC website acsc.gov.au. Australian government agencies and businesses reporting cyber security incidents to the ACSC can request advice and assistance on how to remediate these incidents.

The ACSC uses cyber security incident reports as the basis for identifying and responding to cyber security incidents across Australia. These reports can also be used to develop new policies, procedures, techniques and training measures to prevent the recurrence of similar cyber security incidents.

Organisations that have outsourced ICT services may request that their service provider report cyber security incidents to the ACSC. This could be specified in either a memorandum of understanding or as part of the service contract. In these cases, it is recommended the service provider inform the organisation's IT Security Advisor about any reporting of cyber security incidents to the ACSC.

ACORN is the primary method for Australians to report cybercrime. ACORN is a national policing initiative of the Commonwealth, State and Territory governments and has been designed to make it easier for Australians to recognise, report and avoid common types of cybercrime. Visit the ACORN website at acorn.gov.au.

In January 2015, the ACSC released a video, *Recognise. Report.* to encourage reporting of cyber security incidents. This video may assist organisations in reinforcing important cyber security messages to staff. Visit the ACSC website to watch the video.

Outlook

The ever-changing nature of technology offers significant opportunities and challenges for Australia's cyber security. Robust cyber defences will continue to allow a high degree of confidence in network and information security. However, the ability of cyber adversaries to create, identify and exploit vulnerabilities in networks and ICT-enabled capabilities will continue to provide opportunities to take advantage of networks. Through support and collaboration, cyber defenders can make it more difficult for adversaries to succeed.

Trends for 2015 and beyond

While the ACSC is still developing a detailed understanding of the full spectrum of threats to Australian networks, we predict the following trends to manifest globally in the near future:

- The number of state and cyber criminals with capability will increase.
- Due to the limited number of quality software developers, cybercrime-as-a-service is likely to increase, reducing the barriers for entry for cybercriminals.
- The sophistication of the current cyber adversaries will increase, making detection and response more difficult.
- Spear phishing will continue to be popular with adversaries, and the use of watering-hole techniques will increase.
- Ransomware will continue to be prominent.
- There will be an increase in the number of cyber adversaries with a destructive capability and, possibly, the number of incidents with a destructive element.
- There will be an increase in electronic graffiti, such as web defacements and social media hijacking, which is designed to grab a headline.

Ensuring a resilient, cyber secure Australia requires the expertise and collective capabilities of the ACSC, government and industry network owners, operators and users, academia and our international partners.

In our approach to cyber security, Australia must remain vigilant, proactive and resourced to meet the challenges of a complex cyber environment.

Cyber security efforts should aim to make Australia a harder target and thereby increase the trust and confidence of all Australians to engage in the benefits the internet brings. Effective cyber security requires a partnership between government and the private sector, with organisations and their users taking greater responsibility for the security of their networks and information.

Glossary

Term	Definition
application whitelisting	Application whitelisting is one of the top four strategies in ASD's *Strategies to Mitigate Targeted Cyber Intrusions*. It is designed to protect against unauthorised and malicious programs executing on a computer. It aims to ensure that only specifically selected programs and software libraries (DLLs) can be executed, while all others are prevented from executing.
botnet	A collection of infected computers remotely controlled by a cyber adversary to conduct malicious activities without the user's knowledge, such as to send spam, spread malware, conduct denial of service activities and steal data.
cloud computing	A service model that enables network access to a shared pool of computing resources such as data storage, servers, software applications and services.
compressed file formats	A type of file format which compresses data to consume less storage space and network bandwidth. Examples of compressed file formats include .zip files, .rar files and .jar files.
critical infrastructure	The physical facilities, supply chains, information technologies and communications networks which if destroyed, degraded or rendered unavailable, damage national security, or the social or economic wellbeing of the nation.
cyber adversary	An individual or organisation (including an agency of a nation state) that conducts cyber espionage, crime or attack.
cyber attack	Includes deliberate acts through cyber space to manipulate, destruct, deny, degrade or destroy computers or networks, or the information resident in them, with the effect, in cyber space or the physical world, of seriously compromising national security, stability or prosperity.
cyber espionage	Offensive activity designed to covertly collect information from a user's computer network for intelligence purposes.
cyber intrusion	Occurs when someone gains access to a computer or device without the owner's permission. Also referred to as unauthorised access or hacking.
cyber security incident	An occurrence or activity that may threaten the confidentiality, integrity or availability of a system or the information stored, processed or communicated by it. A compromise is an incident where the security of a system or its information was successfully harmed.
cybercrime	Criminal acts involving the use of computers or other ICT, or targeted against computers or other ICT. • *Pure cybercrime:* Crimes directed at computing or other ICT such as unauthorised access to, modification of or impairment of electronic communications or data. • *Technology-enabled crime:* Crimes where computers or ICT are an integral part of an offence, such as online fraud, online identity theft and the online distribution of child exploitation material.
Denial of Service (DoS)	An attempt by a cyber adversary to prevent legitimate access to online services (typically a website), by consuming the amount of available bandwidth or the processing capacity of the computer hosting the online service. A DoS can also occur unintentionally through misconfiguration or a sudden and unexpected surge in legitimate usage. When multiple computers are used to conduct these activities, such as through the use of a botnet, it is referred to as Distributed Denial of Service (DDoS).

Term	Definition
drive-by download	Occurs when a user visits a malicious website or a legitimate website that has been compromised, involving malicious software designed to automatically run on the user's computer typically without requiring any additional user interaction.
exploit	A piece of software, a chunk of data, or sequence of commands that takes advantage of a bug, glitch or vulnerability in order to cause unintended or unanticipated behaviour to occur on computer software, hardware, or something electronic (usually computerised). This frequently includes such actions as gaining control of a computer system, allowing privilege escalation or a denial-of-service attack.
form-grabbing	A more advanced type of keylogging where the data is captured from browser forms, before data is sent over the internet to a secure server. This method is able to acquire data regardless of input method (i.e. through the use of virtual keyboard, auto-fill or copy and paste). It only records data specified by the cyber adversary, and logs which website data origin, such as IP address and URL.
hacktivism	Malicious cyber activity conducted by issue-motivated groups or individuals for the purpose of promoting a particular cause or targeting a particular person or organisation associated with an issue or cause.
issue-motivated group	A coalition of communities or individuals, often loosely formed, that is primarily drawn around a common interest.
keylogger	Software on a system that records what a user types on their keyboard or the use of their mouse.
malware	MALicious softWARE designed to facilitate unauthorised access to a system, or cause damage or disruption to a system.
malvertising	A drive-by download primarily affecting legitimate websites, where the malicious software is delivered to the user via an advertisement.
ransomware	Extortion through the use of malware that typically locks a computer's content and requires victims to pay a ransom to regain access. It can also be accompanied by a threat that the computer has been locked as a result of illegal or questionable conduct by the victim.
removable media	Storage media that can be easily removed from a system and is designed for removal, for example USB flash drives or optical media.
social engineering	Manipulating a person into performing actions or divulging sensitive information. Cyber adversaries use a wide variety of tools such as email and social media to conduct social engineering against target personnel.
sophisticated capability	An adversary with a full range of access, expertise and operational reach. Sophisticated state-sponsored adversaries fully integrate cyber, information operations programs and traditional signals and human intelligence collection capabilities.
spear phishing	Also referred to as socially-engineered emails, spear phishing emails are constructed to target specific people, often containing a hyperlink or an attachment which, when clicked on or opened, attempts to download malicious code to a workstation to enable a cyber adversary to conduct further malicious activities. The email is crafted to look like a legitimate email from a legitimate sender. Targeted communication (usually email) to members of an organisation as a group or as an individual in order to acquire sensitive information or infect with malware.

Term	Definition
SQL injection	A vulnerability which results in a cyber adversary having the ability to execute malicious SQL queries that are passed to a database in a network, allowing them to have greater access to data within that database.
state-sponsored	An activity initiated and/or conducted by or for a foreign government body.
systems of national interest	Systems that, if rendered unavailable or otherwise compromised, could result in significant impact on Australia's economic prosperity, international competitiveness, public safety, social wellbeing or national defence and security.
tradecraft	The combination of tools, techniques and procedures used by cyber adversaries to conduct their activities. These tools, techniques and procedures can be distinct and attributed to these adversaries.
Trojan	Malicious software that a cyber adversary aims to run on a user's computer by deceiving the user as to the true intent of the software.
vulnerability	In the context of information security, a vulnerability is a weakness in system security requirements, design, implementation or operation that could be accidentally triggered or intentionally exploited and result in a violation of the system's security policy.
watering-hole techniques	Compromise and placement of malware by cyber adversaries on a legitimate website frequented by their intended targets in an attempt to compromise the computers of visitors to the website.
website defacement	An unauthorised change to the content of a website.