Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Ransomware in Australia

Overview

The Australian Signals Directorate's (ASD) Australian Cyber Security Centre (ACSC) has observed an increase in the number of ransomware incidents affecting Australian organisations and individuals.

This information on risks, impacts and preventative actions associated with ransomware incidents is intended to inform Australian small to medium businesses, industry organisations and Commonwealth entities. The preventative measures outlined below can also be applied to Australian individuals seeking to protect themselves against ransomware incidents.

Ransomware can cripple organisations that rely on computer systems to function, by encrypting all connected electronic devices, folders and files and rendering systems inaccessible. Cybercriminals will then demand a ransom in return for the decryption keys, often in the form of untraceable cryptocurrencies such as Bitcoin. Cybercriminals may also demand payment of a ransom to prevent public release of data stolen during the incident. Ransomware is one of the most frequent and damaging types of malware, demonstrated by cybercriminals' success in gaining access to networks and taking money directly from the pockets of Australians.

Key takeaways

- Ransomware continues to be a prevalent global threat. Cybercriminals using ransomware pose a significant risk to Australia.
- Consistent with global trends, the ACSC has observed cybercriminals successfully using ransomware to disrupt operations and cause reputational damage to Australian organisations.
- Most ransomware incidents occur after other malicious activity has been conducted against an organisation (e.g. phishing campaigns).
- Ransomware incidents will remain a common threat in Australia and globally due to cybercriminals' success.
- All sectors and individuals with information of value are potential targets for cybercriminals seeking opportunities for financial gain.
- The ACSC advises against paying ransoms. Payment of the ransom may increase an organisation's vulnerability to future ransomware incidents. In addition, there is no guarantee that payment will undo the damage.
- Investing in preventative cyber security measures, such as keeping regular offline backups of business critical data and patching known security vulnerabilities, is more cost effective than the comparative costs incurred when attempting to recover from a ransomware incident.
- The ACSC has produced this guidance to raise public awareness and resilience to ransomware incidents to ensure Australia remains the safest place to connect online.

What is ransomware?

Ransomware is a type of malware that cybercriminals use against a victim to prevent access to files or systems that are of value to the organisation until a ransom is paid. Ransomware can cause severe reputational damage and be costly to mitigate. The impact of ransomware may include threat to life, demonstrated by a recent incident targeting a German hospital which resulted in the first reported death from a ransomware attack[1]. Ransomware incidents commonly occur after other malicious activity.

The size or sensitivity of information held by an organisation is largely irrelevant. If a cybercriminal can prevent business-as-usual activities, they have sufficient leverage to deploy ransomware.

Ransomware can infect a device in the same way as other malware or viruses, for example by a user:

- visiting unsafe or suspicious websites,
- opening emails or files from unknown sources, or
- clicking on malicious links in email, social media and peer-to-peer networks.

Cybercriminals may also use these actions to steal credentials in order to exploit vulnerable Remote Desktop Protocol sessions, or find alternate ways to compromise a victim's network.

If affected by ransomware, the ACSC advises against paying the ransom. There is no guarantee the cybercriminal will decrypt files once the ransom is paid, and willingness to pay a ransom potentially makes an organisation vulnerable to future ransomware incidents. For this reason, it is important to maintain regular offline backups of important information and implement good cyber security practices.

Innovations in ransomware

Innovations by cybercriminals have increased the potential damage of ransomware incidents in recent years. Cybercriminals are tailoring their methods to increase the likelihood of a ransom being paid.

Cybercriminals are often sophisticated enterprises. Many have dedicated websites to advertise their successful compromises and publish stolen data from victims. They also employ specialised customer service teams to assist victims with paying in Bitcoin or other cryptocurrency.

There are a number of tactics adopted by cybercriminals to incentivise victims to pay ransoms. Common tactics include:

- Undertaking extensive reconnaissance on a target to understand their size, scope and vulnerabilities and subsequently tailoring their approach to a victim's perceived ability to pay, or potential impact. Some cybercriminals claim to review a company's net income to establish an appropriate ransom amount.
- Increasing the ransom price after a specific time period in order to persuade the victim to make payment early, increasing the pressure on the organisation to resolve the incident quickly and reducing the window for intervention.
- Offering to decrypt a portion of the encrypted network for a reduced price in order to encourage the victim to pay at least part of the ransom. This may also reveal to the cybercriminal which parts of the victim's network are particularly valuable, information they can on-sell to other cybercriminals, or use in subsequent ransomware incidents.
- Targeting sectors who are vulnerable and likely to be under pressure to pay in order to maintain business-as-usual operations for essential or critical services (e.g. the health sector).
- Combining encryption with exfiltration of data, threatening to publicly release information if the ransom is not paid, and publicly releasing stolen information when a ransom is refused (see Case Study 3 below for an example of this occurring).
- Publicly advertising successful compromises prior to the ransom due date, including notifying the victim's customers and partners, designed to place added pressure on the victim.

[1] https://www.zdnet.com/article/first-death-reported-following-a-ransomware-attack-on-a-german-hospital/

How do I prevent ransomware and its impacts?

Australian organisations are advised to adopt multiple layers of defence against ransomware, no single mitigation will protect against all threats. To assist with this, the ACSC has published a prioritised list called the *Strategies to Mitigate Cyber Security Incidents*, under which an Essential Eight mitigation strategies are outlined[2].

The ACSC recommends organisations implement the following approaches in order to prevent and prepare for ransomware incidents[3].

1. Implement 'essential' mitigation strategies to:
   a) recover data and system availability,
   b) prevent malware delivery and execution,
   c) limit the extent of cyber security incidents, and
   d) detect cyber security incidents and respond.
2. Repeat step one with 'excellent' mitigation strategies.
3. Repeat step one with less effective mitigation strategies until an acceptable level of residual risk is reached.

Some of the strategies to consider implementing:

- **Back up computers, phones and other devices regularly**, choosing automatic backups where possible. Backups need to be kept separately from the network, on separate devices or using a cloud service. Immediately disconnect external storage after backups are created to avoid backups also being encrypted. Ransomware can encrypt cloud backups if a user remains authenticated to the service, or auto-sync is enabled with local files. Ensure staff know how to restore files from backups and practice restoration regularly. Additionally, the ACSC recommends:
  - Removal of administrative privileges for staff that don't require them.
  - Education of users so they're less likely to access malicious hyperlinks, visit unknown websites, and are able to recognise slight changes in URLs.
  - Looking for the padlock symbol and 'https' in the browser address bar when surfing the net. Information about secure browsing can be found on the ACSC's website[4].
  - Installation and regularly updated antivirus software, or utilisation of the build-in Windows 10 virus protection functionality.
  - Installation of a firewall to stop traffic from untrustworthy sources getting onto the network.
  - Enabling multi-factor authentication where possible and encouraging the use of passphrases. Visit the ACSC's website for more information on how to enable multi-factor authentication[5].
- **Ensure operating systems and software are regularly patched**. As with the regular backups, this should be done automatically where possible. This includes ensuring internet-facing devices are configured properly, with security features enabled. Information about enabling software updated can be found on the ACSC's website[6].
- **Disable macros in Microsoft Office** where possible. For instance, disable the use of Microsoft Office macros for users that don't require them, and only allow the use of digitally signed macros for all other users. Macros originating from files from the internet should be blocked, and macro antivirus scanning used.

[2] https://www.cyber.gov.au/acsc/view-all-content/publications/essential-eight-explained

[3] https://www.cyber.gov.au/acsc/view-all-content/publications/strategies-mitigate-cyber-security-incidents

[4] https://www.cyber.gov.au/acsc/view-all-content/publications/quick-wins-your-website

[5] https://www.cyber.gov.au/acsc/view-all-content/advice/multi-factor-authentication

[6] https://www.cyber.gov.au/acsc/view-all-content/advice/software-updates

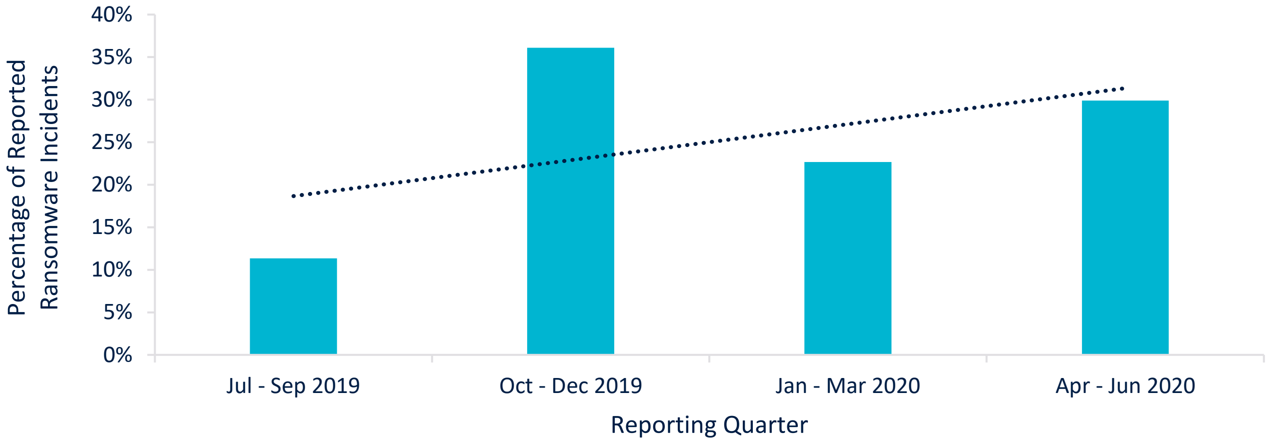
- **Have a plan ready** to reduce the damage and impact of ransomware to business operations. This may include the development and exercising of a business continuity plan and a disaster recovery plan. This will enable a quick recovery and safeguard against future incidents.

How prevalent is ransomware?

Since the 2017 WannaCry[7] ransomware campaign, the ACSC has observed an increase in the number of ransomware incidents against Australian organisations.

The number of ransomware-related cyber security incidents reported to the ACSC during the 2019-20 financial year is outlined in Figure 1 below. Notably, following a compromise targeting the Victorian health sector in September 2019, the ACSC observed a significant increase in the use of ransomware during the October to December 2019 reporting period. Case Study 1 below provides further detail of the health sector targeting which contributed to this observed spike.

Figure 1: Ransomware-related cyber security incidents reported to the ACSC 2019-20 FY



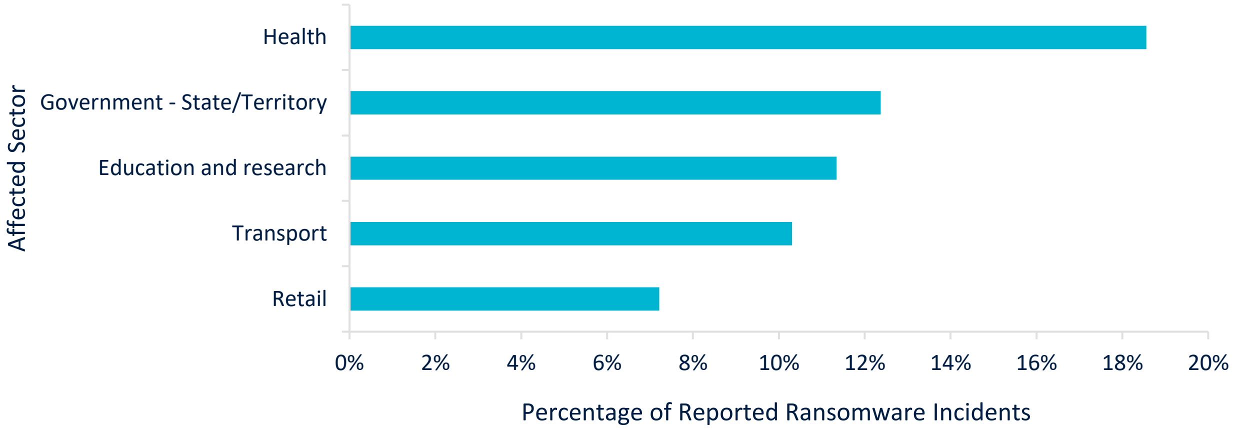
Who is targeted by ransomware?

Anyone that stores digital information is susceptible to a ransomware incident. The size and sensitivity of information stored by the organisation is largely irrelevant. Cybercriminals may use this information to tailor their approach, however, if a cybercriminal can cause disruption by encrypting information that is of value to a victim, they will take advantage of the situation.

The top five sectors to report ransomware incidents to the ACSC during the 2019-20 financial year are outlined in Figure 2. The ACSC observed deliberate targeting across the Australian health sector from September through December 2019 which is reflected in Figures 1 and 2. This trend was also observed globally.

[7] https://www.cyber.gov.au/news/ransomware-campaign-impacting-organisations-globally

Figure 2: Top five sectors affected by ransomware reported to the ACSC 2019-20 FY



Note: These figures are representative of data reported to the ACSC. To provide broader visibility and help accurately identify the volume of cyber security incidents affecting Australia, the ACSC encourages all organisations to report cybercrime and cyber security incidents. This can be done by visiting www.cyber.gov.au/acsc/report and following the relevant prompts.

Case Study 1: Victorian health sector MSP targeted by ransomware

In late September 2019, a number of hospitals and health clinics across the Barwon, Gippsland and South Western regions of Victoria were targeted by a ransomware incident which stemmed from a shared Managed Service Provider (MSP) that had been infected with ransomware. In order to quarantine the spread of ransomware across the networks, the hospitals isolated and disconnected a number of systems from the internet. As a result, access to patient records and contacts, as well as scheduling and financial management systems was significantly impacted. Medical staff had to revert to manual paper-based administration, resulting in patient appointments and surgeries being rescheduled.

There was no indication that the personal or medical information belonging to patients was subject to unauthorised access or exfiltration. A multi-agency incident response team was established, comprising of hospital officials, service providers and cyber security experts working alongside state and federal police and the ACSC. Compromised networks were fully remediated within a number of weeks.

The incident highlights the importance of carefully scrutinising the cyber security measures that are implemented by an organisation's MSP. The ACSC has produced advice for managing risks associated with engaging an MSP, available on the website[8].

Case Study 2: Health provider reacted quickly to avoid ransomware

In March 2020, the ACSC received a report that the network of an Australian health provider was communicating with known malicious infrastructure. The observed activity was historically seen as a precursor to ransomware deployment. The ACSC notified the health provider who then identified an unsupported Microsoft Windows machine as the initial point of compromise. The medical provider then rebuilt and upgraded the machine, ran further checks and remediation across the remainder of the network, and invested in upgraded antivirus software for all machines on the network. As a result, the cybercriminal's access was removed and the provider avoided a ransomware incident.

[8] https://www.cyber.gov.au/acsc/view-all-content/publications/managed-service-providers-how-manage-risk-customer-networks

The incident highlights that ransomware deployment can be avoided if action is taken quickly. Research undertaken by cyber security company FireEye revealed that, in most cases, at least three days passed between the first evidence of malicious activity and the deployment of ransomware[9]. Importantly, organisations must keep and review consistent logs in order to effectively detect indications of malicious activity. The ACSC has produced advice for Microsoft Windows event logging which may assist organisations with their logging activities[10].

Case Study 3: Transport and logistics company becomes victim of two, separate ransomware incidents

In January 2020, the ACSC received a report of a ransomware incident affecting a large Australian transport and logistics company. The incident affected the company's network and telephony systems.

To contain the incident, the company's systems were immediately taken offline which impacted their ability to deliver customer services. The impact of the ransomware also prevented the organisation from fully restoring all of its core systems back online for a number of weeks after the incident.

In May 2020, the company reported to the ACSC that they were experiencing a second, separate ransomware incident. At the time of reporting to the ACSC, the company had shut down all systems, engaged a commercial incident response provider, and was working to contain the incident and provide insights from their investigation to the ACSC for sharing with partners.

Unlike the first incident, the cybercriminal accessed a particular server containing information relating to past and present employees, and details of commercial agreements with customers of the company. The cybercriminal proceeded to exfiltrate and progressively publish a small proportion of that information in an attempt to force the company to pay a ransom. The company did not pay but released a statement that its corporate server containing this information had been accessed. The company proactively informed impacted employees of the incident, providing support and data protection measures.

The incidents draw attention to the disruptive nature of ransomware and the importance of organisations maintaining a forward leaning cyber security posture. The company has completed a number of remediation activities across its environment and is accelerating its strategic cyber security program in partnership with industry, customers and cyber security experts.

How do I respond to ransomware?

Don't pay the ransom: If affected by ransomware, the ACSC advises against paying the ransom. There is no guarantee cybercriminals will decrypt files once the ransom is paid, and there is a chance that files may not be recoverable – wiper malware, where files are permanently modified or deleted, sometimes masquerades as ransomware. Further, the link provided to the victim directing them to information about payment and contacts may inadvertently install further malware onto the victim's system or network.

Payment of a ransom demonstrates a willingness to give in to criminal demands. The willingness of Australian organisations to pay ransoms can perpetuate further criminal activity and may result in unnecessary diversion of investments away from the Australian economy.

Report it: The ACSC manages ReportCyber[11], an online portal for reporting cybercrime incidents. The portal is designed for individuals, businesses, large organisations and Commonwealth entities to report a variety of computer-enabled crimes, including ransomware.

[9] https://www.fireeye.com/blog/threat-research/2020/03/they-come-in-the-night-ransomware-deployment-trends.html

[10] https://www.cyber.gov.au/acsc/view-all-content/publications/windows-event-logging-and-forwarding

[11] https://www.cyber.gov.au/report

Seek help from a cyber security provider: Recovery from ransomware incidents is costly, both from a reputational and financial standpoint. Both Maersk and FedEx shipping companies reported that the NotPetya ransomware incident cost them approximately $300 million each. Early engagement of a cyber security provider may result in timelier remediation than relying on internal IT teams who may not be resourced appropriately to respond, enabling a faster return to business-as-usual operations and saving money in the long run. When a cyber security provider is engaged, ensure they also review the network for security vulnerabilities, preventing future ransomware incidents from occurring.

Note: the ACSC, and most cyber security providers, will not be able to provide you with a decryption key.

Further information

Our partners have additional information available on their websites. Australian organisations are encouraged to also visit:

- The United Kingdom's National Cyber Security Centre (NCSC) (https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks#stepsifinfected). The NCSC has provided a series of steps that can be taken to prevent a ransomware incident, and advice on what to do if your organisation has already been attacked by ransomware. They have also recently released an advisory targeted at UK education sector (https://www.ncsc.gov.uk/news/alert-targeted-ransomware-attacks-on-uk-education-sector).
- The United States' Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) ransomware webpage (https://us-cert.cisa.gov/Ransomware) for additional information, training, mitigations, and best practices.