Australian Government
Australian Digital Health Agency

Risk Mitigation Advice

Preventing and recovering from ransomware

2 May 2017 v1.0
Approved for external information

This document has been prepared for information, communication and technology (ICT) teams in medium to large organisations within the health sector to help increase understanding and facilitate better management of the risks posed by ransomware. The document outlines security measures and practices to help prevent and recover from a ransomware attack.

This document provides general guidance in relation to the risks posed by ransomware and is not intended to be comprehensive.

Summary

Ransomware is a type of malicious software that denies access to computers and files and demands that affected organisations make a payment to regain access to their information. CryptoLocker is a particularly virulent and widely known form of ransomware that encrypts all files located within the infected computer, its shared network drives, and any attached storage. Ransomware has become increasingly common within the health sector [1] and may pose a significant risk to the security and privacy of individual health information and impede organisations' ability to deliver healthcare services [2].

Given that healthcare providers have professional and legal obligations to protect individual health information [3], it is recommended that ICT teams review and assess the adequacy of security measures in place to mitigate the risks posed by ransomware.

Impact

A ransomware attack on a healthcare provider can potentially cause significant financial, reputational, health and safety harm. The level of harm depends on the effectiveness of existing security measures and the number and criticality of affected systems. Any network connected system could be affected, such as: desktop computers; clinical, personnel or financial information systems; databases containing sensitive digital health records; or medical devices. The impact could be minor or severe with the potential to disrupt a healthcare facility's ability to deliver effective healthcare.

While ransomware attacks generally seek to deny access to an organisation's files and systems, depending on the access obtained, an attacker could also read, modify, export or publicly release digital health records. In the USA, health records have a high value on the black market and provide attackers an additional revenue stream to ransom payments [4]. Some attackers may threaten to publicly release sensitive data if a ransom is not paid [5].

Attack vectors and vulnerabilities

Generally, attackers initiate ransomware attacks by exploiting vulnerabilities in browsers or other applications (for example, email clients, PDF readers and so on), or by fooling users to open email an attachment, or follow a link in an email.

More recently, other variants have exploited weaknesses in the Remote Desktop Protocol in Windows [6] or compromised an organisation's web server to distribute ransomware [2]. It is possible that future variants could exploit any network, operating system, or application vulnerability remotely accessible from the internet.

Depending on the variant, ransomware may install itself on a single computer, or propagate and compromise many computers [7]. Once it has installed itself, most variants will encrypt files on the infected computer and files that are connected to, or accessible by, the compromised computer, such as network shares, external hard drives, synchronised cloud storage, and potentially some cloud applications [8].

Ransomware variants differ in how they encrypt files. Some variants, such as CryptoLocker, use public key encryption and delete Shadow Volume Copy in Windows, which means the only way to recover encrypted files is by restoring them from backups. Some variants target web application servers and encrypt data as it is written to the database and decrypt it when the data is read through the web application. Later, when the attacker removes the decryption key, any content that was previously encrypted becomes unreadable. The longer an attacker is able to delay detection, the more difficult it is to recover data following the initial compromise due to the contamination of backups [9].

Typically, attackers tweak and test their ransomware to ensure the variant has a low rate of detection by anti-virus software when first distributed. Hence there is a lag between the release of a new ransomware variant and the ability for anti-virus signatures to detect and prevent the ransomware executing.

Preventing and recovering from an attack

Preventative measures

Controls to help prevent ransomware attacks include:

1 Segment and segregate the network to ensure that valuable data, systems and storage are only readable and writable by authorised, authenticated users [10]. Deploy network level authentication via 802.1x or network access control, or both, to ensure only authorised devices connect to your network.

2 Once you control the devices on your network, it is easier to manage the security of software on your network. Ensure that only fully supported and up-to-date operating systems and applications (including web browsers and email clients) are allowed to operate within your network [11].

3 Implement an application whitelisting solution for servers and desktops [12]. For example, AppLocker [13] is built into Windows 7 and Windows Server 2008 R2 and later versions. Software Restriction Policies are available for earlier versions of Windows [14].

4 Configure hardware and software to be secure [15] [16]. Disable pop-ups and plugins in browsers and disable or control the use of macros in Microsoft Office applications [17]. Configure desktops and servers so they do not auto-run content from removable media such as USBs, DVDs and mounted network shares.

5 Reduce the use of administrative privileges [18]. Ensure all users operate from a limited user account when accessing email and the web and that privileged accounts

(administrator or root) are restricted to staff who need them and only use them when required.

6 Deploy up-to-date anti-virus and spam filter protection on mail gateways, desktops and servers. Configure anti-virus protection to automatically conduct a malware scan of removable media when inserted.

7 Implement an authenticated web proxy server for outbound connections to the internet and to block access to known malicious URLs, domains or IP addresses.

8 Educate users about the dangers of phishing and clicking on links or opening attachments in email from unknown sources [19]. The Australian Government's Stay Smart Online and ScamWatch sites provide useful resources to help raise user awareness of online threats.

Prepare to recover

If prevention fails, having backups that are not contaminated by the ransomware will significantly mitigate the impact of a ransomware attack.

1 Develop an Incident Response Plan that outlines the procedure for reporting and handling incidents [20]. The plan should detail who is responsible for coordinating the response to the incident, and the internal and external contacts, including cloud application vendors (if applicable). Once developed, all staff should be made aware of the content of the plan so that they understand their responsibility to report incidents in a timely manner, and know how to do so.

2 Develop and implement a backup plan that identifies critical data sources and backup processes. Ensure that at least one backup destination is not continuously connected and is separate from its source systems. This is important as backup files stored on a continuously connected USB external drive, accessible from a connected network drive, or copied and synchronised to a cloud destination, for example, are at risk of being contaminated by ransomware. The plan should include verification that scheduled backups complete successfully.

3 Maintain pre-prepared, up-to-date, securely configured images (operating system and applications) to re-image affected desktops and servers if required.

4 For critical cloud hosted applications, such as clinical information systems, contact the vendor to determine what protection they provide to prevent a malware infection, and what recovery assistance they will provide if ransomware either infects the cloud application or encrypts cloud data.

5 Document the system recovery process (system and data) and practise restoring backup data at least quarterly. This will help identify and address any problems with the backup and recovery process.

Corrective actions after an attack

1 Disconnect affected systems from the network as quickly as possible to prevent the ransomware encrypting connected file shares or propagating further.

2 Identify systems compromised, including accessible data sources.

3 Attempt to identify the ransomware variant as this may inform your mitigation and recovery options and help assess the impact of the attack [21] [22].

4 Follow your procedures to re-image the infected systems and restore data from backups.

5 Review the adequacy of existing security measures to help prevent further attacks.

Additional advice

1 Paying attackers is not recommended as this will encourage further attacks and does not guarantee you will be able to recover affected files or avoid a data breach [23]. It is suggested that you seek legal advice if paying the ransom is considered necessary.

2 If systems used to access or update the My Health Record system are compromised, it is possible that the security or integrity of the My Health Record system has also been compromised. For any event or situation where there is a suspected or actual data breach of the My Health Record system, organisations are required to notify us, the Australian Digital Health Agency, (the System Operator) [24]. In addition, organisations in the private sector are required to notify the Office of the Australian Information Commissioner (OAIC) [25].

3 Government agencies and businesses covered by the *Privacy Act 1988* (Cth) will also need to report individual health information breaches under recently introduced amendments to the Privacy Act. Refer to advice from the Office of the Australian Information Commissioner (OAIC) for details [26].

4 If your organisation doesn't have the resources or expertise to implement effective mitigation strategies, it is recommended seeking professional advice from a reputable IT service provider or consultant.

There are a range of information security standards and frameworks, including those applicable to state jurisdictions, which healthcare providers can use to improve the security and resilience of their digital health systems and help meet their professional and legal obligations to protect individual health information.

References

1. *Healthcare held to ransom.* [Internet]. Available from: http://www.cso.com.au/article/597125/healthcare-held-ransom-how-protect-australian-healthcare-systems-patients-from-cybercrime/.
2. *Ransomware and recent variants.* [Internet]. Available from: https://www.us-cert.gov/ncas/alerts/TA16-091A.
3. *Privacy and security of digital health.* [Internet]. Available from: http://www.digitalhealth.gov.au/using-the-my-health-record-system/maintaining-digital-health-in-your-practice/privacy-and-security.
4. *Hackers selling healthcare data in the black market.* [Internet]. Available from: http://resources.infosecinstitute.com/hackers-selling-healthcare-data-in-the-black-market/.
5. *Webcast: Prepare and respond to healthcare ransomware.* [Internet]. Available from: http://healthitsecurity.com/resources/webcasts/prepare-and-respond-to-healthcare-ransomware-attacks.
6. *Ransomware using Remote Desktop to spread itself.* [Internet]. Available from: https://www.scmagazineuk.com/ransomware-using-remote-desktop-to-spread-itself/article/535270/.
7. *Microsoft warns of a new self-propagating malware.* [Internet]. Available from: https://www.scmagazine.com/new-ransomware-has-worm-like-ability/article/528210/.
8. *Ransomware a threat to cloud services too.* [Internet]. Available from: https://krebsonsecurity.com/2016/01/ransomware-a-threat-to-cloud-services-too/.
9. *Ransomware 2.0 'crypts website databases – until victims pay up.* [Internet]. Available from: https://www.theregister.co.uk/2015/02/03/web_ransomware_scum_now_lay_waste_to_your_backups/.
10. *Network segmentation and segregation.* [Internet]. Available from: http://www.asd.gov.au/publications/protect/network_segmentation_segregation.htm.
11. *Assessing security vulnerabilities and applying patches.* [Internet]. Available from: http://www.asd.gov.au/publications/protect/assessing_security_vulnerabilities_and_patches.htm.
12. *Implementing application whitelisting.* [Internet]. Available from: https://www.asd.gov.au/publications/protect/application_whitelisting.htm.
13. *AppLocker Overview.* [Internet]. Available from: https://technet.microsoft.com/en-us/library/hh831409.aspx.
14. *Software Restriction Policies.* [Internet]. Available from: https://technet.microsoft.com/en-us/library/hh831534(v=ws.11).aspx.
15. *Workstation and server configuration management.* [Internet]. Available from: http://www.asd.gov.au/infosec/top-mitigations/mitigations-2014-details.htm#21.
16. *User application configuration hardening.* [Internet]. Available from: http://www.asd.gov.au/infosec/top-mitigations/mitigations-2014-details.htm#05.
17. *Microsoft Office Macro Security.* [Internet]. Available from: http://www.asd.gov.au/publications/protect/ms-office-macro-security.htm.
18. *Restricting administrative privileges.* [Internet]. Available from: http://www.asd.gov.au/publications/protect/restricting_admin_privileges.htm.

19. *User education.* [Internet]. Available from: http://www.asd.gov.au/infosec/top-mitigations/mitigations-2014-details.htm#28.
20. Australian Signals Directorate. *Australian Government Information Security Manual*. 2016. Available from: http://www.asd.gov.au/publications/Information_Security_Manual_2016_Controls.pdf.
21. *Virus Total.* [Internet]. Available from: https://www.virustotal.com/.
22. *Ransomware: Q&A.* [Internet]. Available from: https://www.nomoreransom.org/ransomware-qa.html.
23. *Ramsomware.* [Internet]. Available from: https://www.us-cert.gov/security-publications/Ransomware.
24. *Notifications of data breaches.* [Internet]. Available from: https://myhealthrecord.gov.au/internet/mhr/publishing.nsf/Content/notifications-of-data-breaches.
25. *Guide to mandatory data breach notification in the PCEHR system.* [Internet]. Available from: https://www.oaic.gov.au/agencies-and-organisations/guides/guide-to-mandatory-dbn-in-pcehr-system.
26. *Mandatory data breach notification.* [Internet]. Available from: https://www.oaic.gov.au/media-and-speeches/statements/mandatory-data-breach-notification.

Publication date: 2 May 2017

Contact for enquiries
Telephone: 1300 901 001 or email: help@digitalhealth.gov.au

Acknowledgements

Council of Australian Governments
The Australian Digital Health Agency is jointly funded by the Australian Government and all state and territory governments.