A Singapore Government Agency Website

SingCERT
Singapore Computer Emergency Response Team

Listen

Protect Your Systems and Data From Ransomware Attacks

Published on 28 Dec 2020
Updated on 20 Aug 2021

Prevention is key to avoid falling victim to ransomware

What is Ransomware?

Ransomware is a form of malware designed to encrypt files on a device. Threat actors then demand a ransom, typically in cryptocurrency, from the victim to decrypt the files. Some ransomware variants will also try to spread to other machines on the network.

Ransomware is a perennial and constantly evolving global threat in the cyber security landscape, as cyber criminals' tactics evolve in response to improvements made by businesses. To learn more about recent developments in ransomware, as well as other cyber security issues, please visit our monthly CyberSense publication.

How does Ransomware Spread?

Ransomware may spread through phishing emails that contain malicious links or attachments. Clicking on these links typically results in the ransomware being downloaded from an external server. Malicious advertisements may also exploit vulnerabilities in the web browser to serve and install ransomware, commonly known as "drive-by downloads". Ransomware may also be distributed through methods such as brute-force attacks, exploitation of insecure Remote Desktop Protocols (RDPs), unpatched Virtual Private Networks (VPNs), and spam campaigns.

Once a machine has been infected by ransomware, some types of ransomware may propagate across the network by exploiting vulnerabilities in background services. For instance, in 2017, the WannaCry ransomware exploited the Server Message Block (SMB) protocol.

Impact of Ransomware

Ransomware attacks are disruptive to business operations as employees are unable to access the infected files. It is difficult to recover infected files as each type of ransomware requires a unique decryptor, which may not be available for newer ransomware variants. Sensitive and proprietary information may be lost if the data was not backed-up.

Ransomware threat actors may also threaten to publish the data online to pressure victims to pay the ransom, such as what was done by the MAZE ransomware group which publicised the medical files of the Hammersmith Medicines Research to pressure them into paying the ransom, even though they were able to restore their systems.

Preventive Measures

Prevention is key to avoid falling victim to ransomware. Organisations need to take appropriate measures to secure their infrastructure and systems. It is also essential to formulate a backup and recovery plan for critical data, and to perform data backups regularly. To avoid falling victim to ransomware attacks, it is recommended that organisations also adopt the following cyber hygiene practices.

1. Secure Your Systems

Use Anti-Virus; Update your Systems, Software and Applications Promptly

Threat actors commonly exploit unpatched vulnerabilities to gain unauthorised access into systems and networks to carry out other malicious activities, such as ransomware attacks. Organisations should:

- Install anti-virus/anti-malware software and keep the software (and its definition files) updated. Perform a scan of your systems and networks at least once a week and scan all received files. Removable storage devices should be scanned upon connection.
- Update systems, applications and software to the latest version and download the latest security patches. If patching is not immediately possible feasible, implement vendor-provided mitigations instead.

Enable Spam Email Filters, Use Digital Signature and Anti-Spoofing Controls

To reduce the risk to phishing emails reaching end users, organisations should enable strong spam filters, sign emails with a digital signature, and enable the following email authentication protocols to prevent email spoofing where possible:

- Domain Keys Identified Mail (DKIM) to cryptographically sign the email you send to show it is from your domain.
- Sender Policy Framework (SPF) to publish IP addresses which should be trusted for your domain.

- Domain-based Message Authentication, Reporting and Conformance (DMARC) to set a policy for how receiving email servers should handle emails which does not pass either SPF or DKIM checks. DMARC also generates reports, which could be used to understand how your email is being handled.

Enable Microsoft Office macros only when required

One possible delivery mechanism of ransomware comes in the form of malicious Microsoft Office documents that trick victims into enabling macros in order to view its contents. Organisations should allow macros to be enabled only when required.

Implement Network Segmentation and Monitor Network Traffic

- Implement network segmentation. This will limit the spread of ransomware across the network, if one part is compromised.
- Monitor the network traffic for any suspicious connections and block inbound/outbound connections with known malicious IP addresses and URLs.

Review Settings on Exposed Services and Open Ports

Some ransomware variants may take advantage of exposed services and open ports such as the RDP port 3389 and SMB port 445 to spread across the network. Organisations should review if there is a need to leave these ports exposed and restrict connections to only trusted hosts.

Implement Application Control

Consider installing application control software that provides application and/or directory whitelisting. Whitelisting allows only approved programs to run, and can prevent unknown programs, such as malware, from running.

Limit Privileged Access to Authorised Personnel

User accounts with administrative privileges have the rights to execute a wide range of actions on the system, including installing software or accessing sensitive data.

To reduce the chances of a threat actor gaining administrative privileges, organisations should:

- Control and limit privileged access to only authorised individuals who require full access to carry out their work.
- Give users, other than the administrator, the lowest user privileges necessary for work.

- Review and manage the use of all user accounts and disable inactive accounts when they are no longer in use.

Use Strong Passwords and Enable Two-Factor Authenciation (2FA)

Organisations should use strong passwords of at least 12 characters which includes upper case, lower case, numbers and/or special characters, and implement 2FA for all internet-facing services, particularly for webmail, virtual private networks (VPNs), and accounts that access critical systems.

Raise Awareness

Awareness is key to preventing ransomware attacks. Organisations should conduct regular training for employees to raise their awareness and learn good cyber hygiene practices, such as identifying suspicious emails and not clicking on links or opening attachments found in emails from unknown or untrusted sources.

Monitor for Suspicious Activities

Be vigilant in monitoring for suspicious scanning activities and unauthorised login attempts. This will go a long way to prevent your organisation from falling victim to a ransomware attack.

2. Protect your Data

Encrypt Important or Sensitive Data

Organisations should encrypt important or sensitive data as this makes it more difficult for threat actors to access the data if it is stolen. Encryption may also prevent some ransomware variants from detecting the files, if they work by looking for commonly used file types such as images and documents.

Maintain an Updated Backup, and Keep it Offline

Performing regular data backups facilitates data restoration in the event of a ransomware attack. It is important that the backup data is stored offline and not connected to your network, as certain ransomware variants can propagate across the network.

Maintain regularly Updated "Golden Images" of Critical Systems

This entails maintaining image "templates" of virtual machines or servers. These images should include a preconfigured operating system (OS) and relevant software applications. If there is a need to rebuild the system, these images can be quickly deployed.

Limit Data and Properly Dispose Data That Is No Longer Needed

Organisations should limit the data by only storing information needed for business operations, and ensure that data is properly disposed of when no longer needed.

3. Prepare an Incident Response Plan

It is important to develop an incident response plan and conduct exercises to test the plan, before an incident happens. In the unlikely event that the organisation is affected by an attack, having a plan in place and exercising it will help the staff know what actions to take, and prioritise system recovery.

Response and Recovery for Ransomware Victims

If your organisation has been infected with ransomware, these steps may help in response and recovery:

1. Disconnect the infected computer immediately from your network. Doing so isolates the infected system and prevents the ransomware from spreading to other computers. If several systems appear impacted, take the network offline at the switch level. If taking the network temporarily offline is not immediately possible, locate the network (e.g., Ethernet) cable and unplug affected devices from the network or remove them from Wi-Fi to contain the infection.
2. Scan and disinfect the computer with an updated anti-virus or anti-malware application.
3. Go to https://www.nomoreransom.org/ to check if there is a decryptor available for it.
4. Perform data restoration from the backup sources. Most types of ransomware create some form of persistence in the infected computer, and may re-encrypt data if not properly removed. As such, be sure to perform data restoration on a clean installation that is completely free of the malware.

Should you pay the ransom?

SingCERT does not recommend paying the ransom. Doing so does not guarantee that the data will be decrypted or that your data will not be published by threat actors. It also encourages the threat

actors to continue their criminal activities and target more victims. Threat actors may also see your organisation as a soft target and may strike again in the future.

References

https://www.nomoreransom.org/
https://www.cisa.gov/ransomware
https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks
https://www.csa.gov.sg/singcert/publications/global-local-ransomware-trends-2020-q1-q3
https://us-cert.cisa.gov/ncas/alerts/aa21-131a
https://www.cisa.gov/sites/default/files/publications/CISA_Fact_Sheet-Protecting_Sensitive_and_Personal_Information_from_Ransomware-Caused_Data_Breaches-508C.pdf
https://www.ncsc.gov.uk/collection/email-security-and-anti-spoofing

Cyber Security Agency of Singapore

Who We Are

Our Organisation

Mission, Vision and Values

Corporate Logo

Contact Us

News

Press Releases

News Articles

Publications

Speeches

Legislation

Cybersecurity Act

Codes of Practice

Forms

Notices

Supplementary References

Whistleblowing

Programmes

CSA Common Criteria

CSAT Programme

Cybersecurity Labelling Scheme

Cybersecurity Career Mentoring Programme

Cybersecurity Co-innovation and Development Fund

ICE71

PSG Cybersecurity Solutions

SG Cyber Safe Seniors

SG Cyber Safe Students

SG Cyber Talent

SG Cyber Safe Programme

Careers

Overview

Working in CSA

How We Recruit

Job Opportunities

Cybersecurity Development Programme (CSDP)

Internships

Scholarships

SingCERT

Gosafeonline

Contact Us

Feedback

FAQ

Report Vulnerability

Privacy Statement

Terms of Use

Rate This Website

Sitemap

Last Updated 20 Aug 2021