Protect Your Systems and Data from Ransomware Attacks

Prevention is key to avoid falling victim to ransomware

What is Ransomware?

Ransomware is a type of malware designed to encrypt files on a device until a ransom, typically in cryptocurrency, is paid to decrypt the files. Some ransomware variants will also try to spread to other machines on the network, and in some instances, victims' data might be exfiltrated. Organisations may feel compelled to pay the ransom when they have no backup to restore business operations or to stop attackers from divulging sensitive business information.

The recent spate of disruptive, high-impact ransomware attacks has elevated the profile of ransomware attacks from being a sporadic and isolated risk affecting a small number of devices or computer systems, to a massive and systemic threat with demonstrable potential to pose a threat to national security and disrupt critical services. Such disruptions would adversely impact operations and business continuity of any organisation. In some of these attacks, operations were disrupted not because core business-critical systems were hit, but because the attack affected the IT systems that business operations were critically dependent on, causing operations to be halted.

The proliferation of such attacks means that businesses need to review their cybersecurity posture urgently and ensure that their systems are resilient and able to recover quickly from any successful cyber-attacks. Prevention is key to avoid falling victim to a ransomware attack, and organisations need to take preventive measures and be prepared to deal with a ransomware incident before it happens.

This advisory aims to guide organisations in preventing and responding to a ransomware incident. Depending on your organisation's needs, you may refer to the specific section for details:

- What should I know about ransomware?
  - How Ransomware Spreads
  - Impact of Ransomware
- What preventive measures can I implement to protect my organisation?
  - Secure your systems
  - Protect your data
  - Prepare Incident Response and Business Continuity Plans
- I'm hit! What should I do?
- Should you pay the ransom?

What should I know about ransomware?

How Ransomware Spreads

Ransomware commonly spreads through the following means:

- 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 that may exploit vulnerabilities in the web browser to serve and install ransomware, commonly known as “drive-by downloads”.
- Other methods such as brute-force attacks, exploitation of insecure Remote Desktop Protocols (RDPs), unpatched Virtual Private Networks (VPNs), replication through removable media and spam campaigns.

Once a device has been infected by ransomware, some ransomware variants may leverage the initial access to propagate across the network (i.e. lateral movement) by exploiting vulnerabilities found in background services. For instance, the 2017 WannaCry ransomware exploited vulnerabilities found in the Server Message Block (SMB) protocol. The ransomware may also propagate through other commonly exploited authentication techniques (e.g. Kerberoasting, Pass-The-Hash, Pass-The-Ticket) that leverage stolen Kerberos tickets and password hashes to perform lateral movement and subsequently deploy the ransomware payload.

Impact of Ransomware

Ransomware attacks can lead to serious consequences for the organisations, including:

- Temporary or permanent loss of files or data. Recovery of infected files is usually difficult as each ransomware variant requires a unique decryptor, which may not be available for newer ransomware variants. The organisation could lose access to its data, including any sensitive or proprietary if there was no proper backup of data. Besides encrypting the data, the threat actor could also exfiltrate a copy or modify the data in the system which would complicate the recovery efforts.
- Disruption to operations as files or data tied to business-critical computer systems/networks are encrypted, and organisations are unable to deliver their services. If the infection is widespread, an organisation may even be required to shut down operations (and take online services offline) temporarily as system recovery takes place. Given that a ransomware incident is also a sign that the organisation’s network has been successfully breached, organisations would have to devote significant resources to clean up any entry points or backdoors that the threat actor may have used to gain access to the organisation’s systems and networks.
- Leakage of sensitive data could result in reputation damage or fines by the Personal Data Protection Commission (PDPC) as confidential client or vendor information may be exfiltrated and published in the public domain.

Threat actors have also been observed to use the following tactics to coerce victims into making ransom payment:

- Threatening to publish/auction exfiltrated data online, intimidating employees directly through emails or calls, or threatening to notify the victim's stakeholders and media about the data breach.
- Creating a new domain admin account and resetting passwords for other admin accounts to block login access by IT administrators attempting to resolve the incident. IT administrators would then be required to set up a new domain before attempting any system recovery from available backup. If the threat actor detects backups connected to the victim's network, they may delete these backups to delay or prevent system restoration efforts.
- Launching DDoS attacks on the victim's network to coerce victims to negotiate or when ransom negotiations have stalled. These attacks may also be used as distractions to tie up IT security resources while the main ransomware attack is ongoing or simply as a standalone extortion attack.

What preventive measures can I implement to protect my organisation?

Prevention is key to avoid falling victim to ransomware. Organisations should take appropriate measures to secure your network infrastructure and systems. It is also essential to formulate a backup and recovery plan for critical data and perform data backups regularly before an incident. This section outlines several key measures organisations should implement to secure your networks and data, as well as the importance of developing incident response and business continuity plans.

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 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 regularly, and scan all received files. Removable storage devices should also be scanned upon connection.
- Update systems, applications and software to the latest version and apply the latest security patches promptly, especially for business-critical functions. If immediate patching is not possible or feasible, vendor-provided mitigations should be implemented.

Isolate devices that use legacy operating systems

Organisations are advised to upgrade their devices that use legacy operating systems to supported operating systems. If organisations are unable to upgrade their devices, they are advised to take precautionary measures to isolate these devices. The precautionary measures include the following (non-exhaustive):

- Set up Internet Protocol security (IPsec) rules
- Enforce login restrictions
- Isolate network/virtual local area network (VLAN)

Enable Spam Email Filters; Use Digital Signatures and Anti-Spoofing Controls

To reduce the risk of 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 email which does not pass either SPF or DKIM checks. DMARC also generates reports, which can be used to understand how your email is being handled.

Enable Microsoft Office Macros only when required

Another delivery mechanism of ransomware comes in the form of malicious Microsoft Office documents that trick victims into enabling macros to view their content. Organisations should disable macros by default and only allow macros to be enabled when required.

Implement Network Segmentation

Organisations can also consider implementing network segmentation that divides a larger network into smaller sub-networks with limited interconnectivity between them. This will control traffic flow between the sub-networks, prevent lateral movement and limit the spread of ransomware, should one part be compromised. Implementing network segmentation also generates logs for traffic flow between various sub-networks. Organisations should monitor these logs for any suspicious activities and carry out remediation measures, where necessary.

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 your business needs to leave for open ports and if necessary, restrict connections only to 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 and Regularly Monitor all User Accounts

User accounts with administrative privileges have the right to execute a wide range of actions on the system, including installing software or accessing sensitive data. Zero Trust model is a framework that maintains strict access controls by ensuring that all users are authenticated, authorised and continuously validated. Organisations may wish to incorporate the Zero Trust model or any other applicable established framework when monitoring and validating privileges of users and devices.

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 all other users the lowest user privileges necessary for work.

- Review and manage the use of all user accounts and disable inactive accounts.

Regular monitoring should also be conducted on all accounts to detect any suspiciousactivities, such as multiple failed login attempts.Use Strong Passwords and Enable Multiple-Factor Authentication (MFA)

Threat actors may use valid user account(s) with weak credentials as an attack vector. Organisations should implement password policies requiring the use of strong passwords of at least 12 characters which include upper case, lower case, numbers and/or special characters, and implement MFA for all internet-facing services, particularly for webmail, virtual private networks (VPNs), and accounts that access critical systems.

Conduct Regular Penetration Testing & Validate Defence Mechanisms

Conduct regular penetration testing on both external and internal facing networks to identify any vulnerabilities that may be exploited during an attack. This will allow organisations to make timely patches to existing vulnerabilities in networks or systems. Key defense mechanisms such as securing access to sensitive data with robust authentication methods and checking of users' privileges should be validated against simulated actions typically performed by attackers such as data erasure.

Raise Awareness

Awareness is key to preventing ransomware attacks. Organisations should conduct regular training for employees to raise their awareness of cyber threats such as phishing, which is one ofthe most common attack vectors used by threat actors. Employees can 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. Organisations can refer to the cybersecurity toolkits under CSA's SG Cyber Safe Programme as a training resource here: https://www.csa.gov.sg/our-programmes/support-for-enterprises/sg-cyber-safe-programme/cybersecurity-toolkits

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 some 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 then be quickly deployed.

Limit Data Stored and Properly Dispose Data That Is No Longer Needed
Organisations should limit the data by only storing information essential for business operations and ensure that data is properly disposed of when no longer needed.

Prepare Incident Response and Business Continuity Plans

Identify and Protect Business-Critical Assets
Organisations should prioritise the identification and protection of your core business-critical assets. Threat actors may leverage on connections between internet facing servers and internal networks to discover and access business-critical assets. Organisations should also implement data protection measures such as email filtering solutions, network segmentation and data backups to block ransomware techniques and ensure a smooth recovery from an attack. As such, organisations should strongly consider the implementation of network segregation that restricts such connections to protect sensitive information stored in internal servers.

Develop an Incident Response Plan
It is important to develop an incident response plan and conduct exercises to test the plan before an actual attack takes place. This will ensure that instead of having to develop one in the midst of an attack, organisations can swiftly and decisively implement a plan to mitigate the situation. The plan should also be regularly exercised, such as via cyber drills, to help relevant personnel know what actions to take. Organisations may wish to refer to the following Incident Response Checklist developed by SingCERT when developing such a plan:
https://www.csa.gov.sg/Tips-Resource/Resources/singcert/incident-response-checklist

Develop a Business Continuity Plan
Organisations should also work out Business Continuity Plans (BCPs) with measures tailored to your needs to minimise impact to your operations in the event of an attack. BCP drills should be conducted with operational departments and key decision-makers so that all relevant stakeholders are familiar with the plan. In addition, the BCP should also be updated whenever there are important changes in assets or stakeholders.

I'm hit! What should I do?

Should your organisation fall victim to ransomware, please refer to our Ransomware Response Checklist for information on the response and recovery steps. Organisations are recommended to review and familiarise with the steps in the checklist before an incident.

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.cisa.gov/ransomware
https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks
https://news.sophos.com/en-us/2021/10/28/the-top-10-ways-ransomware-operators-ramp-up-the-pressure-to-pay/
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.cisa.gov/sites/default/files/publications/CISA_Fact_Sheet-Rising_Ransomware_Threat_to_OT_Assets_508C.pdf
https://us-cert.cisa.gov/ncas/alerts/aa21-131a
https://www.lepide.com/blog/how-to-prevent-kerberoasting-attacks/
https://www.ncsc.gov.uk/collection/email-security-and-anti-spoofing
https://www.nomoreransom.org/
https://www.cisa.gov/known-exploited-vulnerabilities-catalog
https://www.manageengine.com/products/eventlog/cyber-security/pass-the-ticket-attack.html
https://www.beyondtrust.com/resources/glossary/pass-the-hash-pth-attack
https://learn.microsoft.com/en-us/security/operations/incident-response-playbook-dart-ransomware-approach