Ransomware Response Checklist

If your organisation is a victim of a ransomware incident, the following checklist may assist in identification, containment, remediation and system(s) recovery. Organisations are recommended to review and familiarise with the steps in the checklist before an incident.

👁 Identification and Analysis

- **Step 1:** Identify the systems, applications and accounts involved in the initial breach and secure the identified systems, applications or accounts to prevent continued unauthorised access.

  - As breaches may lead to credential exfiltration, the corporate network should also be secured from continued credential-based access, i.e., the same credentials that can be used to log in to other systems. Examples of such measures include disabling virtual private networks, remote access servers, single sign-on resources and cloud-based or other public-facing assets.]

  - A list can be created to record tasks with assigned owners. This list should be tracked, and each task documented with information such as findings, date, time, etc. for ease of compilation.

- **Step 2:** Identify any outside-in or inside-out persistence mechanisms as threat actors may create some form of persistence in the infected system/network.

  - Outside-in persistence may include authenticated access to external systems via rogue accounts, backdoors on perimeter systems, exploitation of vulnerabilities, etc.
  - Inside-out persistence may include malware implants in the internal network. Attackers may also use a variety of living-off-the-land mechanisms/tools/modifications such as Cobalt Strike, PsTools Suite,

PowerShell Scripts, etc.

- Identification may require the deployment of Endpoint Detection and Response (EDR) solutions, audits of local and domain accounts, examination of data found in centralised logging systems, or deeper forensic analysis of specific systems once movement within the environment has been mapped out.

- **Step 3:** Review existing detection and prevention systems (e.g. AV software, EDRs, Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), etc.) and other relevant logs. This can help identify systems or malware involved in the earlier stages of the ransomware attack.

  - A ransomware incident may sometimes be the result of a prior unresolved network compromise (i.e. the result of existing malware infections such as TrickBot, Dridex or Emotet). Care should be taken to identify and clean up such malware to prevent continued compromise.

- **Step 4:** Acquire evidence for investigation and triaging

  - It is important for organisations to identify the critical devices for restoration and the types of data affected by the malware infection. If the data consists of Personally Identifiable Information (PII), organisations should also refer to and proceed with *Step 18* concurrently.
  - Use an unaffected device or camera to take images of important information, such as the ransom note, any URLs/links, email addresses, bitcoin addresses, encrypted file names, etc.
  - In addition, take note of the date and time of the infection, as well as what the infected device(s) was doing right before the ransomware encrypted the files. Make a record of the time you disconnected the infected device, as well as any actions taken. This information may be important for subsequent investigation purposes.

Containment

- **Step 5:** Disconnect the infected device(s)[1] immediately from your network, the Internet, as well as any wired and wireless connected devices[2]. This will isolate the infected device(s) and disrupt the ransomware's ability to spread to other devices.

  - Remove all network and data cables and unplug any storage devices and dongles from the infected device.
  - Disable all privileged user accounts except for administrator accounts that are required for resetting the infrastructure of the infected device.
  - Isolate at least one known good domain controller in every domain to ensure availability and functionality of domain services.
  - Isolate critical applications hosted on servers such as SAP and billing systems.
  - Disable wireless connectivity, including Wi-Fi and Bluetooth on the infected device.
  - Ensure that the infected device is not able to access the internet.
  - If several devices/subnets appear impacted, consider taking the network offline at the switch level as it may not be feasible to disconnect multiple individual devices/subnets during the incident.
  - 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.

[1] Example: Computers/Laptops, Mobile Phones/Tablets, Storage Devices, Servers
[2] Example: Storage devices, Dongles

- **Step 6:** If disconnecting affected devices from the network is not possible, the last option is to power the devices down. However, this should only be carried out as a last resort as doing so will prevent you from retaining ransomware infection artifacts and evidence stored in volatile memory.

- **Step 7:** Create forensic copies of affected devices for further analysis.

- **Step 8:** Document your incident response process, i.e., all the actions taken thus far.

- **Step 9**: Ensure all evidence is retained for either prosecution and/or post-incident activities.

Eradicate and Disinfect Infected Devices

- **Step 10:** Perform a full anti-virus or anti-malware scan on infected device(s) and connected device(s) to detect and remove any malware found. Ensure that your anti-virus definitions are up to date. Remember to record and/or take images of any suspicious files, programs, or other events that may be significant while running the anti-virus scan and record any malware identified before removing it.

  For further information on managing a malware infection, please refer to the recommendations in the Malware Infection Playbook.

Recovery and Restoration

- **Step 11:** Ensure the ransomware has been removed.

  - Confirm that the ransomware has been completely removed from the device(s). Many types of ransomware create some form of persistence in the infected device(s) and may re-encrypt data if not properly removed. This may

require a factory reset and a clean installation of the operating system and other software.

- You should perform another full anti-virus or anti-malware scan with an updated anti-virus definition and monitor your network traffic after recovery. This is to ensure that there are no traces of malware left in the system.

- **Step 12:** Rebuild devices with prioritisation based on triage results in Step 4 using pre-configured standard images, if available. Once the environment has been cleaned and rebuilt (including affected accounts and the removal malicious persistence of mechanisms), mandate password resets for all accounts, and implement MFA if possible and reset krbtgt password twice. Any associated vulnerabilities should also be addressed through patches, software updates or by implementing other security precautions not previously taken.

- **Step 13:** Progressively reconnect devices/subnets to the network and restore data from an unaffected backup.

  - If you have a backup of your original files that have not been affected by the ransomware, it may be possible to restore your files from this backup.
  - Before starting this process, ensure that backups are only connected to known clean devices. Scan backups for malware to ensure that the backup has not been infected with ransomware.

- **Step 14:** Decrypt your files.

  - Depending on the variant of ransomware, a decryptor may be available for it. No More Ransom (https://www.nomoreransom.org) is a free and reputable online resource for open source decryptors. If a decryption tool is not available, make a backup of the important files that have been encrypted and regularly check the No More Ransom website for relevant decryptor(s).

Lessons Learnt

- **Step 15:** Document lessons learnt from the incident and associated response activities, and update/refine existing incident response plans based on lessons learnt and recommended security guidelines.

- **Step 16:** Consider sharing the learning with relevant staff and authorities.

Notify and Report

- **Step 17:** If you are an organisation, notify your customers, clients, suppliers, as well as staff and employees about the attack as soon as possible so that they can take steps to protect themselves. Your legal team/provider may be able to assist you in the notification process.

- **Step 18:** Organisations may need to assume that data could have been exfiltrated, if the threat actor has successfully gained access to your infrastructure or systems. If your organisation handles personally identifiable information (PII) or business sensitive information, you may be required to report the incident to the Personal Data Protection Commission (PDPC). The website also provides guides and other resources on handling sensitive data.

- **Step 19:** If you believe that financial information was compromised, contact your financial institution.

- **Step 20:** Please provide SingCERT with additional information (e.g. screenshots of ransom note and encrypted files) for our review via the reporting form. The information from your incident - such as the indicators of compromise and how the threat actor gained access to your network - will enable us to understand the scope and nature of the incident, as well as alert and assist a broader range of individuals and organisations.

Note: Several steps in incident response may be highly technical. If necessary, organisations should consider engaging a cybersecurity services vendor to assist with the investigation and/or remediation. Please refer to this list of Cybersecurity Advisory and Consultancy service providers (if required): https://sgtech-prod-api.sgtech.org.sg/api/Common/GetPDF?type=artical&&fileName=f509e67b-1734-4f68-b03e-743fdd659e95.pdf

Disclaimer: This checklist provides guidelines and recommendations on how to prevent and respond to possible ransomware incidents. It is intended purely as a guide and should not be construed as comprehensive. Always consult a trained cybersecurity professional for advice before making any business-critical decisions within your organisation.

References

https://www.cisa.gov/ransomware
https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks
https://www.sans.org/white-papers/33901
https://www.nomoreransom.org/
https://learn.microsoft.com/en-us/security/operations/incident-response-playbook-dart-ransomware-approach