Malware Infection Playbook

What is Malware?

Malware is a malicious software that can cause harm to device(s) if they are executed. Some examples of what malware can do are:

- Corrupt data stored in infected device(s)
- Steal, delete, or encrypt data
- Control your device(s) to perform other malicious actions
- Obtain credentials and access your organisation's systems or services
- Cryptocurrency mining

How does Malware Spread?

Malware may spread through phishing emails that contain malicious links or attachments. Clicking on these links typically results in the malware being downloaded from an external server.

Malicious advertisements may also exploit vulnerabilities in the web browser to serve and install malwares, commonly known as “drive-by downloads”. Malware 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.

The purpose of this playbook is to provide guidance to organisations on the prevention and remediation of a malware infection. This playbook comprises three main sections:

Possible Signs of Malware Infection(s)

Common signs of malware infection may include:

- Significant decrease in device(s) performance
- Inexplicable high CPU/Disk usage
- Unknown program/service running in the background
- Inexplicable device(s) behaviours
- Unknown application installed on devices
- Unexplained internet activities (suspicious search results, browsers having unknown extensions)
- A ransom note demanding payment to release encrypted files ***(Refer to Ransomware Playbook for more information***)

How to Prevent Malware Infection

Organisations should take appropriate measures to review and secure their infrastructure and systems in order to raise their defences against malware threats. The following measures may help to prevent malware infection(s) and/or any monetary losses that may result from it.

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

- 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

Enable Microsoft Office Macros only when required

- A mechanism used by attackers to distribute malware comes in the form of malicious Microsoft Office documents that trick victims into enabling macros to view its contents. Organisations should allow macros to be enabled only when required.

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.

Raise Awareness

- 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 activities such as tell-tales signs of a malware infection listed in the introduction section.

Backup Critical Data and Keep it Offline

- Perform regular backups to facilitate data restoration in the event of a ransomware attack. Backup data should be stored offline and not connected to your network, as some ransomware variants can propagate across the network

For more information, CSA has tailored the SG Cyber Safe cybersecurity toolkits for Enterprise leaders, SME Owners, IT teams and employees. These toolkits will provide one with a deeper understanding of cybersecurity issues and threats, enable stakeholders and IT teams to adopt and implement cybersecurity within the organisation and employees adopting tips to address the most common threats they might face. You can find the toolkits here: https://www.csa.gov.sg/our-programmes/support-for-enterprises/sg-cyber-safe-programme/cybersecurity-toolkits

Incident Response Steps

If your organisation is a victim of a malware infection, the following steps may assist in containment, remediation, and system(s) recovery:

Step 1: Identify and Disconnect the Infected Device(s)

Identify and 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 malware's ability to spread to other devices.

1. Identify the infected device(s)
2. Remove all network and data cables and unplug any devices connected to the infected device(s)
3. Disable wireless connectivity, including Wi-Fi and Bluetooth on the infected device(s)
4. Ensure that the infected device(s) is/are not able to access the internet

It is also important for organisations to identify the types of data affected by the malware infection. If the data consist of Personally Identifiable Information (PII), organisations should also refer to and proceed with *Step 5* concurrently.

Note: If the files in the infected device(s) is/are encrypted and has a ransom note asking for payment to restore encrypted data, your device(s) is/are likely to be infected with Ransomware. For remediation measures on Ransomware, please refer to the Ransomware Playbook.

[1] Example: Computers/Laptops, Mobile Phone/Tablets, Storage Devices, Servers

[2] Example: Storage devices, Dongles

Step 2: Acquire Evidence(s) for Investigation and Analysis

Use an unaffected device or camera to take images of important information, such as suspicious programs, any URLs/links, email addresses.

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 malware infection. Make a record of the time you disconnected the infected device, as well as any actions taken. This information may be important for investigation purposes later on.

Step 3: Scan and Disinfect Infected Devices

Perform a full anti-virus or anti-malware scan on infected device(s) and connected devices to detect and remove any malware found. Ensure that your anti-virus definitions are up to date. Please keep in mind to record and/or take images of any suspicious files, programmes, or other events that may be significant while running the anti-virus scan and record any malware identified before removing them.

Step 4: Recovery/Restoration

Reset Credentials including Passwords

- Change all affected account passwords (especially for administrator and other system accounts) immediately to a strong password of at least 12 characters which includes upper case, lower case, number and/or special characters. (*This will vary in accordance with your organisation's existing password policy.*)

Ensure the Malware has been Removed

- A factory reset, and a clean installation of the operating system and other software may be necessary to completely remove the malware from the device(s) as there are many types of malware that may create some form of persistence in the infected device.
- You are advised to 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.

Restoring from an Unaffected Backup

- If you have a backup of your original files, it may be possible to restore your files from this backup. Please ensure that the backup is free from any malware before proceeding with the restoration.

- 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 5: Notify and Report

- 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.
- Organisations may need to assume that data could have been exfiltrated if the threat actor 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) at https://www.pdpc.gov.sg. The website also provides guides and other resources on handling sensitive data.
- If you believe that financial information was compromised, contact your financial institution.
- Please provide us with additional information (e.g., screenshots) for our review via the reporting form. This 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 playbook provides guidelines and recommendations on how to prevent and response to possible Malware Infection incidents. It is intended purely as *a guide and is not comprehensive. Always consult a trained cybersecurity professional for advice before making any business-critical decisions within your organisation.*