Document Type: Guideline
Document Title: Step-by-step procedure for responding to compromise of systems

Background

Once it is learnt from external or internal alerts about possible network intrusion and it is suspected that one or more system(s) in the IT network infrastructure is compromised, the following steps are recommended to identify, contain and remediate the cyber threats.

These steps should be carried out by the cybersecurity teams/ IT infrastructure management team under the supervision of the Chief Information Security Officer (CISO).

Step 1: Identify compromised system(s)

The initial alert or information regarding the compromise may include the following. It may be noted that not all the information may be available.

I. Victim IP addresses (Internal or public) with timestamps and ports.
II. Victim Windows domain names.
III. Victim Host name.
IV. Victim MAC address.
V. Attacker IP addresses with timestamps and ports
VI. Attacker command and control (C2) Domains.
VII. Malicious file(s) hashes and paths or any other relevant information.

From the combination of details available, compromised systems may be identified.

In cases where **only connection logs towards malicious IP addresses or domains (C2) are available,** then the following steps may be taken to identify the compromised system(s):

I. If the Victim IP address is assigned to a system/server/desktop directly, it is likely that the system/server/desktop itself is compromised.
II. If the Victim IP address belongs to perimeter devices of the organisation, such as Firewall/Switch/Router/Access Point/Proxy server etc., then perform as follows:
    a. Check the connection logs of the respective device against the specific Indicators such as malicious known Attacker IP addresses/ C2 servers (IP address, domain) to identify internal systems. Trace the connections to the internal IP address or end-user system as per the logged information.
    b. If the logs are not enabled in the perimeter devices, enable the same, and follow step (a) to identify the victim system.
    c. It is also possible that currently, malware may be inactive, not making any connection or has changed the C2 (IP or domains) over time. In such cases, further analysis is required to determine the compromised system.
III. If the organisation does not have perimeter devices, then perform as follows:
    a. Identify the broadband/modem from the provided IP address, user name, and timestamp.
    b. In many cases, broadband/modem uses dynamic IP addresses allocated by the ISPs. Identify the correct device based on the given IP address, user name and timestamp. The help of ISP may also be taken for correct modem identification.
    c. All the system(s) behind the broadband/modem must be investigated to identify the compromised system (s).

It should be noted that systems/devices so identified are often just a subset of compromised systems. As the incident analysis on these systems is carried out, additional indicators and information gathered would lead to the identification of additional compromised systems and/or Indicators of Compromise.

Step 2: Isolate the compromised system(s) and contain the damage

Take the following steps to ensure the isolation of the identified compromised system(s) and contain further compromise:

I. Disconnect the affected system(s) from the network. This can help prevent the lateral movement of the attacker to other parts of the network and minimise further damage.
II. Preserve evidence – Do not shut down, format or tamper with evidence and ensure evidence collection as per Step 3.
III. Identify and block the suspected IPs and domains on the network perimeter (Firewall, IPS/IDS etc.)

Step 3: Collect Evidence

Once the systems suspected to be compromised are identified, collecting the necessary evidence for detailed analysis is essential. The evidence shall be stored on separate storage media such as external USB hard drives. Sufficient storage media of appropriate capacities must be arranged beforehand. The order, as well as how the evidence is to be captured, is also critical.

The following procedure may be referred to while collecting evidence:

I. If the system is Switched on and running:
    a. First capture the volatile memory of the live system. Tools such as FTK Imager, Belkasoft Live RAM Capturer etc., may be used for this purpose. (https://www.exterro.com/ftk-imager). Steps to create and capture the memory dump of the Windows system are given in **Annexure I.**
    b. If a hardware imaging facility is available, then power down the systems in **Step I** above and create forensic images of all the hard drives using hardware imaging tools.
    c. If a hardware imaging facility is unavailable, the forensic image may be created by using tools such as the FTK imager after **Step I**. Steps to create the forensic image using FTK are given in **Annexure I.**
II. In case the system is already in a powered-down state:
    a. Then, forensic Disk Imaging may be performed first as per **Step I (b &c)** above, and subsequently, the volatile evidence may be captured by powering on the system normally.
III. After evidence collection, systems should be turned off and untouched until the investigation is complete.
IV. If any systems are critical for operational continuance, alternate/backup systems must be built and used as a replacement.
V. Apart from the forensic evidence above, other network artefacts such as firewall logs, proxy logs, VPN logs, Emails etc., must also be extracted and preserved. When exporting any logs, “raw format” should be preferred.

Step 4: Ensure System Hardening for the remaining system(s) in the network

I. Ensure the systems and servers have the latest Operating system.
II. Ensure that the endpoint protection (Antivirus (AV), EDR, XDR etc.) is installed and up-to-date. If no 3rd party anti-virus solution is being used and Windows Defender is available by default, the 'Ransomware Protection' feature can be enabled, and drives/folders containing personal documents can be added to the 'Protected Folder' list.
III. Enforce a strong password policy and enforce periodic password changes.
IV. Implement multifactor authentication (MFA) wherever possible, especially for VPN and privileged users.
V. Perform user access review and ensure only legitimate users have access to the IT resources.
VI. Close FTP, SSH, SMB, RDP and other ports if not used. If any of these are to be used, then ensure appropriate security measures are in place (such as IP White Listing, MFA etc.)
VII. Monitor the IN and OUT traffic volume for early detection of any exfiltration of the sensitive data.
VIII. Monitor any kind of new account creation and privilege escalation use cases.
IX. Ensure that the latest patches are deployed on all systems.
X. Limit or eliminate the use of shared or group accounts.
XI. Prefer Disabling USB. Exercise caution when using removable media (e.g. USB thumb drives, external drives, CDs, etc.)
XII. Ensure no unknown plugins are installed on the browsers.
XIII. Apply software Restriction policies appropriately. Disable running executables from unconventional paths.
XIV. File extension viewing should be enabled to identify the true extension of the file so that inadvertently malicious file impersonation by means of the file/folder icon is not executed. Steps: This PC/My Computer > View > Check on 'File name extension'.

Step 5: Analyse collected artefacts:

I. After the evidence collection, analysis of the artefacts shall be carried out to determine the scope of the compromise, gather additional actionable information and determine the root cause of the incident.
II. Care must be taken to ensure that the evidence is not modified during analysis. Ideally, the original evidence shall be kept aside, and copies of evidence should be created and used for analysis.
III. In addition to the identification of the compromised system, the analysis should also focus on the identification of additional indicators, artefacts such as any unknown C2 IP Addresses/ domain names, malware samples, spear phishing emails, vulnerabilities exploited, attacker motive etc., to ascertain the root cause of the attack.
IV. If any additional compromised systems or indicators are identified during the analysis, the procedure (points 1 to 3) should be repeated for all such systems.
V. The organisation should also asses the business, operational, and data impact due to this incident.
VI. Note that assessment and analysis of all these are necessary to take corrective action, mitigate, and prevent future recurrences.

Step 6: Remediation and Clean-up:

I. After completion of the analysis, affected systems should be rebuilt and restored from a clean backup. The infected system may also be cleaned.

II. It is also important to identify any shortcomings in terms of protective measures at the technological, policy or process level which could have prevented/detected the attack, such as MFA, vulnerability management process, patch management, SOC etc., and those measures may be implemented on priority.

Finally, the analysis report and all collected evidence should be shared with CERT-In.

Annexure I: Procedure to make memory dump and forensic image

Steps to take memory dump using FTK Imager:

1. File> Capture Memory.
2. Select the Destination path (select the machine's local drive or any external hard drive as the destination).
3. Set the destination file name as “Computer_Name.mem”. Here “Computer_Name” is the computer name of the victim system.
4. Start “capture memory”.

Steps for taking a forensic image using FTK Imager:

1. File>Create Disk Image.
2. Choose 'Physical Drive'
3. Select Source Drive and Finish (select the machine's hard drive (as source)).
4. Add Image Destination.
5. Select DD/EO1 File.
6. Fill in the evidence item information.
7. Browse the device to store DD/EO1 File [this is the external hard drive folder].
8. Name the image without extension.
9. Start.