certin
Enhancing Cyber Security in India

Indian Computer Emergency Response Team
Ministry of Electronics and Information Technology
Government of India
सत्यमेव जयते

CERT-In Advisory CIAD-2022-0023

Responding to Ransomware Attacks

Original Issue Date: September 27, 2022

Description

Ransomware is a category of malware that gains access to systems and makes them unusable to its legitimate users, either by encrypting different files on targeted systems or locking the system's screen unless a ransom is paid. The ransomware problem has become multi-dimensional, with grave consequences for the victims.

The following measures are recommended when it is detected that an organisation has suffered or is under a Ransomware attack.

Identify & Isolate

1. Identify systems or subnets which are affected or appear to be impacted.

2. Isolate the identified systems or subnets from the network at the switch level, as during an incident, isolating individual systems from the network may not be feasible.

3. If it is not feasible to isolate the systems at the switch /network level, isolate affected devices by making them offline (such as unplugging the network cables or turning off their Wi-Fi connectivity)

4. Unplug all external storage: memory sticks, attached phones/cameras, external hard drives, USB drives

5. Turn off any wireless functionality: Wi-Fi, Bluetooth, NFC etc.

Contain

1. Identify and secure critical systems (Network Shares, File Servers, Databases etc.) by temporarily restricting their access and isolating them from the network as an interim measure.

2. Secure network backups by taking them offline immediately.

3. Temporarily disable all remote access to the network (VPN, RDP, Remote access tools, SSH etc.)

4. Identify and eliminate sources of threats that may be in many forms and disrupt threat actor activities. Some examples are given below.

    a) Identify and block the suspected IPs and domains on the network perimeter.

    b) Identify and terminate malicious processes and stop the malicious files, scripts, scheduled tasks, etc., from being executed.

Hardening

1. Reset credentials of all the privileged local, VPN and domain accounts (especially for administrator and other system accounts).

2. Implement multi-factor authentication (MFA) wherever possible, especially for VPN accounts and privileged users.

3. Perform user access review and ensure only legitimate users have access to applications or infrastructure.

4. Close SMB and RDP ports as an immediate measure.

5. Close other unused ports in the network.

6. Force domain users to change the credentials on the next login.

7. Ensure that the latest patches are deployed on all systems (prioritising targeted systems, Operating Systems, other system software, etc.).

8. Deploy custom signatures to endpoint protection and network security tools based on discovered Indicators of compromises (IOCs) specific to the incident.

9. Ensure that the endpoint protection (AV, EDR, XDR etc.) is up-to-date and enabled on all systems.

Preserve Artefacts & Sanitise Systems

1. Record basic information like "Ransomware Note" text or image, encrypted file extensions, samples of encrypted files, etc.

2. Obtain Forensic image and memory capture of a sample of affected devices for further analysis.

3. Collect relevant logs (Firewall, IPS, IDS, Proxy, Server Access logs, etc.), malware binaries, and other observable IOCs (suspected command and control IP addresses, registry entries, files, etc.).

4. Backup of the infected systems may be kept so that in case a decryptor is available in future; the encrypted files could be decrypted.

5. Use updated endpoint protection solutions (AV, EDR, XDR, etc.) to sanitise systems. Systems should be connected to the network only after ensuring they are infection free.

Securely Recover & Resume

1. To securely recover from a ransomware attack, it is essential to ensure that the previous vulnerabilities and threats are eliminated and the systems are hardened.

2. Affected systems may be recovered by:-

   a) Restoring from a secure backup (verified to be infection free).

   b) Restoring from a previous secure restore point (verified to be infection free).

   c) Rebuilding and reinstalling from scratch (if a secure backup or restore point is unavailable).

3. When secure backups and restore points are not available, and rebuilding of the systems from scratch is decided, backups of critical system data should be taken so that in case a decryptor is available in future, it could be decrypted.

4. Also, after restoration, scan with updated endpoint protection solutions (AV, EDR, XDR, etc.) to ensure no residual infections like backdoors, trojans etc., are present.

5. Review firewall configurations to ensure that the rules are valid.

6. Implement proper network segmentation to ensure isolation of various systems, segments and zones.

Monitor

1. Test each system, application and other components and verify that there are no deviations from normal operations.

2. If a Security Information and Event Management (SIEM) solution is available, monitor the alerts from the SIEM solution.

3. Periodically analyse relevant logs (Antivirus logs and alerts, Firewall, IPS, IDS, access logs, event logs etc.) and check for abnormal system behaviour.

4. Before fully resuming the systems to their pre-incident level, systems should be thoroughly tested to ensure that they are functioning correctly and that the cyber threat has been neutralised.

References

https://www.csk.gov.in/documents/RANSOMWARE_Report_Final.pdf
https://www.csk.gov.in/alerts/ransomware.html

Disclaimer

The information provided herein is on "as is" basis, without warranty of any kind.

Contact Information

Email: info@cert-in.org.in
Phone: +91-11-24368572

Postal address

Indian Computer Emergency Response Team (CERT-In)
Ministry of Electronics and Information Technology
Government of India
Electronics Niketan
6, CGO Complex, Lodhi Road,
New Delhi - 110 003
India