DSCI
PROMOTING DATA PROTECTION
A nasscom Initiative

DSCI THREAT INTELLIGENCE AND RESEARCH INITIATIVE

THREAT ADVISORY

OCTOBER 2024

STANDARD OPERATING PROCEDURE (SOP) FOR RANSOMWARE INCIDENT RESPONSE

Standard Operating Procedure (SOP) for Ransomware Incident Response

Purpose

This SOP defines the technical and procedural steps for responding to ransomware incidents to minimize impact, ensure recovery, and document the response process.

Scope

This SOP applies to all IT and security personnel involved in the management and response to ransomware incidents within the organization.

Definitions

- **Ransomware**: A form of malicious software designed to encrypt files or lock systems, demanding a ransom for decryption.
- **Incident**: Any event or series of events that disrupts confidentiality, integrity and availability of systems, network or data caused by malicious action.

Roles and Responsibilities

- **Incident Response Team (IRT)**: Responsible for managing and mitigating ransomware incidents.
    - **Incident Commander**: Oversees incident response, coordinates between teams, and makes strategic decisions.
    - **Technical Lead**: Handles technical response, including detection, containment, eradication, and recovery.
    - **Communications Lead**: Manages internal and external communications and ensures proper documentation.
    - **Legal Advisor**: Provides guidance on legal and compliance issues, including lodging complaint to law enforcement agencies and reporting obligations.
    - **IT Support**: Assists with the technical recovery process and system restoration.

Incident Response Procedure

➢ **Identification and Reporting**

1. **Detection**: Monitor for indicators of ransomware, such as:
    - Unusual file encryption or extensions.

- Presence of ransom notes or pop-up messages.
- Determine the ransomware strain.
- Unexplained network traffic or system behaviour.
- Identify systems affected and subnets appear to be impacted.
- Identify and isolate critical systems (e.g., file servers, databases) by restricting access temporarily.
- Do not shut down the affected machine. Instead, isolate the identified systems or subnets at the switch level.

Note: *Avoid negotiating or paying the ransom, as it may encourage further attacks and does not guarantee recovery.*

2. **Notification**: Report the incident to regulatory authorities immediately via established communication channels. Provide:
    - Details of Affected systems and files.
    - Observed symptoms, IOCs and timeline of events.

➢ **<u>Containment</u>**

1. **Isolate Affected Systems**:
    - Disconnect infected systems from the network to prevent further spread.
    - Disable network shares and mapped drives.
    - Temporarily disable all remote access to the network (VPN, RDP, SSH, etc.)
    - Block suspected IPs and domains at the network perimeter level.
    - Terminate malicious processes and prevent the execution of malicious files, scripts, and scheduled tasks.
2. **Preserve Evidence**:
    - Take forensic images (Disk and RAM) of affected systems to capture the state before remediation.
    - Preserve artefacts and relevant logs (firewall, IPS/IDS, proxy, server access) with malware binaries, suspected C2 IPs, registry entries, and files.
    - Document all observed indicators of compromise (IOCs) and actions taken.

- **<u>Eradication</u>**

1. **Identify Ransomware IoCs and IoAs**:

   Leverage threat intelligence and forensic analysis to identify the ransomware strain and attack indicators.

2. **Remove Malware**:
   - Employ updated antivirus and anti-malware tools to clean affected systems.
   - Ingest custom signatures into endpoint protection tools (AV, EDR, XDR, etc.) based on the IOCs and IOAs identified during artifact analysis.
   - Manually check for and remove any remaining ransomware components.

3. **Reset Credentials:**
   - Reset credentials for all privileged local, VPN and domain accounts.
   - Change the "krbtgt" account to invalidate the Golden ticket if a domain controller (DC) is suspected to be compromised.
   - Implement multi-factor authentication (MFA) for VPN accounts and privileged users.
4. **Patch Vulnerabilities and Hardening**:
   - Identify and patch vulnerabilities of public facing applications.
   - Disable internet-facing systems, services, and ports you don't need (3389,445, 135, 139, 22, 21)
   - Restrict the use of legitimate tools commonly used by attackers (Psexec, PingEasy, PS, winrm etc.)
   - Whitelist applications to ensure that only authorised software can run

Note: *Ensure systems are thoroughly checked and confirmed infection-free before connecting to the network.*

- **<u>Recovery</u>**

1. **Restore Systems**:
   - Use clean backups to restore affected systems and data.
   - Verify the integrity of backups before restoration.
2. **Rebuild Systems**:

- If backups are not available or compromised, consider reinstalling operating systems and applications from scratch.

3. **Verify Systems**:
   - Conduct thorough testing to ensure systems are free of ransomware and functioning correctly.
   - Monitor systems for any signs of residual threats or anomalies.

Note: *Keep a backup of the infected systems to enable future decryption if a suitable decryptor becomes available.*

➢ **<u>Documentation</u>**

1. **Incident Report**: Create a detailed report documenting the incident, including:
   - Timeline of events.
   - Actions taken.
   - Impact assessment.
   - Lessons learned.

2. **Post-Incident Review**:
   1. Conduct a review meeting to evaluate the response effectiveness and identify improvement areas.
   2. Update incident response plans and preventive measures based on findings.

➢ **<u>Communication</u>**

1. **Internal Communication**:
   - Provide updates to employees about the incident status, impact, and any required actions.
2. **External Communication**:
   - Notify customers, partners, and regulatory bodies as required by law and contractual obligations.
3. **Public Relations**:
   - Manage public relations and media inquiries in coordination with the Communications Lead.

Ransomware Preventive Measures

1. **Network Segmentation**: Implement network segmentation to limit the spread of ransomware across different network zones.
2. **Endpoint Protection**: Deploy advanced endpoint protection solutions with real-time threat detection and automatic response capabilities.
3. **Threat intelligence**: Implement threat intelligence feeds that include known indicators of compromise (IOCs) associated with different ransomware families.
4. **Email Filtering**: Use email filtering solutions to block malicious attachments and phishing emails.
5. **Regular Backups**: Perform regular backups of critical systems and data, storing them securely offsite. Follow the 3-2-1 backup rule that recommends keeping three copies on two different media types, with one copy stored off-site.
6. **Patch Management**: Ensure all software and systems are up-to-date with the latest security patches and updates.
7. **User Training**: Conduct regular security awareness training to educate employees about recognizing and responding to phishing attempts and other threats.
8. **Simulated Drills:** Conduct simulated ransomware attacks to test response readiness and identify gaps.
9. **Access Controls**: Implement least privilege access controls and regularly review and update user permissions.
10. **Monitoring**: Ensure 24/7 security operations monitor for anomalies and remediate threats before they escalate into a cyber crisis.
    - Monitor for processes that create or modify a large number of files within a short timeframe, especially with unusual file extensions.
    - Look for abnormal file access patterns, such as large-scale file renaming or encryption, which are indicative of ransomware.
    - Alert on the use of administrative tools (e.g., PowerShell, PsExec) in an unusual manner, particularly if they are being used to move laterally or encrypt files.
    - Detect spikes in file creation, modification, or deletion events, especially if occurring in user directories or sensitive folders.
    - Identify and alert on the execution of processes associated with known ransomware families.

- Watch for unusual outbound traffic, such as connections to known command and control (C2) servers or abnormal network activity patterns.
- Monitor for registry changes related to ransomware behaviors, such as those modifying autorun settings or file associations.
- Track and alert on unusual user behavior such as accessing or modifying files that are not typically interacted with by the users.
- Detect unusual command-line activities, such as the use of known ransomware tools or scripts.

References

- https://www.csk.gov.in/alerts/ransomware.html
- https://www.nomoreransom.org/en/decryption-tools.html

DSCI
PROMOTING DATA PROTECTION
A nasscom Initiative

ABOUT DSCI

Data Security Council of India (DSCI) is a not-for-profit, industry body on data protection in India, set up by Nasscom, committed to making cyberspace safe, secure, and trusted by establishing best practices, standards and initiatives in cybersecurity and privacy. DSCI works together with the Government and their agencies, law enforcement agencies, industry sectors including IT-BPM, BFSI, Telecom, industry associations, data protection authorities and think tanks for public advocacy, thought leadership, capacity building and outreach initiatives.

SCAN THE QR CODE FOR MORE UPDATES

Data Security Council of India
4th Floor, Nasscom Campus, Plot No. 7-10, Sector 126, Noida, UP-201303

data-security-council-of-india/ DSCI_Connect dsci.connect

dsci.connect dscivideo security chips

All Rights Reserved © DSCI 2024