Ransomware and Data Extortion Response Checklist

Should your organization be a victim of ransomware, follow your approved IRP. The authoring organizations strongly recommend responding by using the following checklist. Be sure to move through the **first three steps in sequence.**

The authoring organizations do not recommend paying ransom. Paying ransom will not ensure your data is decrypted, that your systems or data will no longer be compromised, or that your data will not be leaked.

Additionally, paying ransoms may pose sanctions risks. For information on potential sanctions risks, see U.S. Department of the Treasury Office of Foreign Assets Control (OFAC) memorandum from September 2021, Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments. The updated advisory states that Treasury's Office of Foreign Assets Control (OFAC) would consider 'mitigating factors' in related enforcement actions. Contact your local FBI field office, in consultation with OFAC, for guidance on mitigating penalty factors after an attack.

Detection and Analysis

Refer to the best practices and references below to help manage the risk posed by ransomware and support your organization's coordinated and efficient response to a ransomware incident. Apply these practices to the greatest extent possible based on availability of organizational resources.

- ☐ **1. Determine which systems were impacted, and immediately isolate them.**
  - ☐ If several systems or subnets appear impacted, take the network offline at the switch level. It may not be feasible to disconnect individual systems during an incident.
  - ☐ Prioritize isolating critical systems that are essential to daily operations.
  - ☐ If taking the network temporarily offline is not immediately possible, locate the network cable (e.g., ethernet) and unplug affected devices from the network or remove them from Wi-Fi to contain the infection.
  - ☐ For cloud resources, take a snapshot of volumes to get a point in time copy for reviewing later for forensic investigation.
  - ☐ After an initial compromise, malicious actors may monitor your organization's activity or communications to understand if their actions have been detected. Isolate systems in a coordinated manner and use out-of-band communication methods such as phone calls to avoid tipping off actors that they have been discovered and that mitigation actions are being undertaken. Not doing so could cause actors to move laterally to preserve their access or deploy ransomware widely prior to networks being taken offline.

- ☐ **2. Power down devices if you are unable to disconnect them from the network to avoid further spread of the ransomware infection.**

  Note: This step will prevent your organization from maintaining ransomware infection artifacts and potential evidence stored in volatile memory. **It should be carried out only if it is not possible to temporarily shut down the network or disconnect affected hosts from the network** using other means.

☐ **3. Triage impacted systems for restoration and recovery.**

- ☐ Identify and prioritize critical systems for restoration on a clean network and confirm the nature of data housed on impacted systems.
    - Prioritize restoration and recovery based on a predefined critical asset list that includes information systems critical for health and safety, revenue generation, or other critical services, as well as systems they depend on.
- ☐ Keep track of systems and devices that are not perceived to be impacted so they can be deprioritized for restoration and recovery. This enables your organization to get back to business in a more efficient manner.

☐ **4. Examine existing organizational detection or prevention systems (e.g., antivirus, EDR, IDS, Intrusion Prevention System) and logs.** Doing so can highlight evidence of additional systems or malware involved in earlier stages of the attack.

- ☐ Look for evidence of precursor "dropper" malware, such as Bumblebee, Dridex, Emotet, QakBot, or Anchor. A ransomware event may be evidence of a previous, unresolved network compromise.
    - Operators of these advanced malware variants will often sell access to a network. Malicious actors will sometimes use this access to exfiltrate data and then threaten to release the data publicly before ransoming the network to further extort the victim and pressure them into paying.
    - Malicious actors often drop ransomware variants to obscure post-compromise activity. Care must be taken to identify such dropper malware before rebuilding from backups to prevent continuing compromises.

☐ **5. Confer with your team to develop and document an initial understanding of what has occurred based on initial analysis.**

☐ **6. Initiate threat hunting activities.**

- ☐ For enterprise environments, check for:
    - Newly created AD accounts or accounts with escalated privileges and recent activity related to privileged accounts such as Domain Admins.
    - Anomalous VPN device logins or other suspicious logins.
    - Endpoint modifications that may impair backups, shadow copy, disk journaling, or boot configurations. Look for anomalous usage of built-in Windows tools such as `bcdedit.exe`, `fsutil.exe` (deletejournal), `vssadmin.exe`, `wbadmin.exe`, and `wmic.exe` (shadowcopy or shadowstorage). Misuse of these tools is a common ransomware technique to inhibit system recovery.
    - Signs of the presence of Cobalt Strike beacon/client. Cobalt Strike is a commercial penetration testing software suite. Malicious actors often name Cobalt Strike Windows processes with the same names as legitimate Windows processes to obfuscate their presence and complicate investigations.

- Signs of any unexpected usage of remote monitoring and management (RMM) software (including portable executables that are not installed). RMM software is commonly used by malicious actors to maintain persistence.
- Any unexpected PowerShell execution or use of PsTools suite.
- Signs of enumeration of AD and/or LSASS credentials being dumped (e.g., Mimikatz, `Sysinternals ProcDump`, or `NTDSutil.exe`).
- Signs of unexpected endpoint-to-endpoint (including servers) communications, for example, Address Resolution Protocol (ARP) poisoning of an endpoint or command and control traffic relayed between endpoints.
- Potential signs of data being exfiltrated from the network, which may include:
    - Abnormal amount of data outgoing over any port. Open source software can tunnel data over various ports and protocols. For example, ransomware actors have used Chisel to tunnel Secure Shell (SSH) over HTTPS port `443`. Ransomware actors have also used Cloudflared to abuse Cloudflare tunnels to tunnel communications over HTTPS.
    - Presence of Rclone, Rsync, and various web-based file storage services, and FTP/SFTP, which are common tools for data exfiltration (and also used by threat actors to implant malware/tools on affected networks.)
- Newly created services, unexpected scheduled tasks, unexpected software installed, unusual files created, legitimate processes with unexpected child processes, etc.

☐ For cloud environments:

- Enable tools to detect and prevent modifications to IAM, network security, and data protection resources.
- Use automation to detect common issues (e.g., disabling features, introduction of new firewall rules) and take automated actions as soon as they occur. For example, if a new firewall rule is created that allows open traffic (`0.0.0.0/0`), an automated action can be taken to disable or delete this rule and send notifications to the user that created it as well as the security team for awareness. This will help avoid alert fatigue and allow security personnel to focus on critical issues.

Reporting and Notification

Note: Refer to the Contact Information section at the end of this guide for details on how to report and notify about ransomware incidents.

- ☐ **7.** Follow notification requirements as outlined in your cyber incident response and communications plan to **engage internal and external teams and stakeholders** with an understanding of what they can provide to help you mitigate, respond to, and recover from the incident.
  - ☐ Share the information you have at your disposal to receive timely and relevant assistance. Keep management and senior leaders informed via regular updates as the situation develops. Relevant stakeholders may include your IT department, managed security service providers, cyber insurance company, and departmental or elected leaders [CPG 4.A].
  - ☐ Report the incident to—and consider requesting assistance from—CISA, your local FBI field office, the FBI Internet Crime Complaint Center (IC3), or your local U.S. Secret Service field office.
  - ☐ As appropriate, coordinate with communications and public information personnel to ensure accurate information is shared internally with your organization and externally with the public

If extended identification or analysis is needed, CISA, MS-ISAC and local, state, or federal law enforcement may be interested in any of the following information that your organization determines it can legally share:

- Recovered executable file.
- Copies of the readme file – DO NOT REMOVE the file or decryption may not be possible.
- Live memory (RAM) capture from systems with additional signs of compromise (use of exploit toolkits, RDP activity, additional files found locally).
- Images of infected systems with additional signs of compromise (use of exploit toolkits, RDP activity, additional files found locally).
- Malware samples.
- Names of malware identified on your network.
- Encrypted file samples.
- Log files (e.g., Windows event logs from compromised systems, firewall logs).
- PowerShell scripts found having executed on the network.
- User accounts created in AD or machines added to the network during the exploitation.
- Email addresses used by the attackers and any associated phishing emails.
- Other communication accounts used by the attackers.
- A copy of the ransom note.
- Ransom amount and if the ransom was paid.
- Bitcoin wallets used by the attackers.
- Bitcoin wallets used to pay the ransom, if applicable.
- Copies of any communications with attackers.

- ☐ **8.** If the incident resulted in a data breach, **follow notification requirements as outlined in your cyber incident response and communications plans.**

Containment and Eradication

If no initial mitigation actions appear possible:

- ☐ **9. Take a system image and memory capture of a sample of affected devices (e.g., workstations, servers, virtual servers, and cloud servers).** Collect any relevant logs as well as samples of any "precursor" malware binaries and associated observables or indicators of compromise (e.g., suspected command and control IP addresses, suspicious registry entries, or other relevant files detected). The contacts below may be able to assist you in performing these tasks.
  - ☐ Preserve evidence that is highly volatile in nature—or limited in retention—to prevent loss or tampering (e.g., system memory, Windows Security logs, data in firewall log buffers).

Upon voluntary request, CISA and MS-ISAC (for SLTT organizations) can assist with analysis of phishing emails, storage media, logs, and/or malware at no cost to help organizations understand the root cause of an incident.

- CISA – Advanced Malware Analysis Center: malware.us-cert.gov/
- MS-ISAC – Malicious Code Analysis Platform (SLTT organizations only): cisecurity.org/spotlight/cybersecurity-spotlight-malware-analysis/

- ☐ **10. Consult federal law enforcement, even if mitigation actions are possible, regarding possible decryptors available,** as security researchers may have discovered encryption flaws for some ransomware variants and released decryption or other types of tools.

To continue taking steps to contain and mitigate the incident:

- ☐ **11. Research trusted guidance** (e.g., published by sources such as the U.S. Government, MS-ISAC, or a reputable security vendor) for the particular ransomware variant and follow any additional recommended steps to identify and contain systems or networks that are confirmed to be impacted.
  - ☐ Kill or disable the execution of known ransomware binaries; this will minimize damage and impact to your systems. Delete other known associated registry values and files.

- ☐ **12. Identify the systems and accounts involved in the initial breach.** This can include email accounts.

- ☐ **13.** Based on the breach or compromise details determined above, **contain associated systems that may be used for further or continued unauthorized access.** Breaches often involve mass credential exfiltration. Securing networks and other information sources from continued credential-based unauthorized access may include:
  - ☐ Disable virtual private networks, remote access servers, single sign-on resources, and cloud-based or other public-facing assets.

☐ **14.** If server-side data is being encrypted by an infected workstation, **follow server-side data encryption quick identification steps.**
- ☐ Review Computer Management > Sessions and Open Files lists on associated servers to determine the user or system accessing those files.
- ☐ Review file properties of encrypted files or ransom notes to identify specific users that may be associated with file ownership.
- ☐ Review the `TerminalServices-RemoteConnectionManager` event log to check for successful RDP network connections.
- ☐ Review the Windows Security log, SMB event logs, and related logs that may identify significant authentication or access events.
- ☐ Run packet capture software, such as Wireshark, on the impacted server with a filter to identify IP addresses involved in actively writing or renaming files (e.g., `smb2.filename contains cryptxxx`).

☐ **15. Conduct extended analysis to identify outside-in and inside-out persistence mechanisms.**
- ☐ Outside-in persistence may include authenticated access to external systems via rogue accounts, backdoors on perimeter systems, exploitation of external vulnerabilities, etc.
- ☐ Inside-out persistence may include malware implants on the internal network or a variety of living-off-the-land style modifications (e.g., use of commercial penetration testing tools like Cobalt Strike; use of PsTools suite, including PsExec, to remotely install and control malware and gather information regarding—or perform remote management of—Windows systems; use of PowerShell scripts).
- ☐ Identification may involve deployment of EDR solutions, audits of local and domain accounts, examination of data found in centralized logging systems, or deeper forensic analysis of specific systems once movement within the environment has been mapped out.

☐ **16. Rebuild systems based on prioritization of critical services** (e.g., health and safety or revenue-generating services), using pre-configured standard images, if possible. Use infrastructure as code templates to rebuild cloud resources.

☐ **17. Issue password resets for all affected systems and address any associated vulnerabilities and gaps in security or visibility** once the environment has been fully cleaned and rebuilt, including any associated impacted accounts and the removal or remediation of malicious persistence mechanisms. This can include applying patches, upgrading software, and taking other security precautions not previously taken. Update customer-managed encryption keys as needed.

☐ **18. The designated IT or IT security authority declares the ransomware incident over** based on established criteria, which may include taking the steps above or seeking outside assistance**.**

Recovery and Post-Incident Activity

- ☐ **19. Reconnect systems and restore data from offline, encrypted backups based on a prioritization of critical services.**
    - □ Take care not to re-infect clean systems during recovery. For example, if a new Virtual Local Area Network (VLAN) has been created for recovery purposes, ensure only clean systems are added.

- ☐ **20. Document lessons learned from the incident and associated response activities** to inform updates to—and refine—organizational policies, plans, and procedures and guide future exercises of the same.

- ☐ **21. Consider sharing lessons learned and relevant indicators of compromise with CISA or your sector ISAC** to benefit others within the community.

DISCLAIMER OF ENDORSEMENT

The information and opinions contained in this document are provided "as is" and without any warranties or guarantees. Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by the United States Government, and this guidance shall not be used for advertising or product endorsement purposes.

PURPOSE

This document was developed in furtherance of the authors' cybersecurity missions, including their responsibilities to identify and disseminate threats, and to develop and issue cybersecurity specifications and mitigations. This information may be shared broadly to reach all appropriate stakeholders.

America's Cyber Defense Agency

NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

Full CISA documentation:
https://www.cisa.gov/resources-tools/resources/stopransomware-guide