[COMPANY LOGO]

RANSOMWARE RESPONSE PLAYBOOK

[COMPANY NAME]

Document Objectives:

The playbook is to be used by the cyber incident response team. It focuses on helping them prioritize their actions and engage the right people during a confirmed ransomware incident during the initial analysis & containment, detailed analysis, eradication, and recovery phases.

Document Properties:

Version:	[VERSION]
Last Revised Date:	[DATE]
Confidentiality Level:	[CONFIDENTIALITY]
Document Owner	[OWNER]
Publication Date:	[DATE]

Table of Contents:

1. Overview

Unlike other security incidents, ransomware puts organizations on a countdown. Decisions must be made swiftly; any delay in the decision-making process could result in public disclosure or complete loss of data.

The playbook is to be used by the cyber incident response team. It focuses on helping them prioritize their actions and engage the right people during a confirmed ransomware incident during the initial analysis & containment, detailed analysis, eradication, and recovery phases. The audience for these playbooks is the Cybersecurity Incident Response Team (CSIRT), therefore playbook steps may be technical. Additionally, the playbook may reference responsibilities of other teams, but only informationally. The focus of the steps of the playbook is the investigation piece by the CSIRT.

The playbook shall be reviewed and updated as needed. This is necessary to address:

- Changes to regulatory requirements
- Industry standards
- Changes to malware/ransomware trends
- Lessons learned via exercises and/or actual events

This playbook becomes activated when a ransomware incident is detected. Initial triage is performed to understand the timing and whether this is a current threat. If triage shows that the alerts are from old, archived files surfacing due to file backup or share access or some other activity determined to be a false positive, then no further escalation through the playbook is required.

2. Ransomware Response Process

2.1 Detection

The initial detection will most often come from one of the following:

- **Analysis efforts in a previous cybersecurity incident.**
- **Automated detection systems:** [EDR], [SIEM], [EMAIL SECURITY SOLUTION], and [FIREWALL].
- **Findings during threat hunting:** [EDR], [SIEM], and [FIREWALL].
- **Managed security service providers:** [MSSP/MDR] and [EDR].
- **Reporting:** User, partner, provider, or third-party.

Decision to Stand Up Cyber Incident Response Team (CSIRT)

Following the initial detection and confirmation of ransomware activities the severity should be determined following the criteria specified in the Incident Response Playbook.

If the determination is made that the incident has a “Low” or “Medium” level of severity, then the internal Standard Operating Procedures can be followed to remediate the incident without activation of the Incident Response team.

If the severity has been determined to be “High” or “Critical” the incident response team must be activated as quickly as possible. That process is detailed in the Incident Response Playbook.

2.2 Initial Analysis and Containment

First Pass Analysis

The primary objective of the first pass is to quickly identify the scope of the impacted resources requiring containment. While other activities like root-cause analysis are critical components of the response process, the priority is to limit the spread of the ransomware.

The ransomware process tree can be examined on one of the impacted hosts in [EDR]. The most obvious indicators of compromise should be immediately pulled out and used to identify additional affected hosts.

Identify Affected Hosts

A list of impacted hosts can be generated based on the IOCs collected during the first pass in [EDR] and [SIEM]. Detailed in: [EDR] IOC-based Hunting [LINK TO TECHNOLOGY-SPECIFIC PLAYBOOK] and [SIEM] IOC-based Hunting [LINK TO TECHNOLOGY-SPECIFIC PLAYBOOK].

Contain Affected Hosts

Hosts can be individually contained via the [EDR] platform. Detailed in: Host Containment [LINK TO TECHNOLOGY-SPECIFIC PLAYBOOK].

Additionally, containing hosts one-by-one may notify the attackers that they have been detected. An automated workflow can be created in [SOAR] to automate the containment of impacted systems if the malicious activities are widespread. Detailed in: Creating Workflows [LINK TO TECHNOLOGY-SPECIFIC PLAYBOOK]. Utilize the indicators of compromise identified in the first pass analysis as a trigger for the automated containment workflow in [SOAR].

Custom indicators of attack (IOAs) and custom indicators of compromise (IOCs) can also be leveraged in [EDR] to proactively prevent machines from being infected. If the mechanism for encryption is identified during the first pass analysis, then a custom IOA/IOC can be added with an action of “block execution” to prevent the encryption mechanism from running. Detailed in Adding Custom Indicators [LINK TO TECHNOLOGY-SPECIFIC PLAYBOOK].

In cases where the impacted systems are not running the [EDR] sensor, it may be necessary to segment parts of the network to contain the spread of malware or to prevent malicious egress altogether. Network containment is available at the node, VLAN, switch, or site levels. This activity requires a network change request in [ITSM], but the change can proceed prior to [ITSM] approval in emergency circumstances with approval from the incident manager. Network containments to the LAN can be performed by the network management SMEs.

If systems are not able to be contained at the host or network levels, it may be required to physically unplug the networking cables or power down the impacted systems. This is reserved as a last-resort method because powering down systems can result in the loss of volatile forensic data.

Disable Impacted User/Host Credentials

Once the ransomware activities have been sufficiently contained, it is critical that impacted user/host credentials be disabled. This can be accomplished by creating a [ITSM] request and messaging the relevant account management SME directly:

- Active Directory – [SME]
- Entra ID – [SME]
- [IAM SOLUTION] – [SME]

Engage IR Retainer, as Necessary

An IR Retainer is available through a third party: [IR COMPANY NAME] to provide outside expertise and advisory services.

Hotline: [PHONE]

[Contact #1]: [PHONE] ext. 123 - [EMAIL]

[Contact #2]: [PHONE] ext. 123 - [EMAIL]

2.3 Analysis

Preserve Evidence

Ideally, it will not be required to power down systems during the initial containment efforts. All volatile evidence should still be accessible. Storage constraints may limit the ability to capture complete memory dumps of all the impacted systems.

Various tools can be leveraged to capture full memory dumps. Detailed in: Capturing Memory [LINK TO TOOL-SPECIFIC PLAYBOOK].

When possible, a full disk image capture of the impacted systems is ideal. It is sometimes more useful to capture this image while the host is still live as information on encrypted drives may not be accessible after it has been powered off. Depending on the scope of compromise, this process could require a centralized storage server with or portal external drives. Detailed in: Full Disk Capture [LINK TO TOOL-SPECIFIC PLAYBOOK].

A Velociraptor offline collector or Kroll Artifact Parser/Extractor can be pushed to the impacted machines via [DEPLOYMENT TECHNOLOGY] and utilized to acquire the most commonly useful forensic artifacts, without taking a complete image of the disk. Detailed in: Artifact Collection [LINK TO TECHNOLOGY-SPECIFIC PLAYBOOK]

Identify Ransomware Strain

The analysis and response process will vary depending on the strain of ransomware that has impacted the organization. The IOCs vary widely, but the threat intelligence platform in [EDR] can be utilized to

identify the ransomware strain based on the IOCs collected in the first pass analysis. Additional OSINT can be performed if no findings are available in [EDR]. Detailed in: Utilizing Threat Intelligence [LINK TO TECHNOLOGY-SPECIFIC PLAYBOOK].

Decryptors are freely available for many ransomware strains. Law enforcement and security companies operate a website (nomoreransom.org) which can identify an unknown strain of ransomware if it is provided a sampling of the IOCs. Once the strain is identified, many decryptors are available to download.

Gather Indicators of Compromise

Build on the list of IOCs composed in the first pass analysis. While the specific indicators will vary, generally the following can be used as IOCs in ransomware incidents:

- A readme file (ransom note)
- Exploit toolkits
- Precursor (dropper) malware
- RDP activity
- Malicious file hashes
- A mechanism of encryption
- The specific type of encryption used
- Uncommon log files/events
- PowerShell scripts
- Newly created user accounts
- Directory or machines added to the network during the exploitation
- Email addresses
- Phishing emails
- Bitcoin wallets used by the attackers
- IP addresses

Establish Infection Vector

It is critical to determine the initial infection vector during the analysis phase, so that it can be closed during the recovery phase. It can vary widely, but the most ransomware attack vectors are:

- Internet-facing vulnerabilities/misconfigurations
- Credential compromise
- Phishing
- A precursor (dropper) malware infection
- Third-party and managed service provider infection

Validate Data Backup Availability and Integrity

Backup integrity and availability can be confirmed with administrators depending on which systems were impacted. These backups may be required in the event that hosts need to be reimaged.

- **Windows Servers** – [SME]: [BACKUP UTILITY]

- **Linux Servers** – [SME]: [BACKUP UTILITY]
- **Workstations** – [SME]: [BACKUP UTILITY]
- **Cloud Instances** – [SME]: [BACKUP UTILITY]

Contact Law Enforcement

Consult federal law enforcement regarding possible decryptors available, as security researchers have already broken the encryption algorithms for some ransomware variants. Additionally, assistance can be provided in conducting a criminal investigation, which may involve collecting incident artifacts, to include system images and malware samples.

FBI Field Office – [LOCAL OFFICE CONTACT INFO]

Decision to Engage Cyber Insurance Carrier

If a decryptor was not available in the previous steps, then it may be necessary to contact the cyber insurance carrier to determine whether they will cover the cost of the ransom or recovery process.

[COMPANY] has cyber liability insurance through [PROVIDER NAME]. The CST can contact [POINT OF CONTACT] ([EMAIL ADDRESS]) for assistance in contacting the provider.

Data Exfiltration

If there was confirmed or suspected data exfiltration, refer to the data exfiltration playbook for remediation steps. Detailed in: Data Exfiltration Playbook**.**

Regulatory Notifications

It is likely that [COMPANY] will be legally required to notify individuals impacted by the ransomware attack of the breach. The notification requirements vary widely depending on the number of people impacted, whether data was exfiltrated, and sensitivity of the data. The CST is to include the legal team in incident notifications so they can best determine what notifications are required.

Decision to Pay Ransom

The decision to pay the ransom is ultimately made by management. The decision will be heavily reliant on whether a decryptor was available in the previous steps, the criticality of the impacted systems, and the level of coverage from the cyber insurance provider. The cost of paying the ransom will be weighed against personnel/resource costs of restoring/rebuilding systems and the potential for public data leaks.

2.4 Eradication

Add Indicator of Compromise (IOC) to Existing Threat Detection Platform

All indicators of compromise identified during the comprehensive analysis process should be added to

[SIEM], [EMAIL SECURITY SOLUTION], [EDR], [WAF], and the [FIREWALL] network firewalls to reduce the risk of reinfection. Follow the standard operating procedures for each technology. Detailed in: [EDR] – Adding Custom Indicators [LINK TO TECHNOLOGY-SPECIFIC PLAYBOOK] and [SIEM]– Adding Custom IOCs [LINK TO TECHNOLOGY-SPECIFIC PLAYBOOK].

Validate all Mechanisms of Persistence have been Removed

Impacted systems will be reimaged during the recovery process. The reimaging should address any boot/autostart executions and scripts, as well as scheduled tasks/jobs. Validate that any impacted accounts/credentials have reset. Detailed in: Password Reset Verification [LINK TO TECHNOLOGY-SPECIFIC PLAYBOOK].

Sweep for IOCs

Threat hunting for the comprehensive list of IOCs should be performed across all technologies to identify potentially impacted systems which were not detected in earlier response efforts or by automated systems. Detailed in: [EDR] IOC-based hunting [LINK TO TECHNOLOGY-SPECIFIC PLAYBOOK] and [SIEM] IOC-based Hunting [LINK TO TECHNOLOGY-SPECIFIC PLAYBOOK].

Submit Samples/IOCs to Vendors as Necessary

Upon successful eradication of the malware, IOCs (without sensitive [COMPANY] information) should be submitted to VirusTotal to help the security community better detect and block similar attempts targeting other organizations.

2.5 Recovery

Restore Infected Hosts to Known Good State

Impacted systems should be reimaged and restored from confirmed-clean backups. If backups are not available, systems will need to be reimaged and rebuilt. These efforts will be managed by the SMEs for the respective impacted systems.

Patch Known Vulnerabilities

If the initial attack vector was identified to be a system vulnerability, the systems hosting the vulnerability should not be brought back online until the vulnerabilities have been successfully patched. The patch effectiveness must be tested following patching efforts.

Close Control Gaps

Any gaps in security controls that lead to the conditions allowing a ransomware infection must be closed prior to restoring business operations either by patching systems or implementing sufficient compensating controls.

Restore All Affected Files

Once the systems have been restored to a known-clean state. The impacted files can be restored to the systems.

Restoration From Backups: Files can first be restored from backups after they have been confirmed to be malware-free.

Restoration via Decryption Key: If a decryption key was recovered either by law enforcement, open-source intelligence, or paying the ransom. The files on the impacted systems can be decrypted. All files and systems should be thoroughly scanned and reviewed following decryption to verify no malicious files/mechanisms for persistence remain.

Reset Impacted User/Host Credentials

Validate that all user, service account, and system account credentials have been reset. A majority of this work likely occurred during the eradication phase, but another verification is recommended.

2.6 Post-Incident Activity

A lessons-learned analysis is conducted by the CST following the closure of a security incident to verify the following:

- The root-cause has been eliminated or adequately mitigated.
- Organizational problems and/or procedures that may have created the conditions which lead to the initial compromise have been adequately remediated.
- Identify technical or operational training needs.
- Identify needed improvements to tools (or usage of tools) or threat intelligence to better perform prevention, detection, analysis, and response actions.

A lesson-learned report is to be generated, and the recommended improvements will be implemented in future incident preparation and response activities.

A complete incident report is developed including all evidence gathered and details of affected systems and data. This report is forwarded to relevant leadership and evidence and findings are forwarded to law enforcement if applicable.

3. Ransomware Response Checklist

The following checklists can be utilized to track incident response efforts throughout the playbook.

3.1 Detection and Analysis

☐ 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.

☐ If taking the network temporarily offline is not immediately possible, locate the network cable and unplug affected devices from the network or remove them from Wi-Fi to contain the infection.

☐ After an initial compromise, malicious actors may monitor [COMPANY]'s activity or communications to understand if their actions have been detected. Be sure to isolate systems in a coordinated manner and use out-of-band communication methods like phone calls or other means 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—already a common tactic—or deploy ransomware widely prior to networks being taken offline.

☐ 2. Only in the event you are unable to disconnect devices from the network, power them down to avoid further spread of the ransomware infection.

☐ 3. Triage impacted systems for restoration and recovery.

☐ Identify and prioritize critical systems for restoration 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 for 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 will enable the organization to get back to business in a more efficient manner.

☐ 4. The CST will confer to develop and document an initial understanding of what has occurred based on initial analysis.

☐ 5. Engage [COMPANY]'s 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 available information to receive the most 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.

3.2 Containment and Eradication

☐ 6. Take a system image and memory capture of a sample of affected devices (e.g., workstations and servers). Additionally, collect any relevant logs as well as samples of any precursor (dropper) 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).

☐ 7. Consult federal law enforcement regarding possible decryptors available, as security researchers have already broken the encryption algorithms for some ransomware variants.

☐ 8. Research the trusted guidance (i.e., published by sources from reputable security vendors) for the particular ransomware variant and follow any additional recommended steps to identify and contain systems or networks that are confirmed to be impacted.

- ☐ Use custom IOCs/IOAs to block the execution of known ransomware binaries; this will minimize damage and impact to your systems. Delete other known, associated registry values and files.

☐ 9. Identify the systems and accounts involved in the initial breach. This can include email accounts.

☐ 10. Based on the breach or compromise details determined above, contain any associated systems that may be used for further or continued unauthorized access. Breaches often involve mass credential exfiltration. Securing the network and other information sources from continued credential-based unauthorized access may include the following actions:

- ☐ Disabling virtual private networks, remote access servers, single sign-on resources, and cloud-based or other public-facing assets.

☐ 11. Additional suggested actions—server-side data encryption quick-identification steps:

- ☐ In the event you learn that server-side data is being encrypted by an infected workstation, quick-identification steps are to:

  1) Review Computer Management > Sessions and Open Files lists on associated servers to determine the user or system accessing those files.

  2) Review file properties of encrypted files or ransom notes to identify specific users that may be associated with file ownership.

  3) Review the TerminalServices-RemoteConnectionManager event log to check for successful RDP network connections.

  4) Review the Windows Security log, SMB event logs, and any related logs that may identify significant authentication or access events.

  5) Run 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").

☐ 12. Conduct an examination of existing organizational detection or prevention systems ([EDR], [FIREWALL] firewalls, [SIEM]) 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. A ransomware event may be evidence of a previous, unresolved network compromise. Many ransomware infections are the result of existing malware infections such as TrickBot, Dridex, or Emotet.

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 in an attempt to further extort the victim and pressure them into paying.

Malicious actors often drop manually deployed ransomware variants on a network to obfuscate their post-compromise activity. Care must be taken to identify such dropper malware before rebuilding from backups to prevent continuing compromise.

☐ 13. 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 events searches in [EDR], audits of local and domain accounts, examination of data found in [SIEM], or deeper forensic analysis of specific systems once movement within the environment has been mapped out.

☐ 14. Rebuild systems based on a prioritization of critical services using pre-configured standard images, if possible.

☐ 15. Once the environment has been fully cleaned and rebuilt (including any associated impacted accounts and the removal or remediation of malicious persistence mechanisms) issue password resets for all affected systems and address any associated vulnerabilities and gaps in security or visibility. This can include applying patches, upgrading software, and taking other security precautions not previously taken.

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

3.3 Recovery and Post-Incident

☐ 17. Reconnect systems and restore data from offline, encrypted backups based on a prioritization of critical services.

☐ 18. Document lessons learned from the incident and associated response activities to inform updates to organizational policies, plans, and procedures and guide future exercises.