RANSOMWARE PLAYBOOK

Contents

[How To Use This Playbook 3](#_Toc115087608)

[Prerequisites/References 4](#_Toc115087609)

[Scope 4](#_Toc115087610)

[Four Phases of Ransomware Response 4](#_Toc115087611)

[Initial Analysis & Containment 4](#_Toc115087612)

[Analysis 4](#_Toc115087613)

[Remediation 4](#_Toc115087614)

[Recovery 4](#_Toc115087615)

[Post-Incident Activity 4](#_Toc115087616)

[Four Phases of Ransomware Response Workflow Diagram 4](#_Toc115087617)

[Detailed Process 4](#_Toc115087618)

[Detection 4](#_Toc115087619)

[Stand Up Cyber Incident Response Team (CSIRT) 4](#_Toc115087620)

[Assembling the CSIRT 4](#_Toc115087621)

[Leadership Notifications 4](#_Toc115087622)

[Engage IR Retainer, as Necessary 4](#_Toc115087623)

[Initial Analysis and Containment 4](#_Toc115087624)

[First-Pass Analysis 4](#_Toc115087625)

[Identify Affected Hosts 4](#_Toc115087626)

[Contain Affected Hosts 4](#_Toc115087627)

[Disable Impacted User/Host Credentials 4](#_Toc115087628)

[Analysis 4](#_Toc115087629)

[Preserve Evidence 4](#_Toc115087630)

[Identify Ransomware Strain 4](#_Toc115087631)

[Establish Infection Vector 4](#_Toc115087632)

[Validate Data Backup Availability and Integrity 4](#_Toc115087633)

[Contact Law Enforcement 4](#_Toc115087634)

[Threat Intel Sharing 4](#_Toc115087635)

[Decision to Engage Cyber Insurance Carrier 4](#_Toc115087636)

[Data Exfiltration 4](#_Toc115087637)

[Regulatory Notifications 5](#_Toc115087638)

[Decision to Pay Ransom 5](#_Toc115087639)

[Eradication 5](#_Toc115087640)

[Add Indicator of Compromise (IOC) to Existing Threat Detection Platform 5](#_Toc115087641)

[Sweep for IOCs 5](#_Toc115087642)

[Submit Samples/IOCs to Vendors as Necessary 5](#_Toc115087643)

[Recovery 5](#_Toc115087644)

[Restore Infected Hosts to Known Good State 5](#_Toc115087645)

[Patch Known Vulnerabilities 5](#_Toc115087646)

[Close Control Gaps 5](#_Toc115087647)

[Restore All Affected Files 5](#_Toc115087648)

[Restoration From Backups 5](#_Toc115087649)

[Restoration via Decryption Key 5](#_Toc115087650)

[Reset Impacted User/Host Credentials 5](#_Toc115087651)

[Post-Incident Activity 5](#_Toc115087652)

[Revision History: 5](#_Toc115087653)

# How To Use This Playbook

Ransomware, unlike other security incidents, puts organizations on a countdown timer. Decisions need to be made swiftly and in an orderly fashion. Any delay in the decision-making process can result in public disclosure or complete loss of data.

The playbook is to be used by the cyber incident response team leader. It focuses on the initial analysis & containment, detailed analysis, eradication, and recovery of the incident by helping organizations prioritize their actions and engage the right people during a confirmed ransomware incident. 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,
* 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, perform the following and no further escalation through the playbook is required:

* 1. <actions>

# Prerequisites/References

# Scope

# Four Phases of Ransomware Response

## Initial Analysis & Containment

## Analysis

## Remediation

## Recovery

## Post-Incident Activity

## Four Phases of Ransomware Response Workflow Diagram

# Detailed Process

# Detection

## Stand Up Cyber Incident Response Team (CSIRT)

### Assembling the CSIRT

## Leadership Notifications

## Engage IR Retainer, as Necessary

# Initial Analysis and Containment

## First-Pass Analysis

## Identify Affected Hosts

## Contain Affected Hosts

## Disable Impacted User/Host Credentials

# Analysis

## Preserve Evidence

## Identify Ransomware Strain

## Establish Infection Vector

## Validate Data Backup Availability and Integrity

## Contact Law Enforcement

## Threat Intel Sharing

## Decision to Engage Cyber Insurance Carrier

## Data Exfiltration

## Regulatory Notifications

## Decision to Pay Ransom

# Eradication

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

## Sweep for IOCs

## Submit Samples/IOCs to Vendors as Necessary

# Recovery

## Restore Infected Hosts to Known Good State

## Patch Known Vulnerabilities

## Close Control Gaps

## Restore All Affected Files

### Restoration From Backups

### Restoration via Decryption Key

## Reset Impacted User/Host Credentials

# Post-Incident Activity

# Revision History:

|  |  |  |  |
| --- | --- | --- | --- |
| **Rev** | **Date** | **Author** | **Description** |
| 1.0 |  |  |  |
|  |  |  |  |
|  |  |  |  |