Incident Response Playbook: Ransomware Attack

Team AnubisX

Version 1.0
September 17, 2025

Document Control

Attribute	Value
Version	1.0
Status	Final
Owner	AnubisX Security Team
Review Cycle	Every Quarter

Contents

1 Introduction **3**
- 1.1 Purpose . . . 3
- 1.2 Scope . . . 3

2 Overview of a Ransomware Attack **3**

3 Incident Response Phases **3**
- 3.1 Phase 1: Preparation . . . 3
- 3.2 Phase 2: Identification & Analysis . . . 3
- 3.3 Phase 3: Containment . . . 4
- 3.4 Phase 4: Eradication . . . 5
- 3.5 Phase 5: Recovery . . . 5
- 3.6 Phase 6: Post-Incident Activities (Lessons Learned) . . . 5

4 MITRE ATT&CK Framework Mapping **6**

1 Introduction

1.1 Purpose

The purpose of this playbook is to provide a clear incident response plan for handling Ransomware Attacks, with the objective of minimizing damage, ensuring business continuity, and preventing recurrence.

1.2 Scope

This playbook applies to all systems, networks, devices, and employees within the organization. It covers all stages of incident response, from preparation to post-incident lessons learned.

2 Overview of a Ransomware Attack

A Ransomware Attack is a type of malicious software that encrypts a victim's files and demands payment (usually in cryptocurrency) to restore access. These attacks are among the most disruptive threats, often resulting in downtime, data loss, and significant financial impact.

3 Incident Response Phases

This playbook follows the NIST Incident Response lifecycle framework.

3.1 Phase 1: Preparation

Goal: To ensure the team is equipped and ready to respond to a ransomware incident before it occurs.

- **Roles and Responsibilities:** Define roles (Incident Commander, Lead Analyst, Forensic Analyst, Communications Lead, Backup & Restore Lead).
- **Tools Resources:** Ensure availability of EDR, SIEM, secure backup systems, forensic imaging tools, and threat intelligence platforms.
- **Training:** Conduct regular ransomware tabletop exercises and restore-from-backup simulations.
- **Contact Lists:** Maintain updated contact lists for executive management, legal, law enforcement, PR, and incident response vendors.
- **Threat Intelligence:** Continuously monitor ransomware TTPs, IOCs, and emerging variants relevant to the industry.

3.2 Phase 2: Identification & Analysis

Goal: To confirm ransomware activity and determine its scope and severity.

1. **Initial Triage:** Collect alerts, isolate suspected systems, open an official incident ticket, and activate secure communication channels. Assemble the AnubisX team.
2. **Initial Analysis and IOC Evaluation:** Analyze logs and alerts to identify Indicators of Compromise (IOCs). Common IOCs include:
    - **Network:** Sudden SMB/HTTP spikes, communication with C2 domains, mass encryption traffic.

- **Endpoint:** Presence of ransom notes, unusual file extensions, high CPU usage from unknown processes.
- **Account:** Privileged account misuse, multiple failed logins, anomalous authentication attempts.

3. **Severity Level Assessment:** Classify the incident to ensure appropriate allocation of resources. Severity is determined based on the operational impact, the criticality of the affected systems and data, and the scope of the encryption.

Level	Description	Example	MTTD	MTTR
Low	Single workstation encrypted, no sensitive data impacted.	An employee laptop gets encrypted after opening a phishing attachment, but the device is isolated quickly and no network shares are affected.	4-6 hours	24 hours
Medium	Limited encryption on non-critical file servers.	A departmental file share storing training materials is encrypted. Operations are slightly impacted, but core business functions continue.	4 hours	1-3 days
High	Multiple systems encrypted, partial disruption of operations.	Several virtual machines in a production environment are encrypted, preventing users from accessing business applications.	24-48 hours	3-7 days
Critical	Widespread encryption including critical systems (e.g., domain controllers, ERP).	A ransomware campaign encrypts domain controllers, Active Directory, and ERP systems, causing a full business outage.	48 hours	7-14 days

Table 1: Incident Severity Matrix

4. **Alert Validation (TP vs. FP):** Correlate suspicious activity with other data points and ransomware-specific threat intelligence.
   - **If True Positive (TP):** The activity is confirmed as ransomware. **Action:** Immediately proceed to the **Containment** phase, escalate to the Incident Commander, and activate the ransomware playbook.
   - **If False Positive (FP):** The activity is confirmed benign. **Action:** Document findings, close the alert, and recommend tuning detection rules.
5. **Incident Declaration:** If confirmed, formally declare a ransomware incident and escalate to leadership and legal counsel.

3.3 Phase 3: Containment

Goal: To limit ransomware spread and prevent further damage.

- **Short-Term Containment (Immediate Actions):**
  - Disconnect infected systems from the network.
  - Disable compromised accounts and revoke session tokens.

  - Block malicious IPs/domains and disable RDP/SMB traffic where possible.

- **Evidence Preservation:** Acquire forensic images of encrypted systems and logs **before** remediation.
- **Long-Term Containment Strategy:** Segment networks, disable unnecessary services, and restrict lateral movement vectors.

3.4 Phase 4: Eradication

Goal: To remove ransomware components and prevent reinfection.

- **Root Cause Analysis:** Identify the entry vector (phishing, RDP exploit, supply chain, etc.).
- **Malware Removal:** Rebuild or reimage infected systems from clean, known-good baselines.
- **Persistence Removal:** Eliminate scheduled tasks, registry keys, or backdoors used by attackers.
- **Security Hardening:** Patch exploited vulnerabilities, enforce MFA, and apply stricter access controls.

3.5 Phase 5: Recovery

Goal: To safely restore systems and business operations.

- **System Restoration:** Recover data from clean, verified backups.
- **Enhanced Monitoring:** Increase monitoring of endpoints and network traffic post-restoration.
- **Validation:** Ensure restored systems are malware-free before reconnecting to the production network.
- **Business Continuity:** Coordinate with leadership to prioritize the restoration of critical services.

3.6 Phase 6: Post-Incident Activities (Lessons Learned)

Goal: To strengthen resilience and prevent recurrence.

- **Post-Incident Meeting:** Conduct a blameless post-mortem meeting within two weeks of incident closure with all stakeholders.
- **Final Incident Report:** Create a detailed report covering the timeline, scope, attack vector, response actions, and costs.
- **Action Plan:** Create a tracked action plan to implement security improvements (e.g., patch management, improved backup strategy, EDR tuning).

4 MITRE ATT&CK Framework Mapping

Ransomware Attack ATT&CK Mapping

- **Tactic: Initial Access**
  - *T1566 – Phishing:* Malicious attachments/links.
  - *T1190 – Exploit Public-Facing Application.*
  - *T1133 – External Remote Services:* Exploiting RDP/VPN.
- **Tactic: Execution**
  - *T1059 – Command-Line & Scripting:* PowerShell, batch.
  - *T1204 – User Execution:* Malicious document execution.
- **Tactic: Persistence**
  - *T1547.001 – Registry Run Keys / Startup Folder.*
  - *T1053 – Scheduled Task/Job.*
- **Tactic: Privilege Escalation**
  - *T1068 – Exploitation for Privilege Escalation.*
  - *T1078 – Valid Accounts:* Using stolen credentials.
- **Tactic: Defense Evasion**
  - *T1562 – Impair Defenses:* Disable AV/EDR.
  - *T1027 – Obfuscated Files or Information.*
- **Tactic: Credential Access**
  - *T1003 – OS Credential Dumping:* LSASS, SAM.
- **Tactic: Discovery**
  - *T1135 – Network Share Discovery.*
  - *T1083 – File and Directory Discovery.*
- **Tactic: Lateral Movement**
  - *T1021.001 – Remote Desktop Protocol (RDP).*
  - *T1021.002 – SMB/Windows Admin Shares.*
- **Tactic: Impact**
  - *T1486 – Data Encrypted for Impact.*
  - *T1490 – Inhibit System Recovery:* Delete shadow copies.
  - *T1489 – Service Stop:* Disable backups/AV services.