Incident Response Report: Initial Response Protocols for Ransomware Attack

---

Executive Summary

This report details the standardized initial incident response (IR) protocols specifically for handling Ransomware Attack incidents within the organization. It outlines the immediate actions required upon detection, describes the components and operational purpose of the supporting case management system, defines clear criteria and procedures for incident escalation, and establishes communication protocols for both internal and external stakeholders. The objective is to provide a clear, actionable framework ensuring a swift, coordinated, and effective response to minimize the impact of ransomware events. This document incorporates industry best practices, drawing from frameworks like NIST SP 800-61, to establish a robust response capability. A standardized template section, completed for a representative ransomware scenario, is included to illustrate practical application.

Introduction

Incident Response (IR) is a critical function within cybersecurity, encompassing the processes and technologies used to detect, respond to, and recover from security incidents. An effective IR capability minimizes breach impact, reduces recovery time and costs, and protects organizational reputation. This document focuses specifically on the **Ransomware Attack** incident type, one of the most prevalent and damaging threats facing organizations today.

The scope of this report covers the *initial* phases of response: detection, initial analysis, containment steps, evidence preservation, system documentation via the case management system, escalation procedures, and initial communication requirements. It adheres to established IR methodologies, primarily following the Preparation, Detection & Analysis, Containment, Eradication, Recovery, and Post-Incident Activity phases outlined in NIST SP 800-61 Rev. 2. This document serves as a foundational guide for the Incident Response Team (IRT) and relevant stakeholders.

Initial Response Protocols (Ransomware Attack)

Upon detection or reporting of a suspected Ransomware Attack, the following initial response protocols must be initiated immediately:

1. **Detection & Initial Verification:**
    - **Source of Detection:** Document how the incident was detected (e.g., user report of ransom note, EDR alert, SIEM correlation rule, filesystem monitoring alert, unusual network traffic).
    - **Verification:** Quickly confirm the signs of ransomware (e.g., encrypted files with specific extensions, presence of ransom notes, system lockout messages). Distinguish from false positives.
2.
3. **Activate the Incident Response Team (IRT):**
    - Notify the designated IRT Lead or on-call responder immediately through predefined channels (e.g., dedicated hotline, secure messaging app).
    - The IRT Lead assumes the role of Incident Commander (IC) or designates one.
4.
5. **Isolate Affected Systems:** *This is the highest priority initial action.*
    - **Network Isolation:** Disconnect the affected machine(s) from the network (disable network adapter, unplug ethernet cable). *Do not power off initially unless advised by forensics specialists, as valuable volatile memory evidence may be lost.*
    - **Account Isolation:** Disable user accounts associated with the infected machine(s) or exhibiting suspicious activity.
    - **Network Segmentation:** If possible and applicable, implement pre-defined network segmentation rules to prevent lateral movement from the affected network segment.
6.
7. **Preserve Evidence:**
    - **Volatile Data:** If feasible and personnel are trained, capture memory (RAM) dump from affected systems *before* powering down or rebooting.
    - **Disk Imaging:** Create forensic disk images of affected systems for later analysis. Store images securely.
    - **Logs:** Collect relevant logs from affected systems, network devices (firewalls, proxies, DNS), SIEM, EDR, and authentication servers (e.g., Domain Controllers) covering the suspected timeframe.
    - **Ransom Note & Samples:** Securely copy the ransom note(s) and samples of encrypted files and, if identifiable, the malware executable itself. *Handle malware samples with extreme caution in an isolated analysis environment.*
8.
9. **Initial Assessment & Scope Identification:**
    - Identify the specific systems confirmed to be infected.
    - Determine the suspected initial infection vector (e.g., phishing email, RDP compromise, software vulnerability).

    - Assess the type of data potentially affected (e.g., general user files, sensitive PII/PHI, critical business data).
    - Check for signs of data *exfiltration* (a common precursor or parallel activity in modern ransomware attacks) by reviewing network traffic logs (especially outbound traffic volumes and destinations).
10.
11. **Documentation (Initiate Case Management):**
    - Create an incident ticket in the Case Management System (details below).
    - Log *all* actions taken, timestamps, personnel involved, systems affected, evidence collected, and observations. Maintain a detailed chronological record.
12.
13. **Containment Strategy Refinement:**
    - Based on initial findings, refine the containment strategy. This may involve broader network segment isolation, blocking C2 domains/IPs identified from logs or malware analysis, or implementing emergency patching for the suspected vulnerability exploited.
    - Identify the ransomware variant if possible (using note details, file extensions, online resources like ID Ransomware). This informs potential decryption options (rarely available for modern variants) and known Tactics, Techniques, and Procedures (TTPs).
14.

Case Management System Components

The Case Management System (CMS) is the central hub for tracking, managing, and documenting all incident response activities. It ensures consistency, facilitates collaboration, and provides an auditable record.

- **Component: Incident Ticketing System** (e.g., ServiceNow Security Operations, JIRA with specific workflows, TheHive, RTIR)
    - **Description:** A system for logging new incidents, assigning unique identifiers, tracking status, assigning tasks to IRT members, and recording actions taken.
    - **Operational Purpose:** Provides structured tracking of each incident from detection to closure. Ensures accountability and allows for metrics reporting (time-to-detect, time-to-contain, etc.). Key fields include: Incident ID, Status, Severity, Reporter, Assignee, Affected Systems, IOCs, Action Log, Resolution Details.
-
- **Component: Evidence Repository** (e.g., Secure Network Share with Access Control, Dedicated Forensic Evidence Management Tool)
    - **Description:** A secure, access-controlled location for storing all collected digital evidence, including disk images, memory dumps, log files, malware samples, and screenshots. Chain of custody forms/tracking mechanisms are essential.

    - **Operational Purpose:** Ensures the integrity and availability of evidence for analysis, legal purposes, and post-incident review. Prevents tampering or accidental deletion.
-
- **Component: Knowledge Base / Playbooks** (e.g., Confluence, SharePoint, integrated CMS feature)
    - **Description:** A repository of IR plans, procedures (like this document), playbooks for specific incident types, contact lists, known IOCs from past incidents, threat intelligence feeds, and lessons learned.
    - **Operational Purpose:** Provides quick access to standardized procedures and historical context, improving response speed and consistency. Facilitates training and knowledge sharing.
-
- **Component: Secure Communication Channel** (e.g., Dedicated Slack/Teams channel with restricted access, PGP-encrypted email list)
    - **Description:** A dedicated channel for real-time communication and coordination among IRT members during an active incident. Must be separate from potentially compromised corporate communication systems.
    - **Operational Purpose:** Enables rapid information sharing, decision-making, and task coordination among the response team without relying on potentially compromised infrastructure.
-
- **Component: Reporting & Analytics Dashboard** (e.g., SIEM dashboard, CMS reporting module, BI tools)
    - **Description:** Visualizes the status of ongoing incidents, key metrics, trends, and potentially displays real-time alerts relevant to the incident.
    - **Operational Purpose:** Provides situational awareness to the IRT and management. Helps in identifying bottlenecks, resource allocation needs, and long-term trends.
-
- **Roles & Responsibilities within CMS:**
    - **Incident Reporter:** Anyone detecting an incident; initiates the initial report/ticket.
    - **Incident Handler (Analyst/Engineer):** Performs technical investigation, containment, eradication, updates ticket details, uploads evidence.
    - **Incident Commander (IC) / IRT Lead:** Oversees the response, makes critical decisions, assigns tasks via CMS, ensures documentation quality, manages escalations.
    - **Forensic Analyst:** Utilizes evidence from the repository for deep-dive analysis.
    - **Communications Lead:** Uses CMS information to draft internal/external communications.
    - **Legal/Compliance Liaison:** Accesses incident details in CMS to advise on legal/regulatory obligations.
-

Incident Escalation Criteria (Ransomware Attack)

Incidents are escalated based on their potential or realized impact. Escalation ensures appropriate resources and authority are engaged.

- **Initial Triage (L1/SOC Analyst):** Verifies the alert/report. Performs initial isolation if confident. Escalates to L2/Incident Handler if ransomware is confirmed or strongly suspected.
- **Escalation to IRT Lead / Incident Commander (IC):**
    - **Trigger:** Any confirmed ransomware incident.
    - **Decision Point:** Made by L1/L2 analyst upon confirmation. IC takes command.
-
- **Escalation to Senior Management (CISO, CIO, Relevant Business Unit Heads):**
    - **Triggers:**
        - Impact on Critical Business Systems (e.g., ERP, production databases, core customer-facing services).
        - Widespread infection (e.g., >10% of endpoints, multiple critical servers).
        - Confirmed exfiltration of sensitive data (PII, PHI, IP).
        - Inability to contain the spread within X hours (e.g., 4 hours).
        - Significant operational disruption expected (> Y hours, e.g., 8 hours).
        - Potential for significant financial loss or reputational damage.
        - Ransom demand received (notification of the demand itself).
    -
    - **Decision Point:** Made by the Incident Commander based on the assessment against these triggers.
-
- **Escalation to Executive Leadership (CEO, Legal Counsel, Board Subcommittee):**
    - **Triggers:**
        - Confirmed breach requiring regulatory notification (e.g., GDPR, HIPAA).
        - Confirmed breach requiring public disclosure.
        - Major operational disruption impacting the entire organization or key business lines.
        - High-stakes ransom demand or negotiation considerations (especially the decision *whether* to pay).
        - Significant media attention or public awareness.
        - Involvement of law enforcement at a strategic level.
    -
    - **Decision Point:** Made by CISO/CIO in consultation with the Incident Commander and Legal Counsel.
-
- **Escalation Flow (Simplified):**
  Detection -> L1/SOC Verify -> L2/Handler Confirm & Initial Actions -> IRT Lead/IC

Activated -> [Triggers Met?] -> Escalate to CISO/Mgmt -> [Triggers Met?] -> Escalate to Exec Leadership/Legal

---

Communication Protocols (Ransomware Attack)

Clear, controlled communication is vital during a ransomware incident.

- **Internal Communication:**
    - **IRT Coordination:** Via the designated secure communication channel. Regular sync-ups (e.g., every 1-2 hours initially, adjusting frequency as needed). Focus on technical findings, actions, obstacles.
    - **IT Operations/Support Teams:** Communicate specific tasks required (e.g., restoring from backups, blocking network access, deploying patches) on a need-to-know basis, often via the CMS ticketing system or controlled channels. Avoid broad, alarming broadcasts initially.
    - **Management/Leadership:** Provide regular, concise updates via email summaries or brief calls from the IC or Comms Lead. Focus on business impact, containment status, key decisions needed (e.g., resource allocation, ransom payment consideration). Use non-technical language where possible.
    - **Employees:** Initial communication should be carefully crafted (with Legal/HR input) to inform without causing panic. May include instructions like:
        - Do not reboot machines exhibiting strange behavior.
        - Report any suspicious activity immediately to the Help Desk/Security.
        - Disconnect from VPN if advised.
        - Reinforce awareness about phishing/social engineering attempts that might follow.
    -
    - **Decision Point (Employee Comms):** Decision to communicate broadly rests with CISO/IC, often after initial containment efforts show progress or if the impact becomes widely visible. Content approved by Comms/Legal/HR.
-
- **External Communication:** *All external communication must be coordinated through designated points of contact (e.g., Communications Lead, Legal Counsel, official PR function) and approved before release.*
    - **Legal Counsel:** Engage *immediately* upon confirming a significant ransomware incident, especially if sensitive data is involved or exfiltration is suspected. Provide details via secure channels.
    - **Cyber Insurance Provider:** Notify according to policy requirements (often within 24-72 hours). Provide information as required by the policy, coordinated through Legal.
    - **Law Enforcement:** (e.g., FBI, CISA, local authorities) Report the incident. They may provide assistance or intelligence but generally do not assist directly with recovery. Decision to engage often made by IC/CISO with Legal advice.

- **Regulatory Bodies:** If data breach notification laws apply (based on type and residency of data affected), notifications must be made within statutory deadlines. Legal counsel determines requirements and manages the process.
- **Affected Customers/Partners:** If their data or services relying on the organization are impacted. Communication strategy (timing, content, method) developed by Comms/PR, approved by Legal and Executive Leadership. Transparency is key but must be carefully managed.
- **Third-Party IR/Forensics:** Engage pre-approved vendors if internal capabilities are insufficient or specialized expertise is needed. Managed by IRT Lead/IC.
- **Threat Actor:** Communication (if any, regarding ransom negotiation) should *only* be handled by designated, trained personnel (often external negotiators engaged via insurance/legal), with explicit approval from Executive Leadership and Legal. *No unauthorized contact.*
- **Media/Public:** Generally avoided unless legally required or strategically necessary (e.g., widespread service outage). All statements managed by official PR/Communications function, approved by Legal and Executive Leadership.
- **Decision Point (External Comms):** Timing and content driven by legal/regulatory requirements, business impact, and strategic considerations. Approved by Legal Counsel and Executive Leadership.

Completion of Incident Response Documentation Template (Illustrative Example)

This section simulates filling out key fields of a standardized template within the Case Management System for a hypothetical ransomware incident at its initial stage.

Field	Value
Incident ID:	RANSOM-20231026-001
Date/Time Detected:	2023-10-26 09:15 UTC
Date/Time Occurred:	Estimated 2023-10-26 08:00 UTC (Initial Access)
Incident Type:	Ransomware Attack
Severity:	Critical
Status:	Active - Containment in Progress
Reporter:	User: J. Doe (via Help Desk Ticket HD-12345)

Detection Method:	User Report (Ransom Note Displayed), EDR Alert (Suspicious Process)
Incident Commander:	[Name of IC]
Assigned Handler(s):	[Name(s) of L2/L3 Analysts]
Affected Systems (Initial List):	WS-FINANCE-01, WS-FINANCE-02, SRV-FILESHARE-03
Suspected Vector:	Phishing Email (Malicious Attachment) - *Under Investigation*
Initial Impact Assessment:	Finance department file share partially encrypted. Two user workstations confirmed encrypted. Potential impact on Q3 financial reporting process. Signs of lateral movement detected by EDR on SRV-AD-01 (blocked). No evidence of data exfiltration *yet*.
Ransomware Variant:	Suspected 'Conti' based on note analysis (TBC)
Ransom Note Received:	Yes (Saved as Evidence EV-RANSOM-001)
Ransom Demand:	$500,000 USD in BTC (Details in EV-RANSOM-001)
Initial Actions Taken:	- IRT Activated (09:20 UTC) - Affected systems isolated from network (WS-FINANCE-01/02 @ 09:25, SRV-FILESHARE-03 @ 09:30 UTC) - Associated user accounts disabled (J.Doe, Finance_Service_Acct @ 09:40 UTC) - Memory dump captured from WS-FINANCE-01 (09:55 UTC) - Disk imaging initiated for affected systems (10:15 UTC) - Log collection initiated (Firewall, EDR, AD, File Server) (10:00 UTC) - Case RANSOM-20231026-001 created in TheHive (09:22 UTC) - Initial IOCs identified (Hash: [abc...], IP: [x.x.x.x]) blocked at firewall (10:30 UTC)
Evidence Collected:	EV-RANSOM-001 (Note), EV-MEM-WSFIN01 (Memory), EV-LOGS-FW/EDR/AD (Logs), EV-SAMPLE-MAL (Malware Sample - quarantined)
Escalation Status:	Escalated to CISO (A. Smith) @ 10:45 UTC due to critical system impact (File Share) and potential business disruption. Legal Counsel (B. Jones) notified @ 11:00 UTC. Cyber Insurance Provider notified @ 11:15 UTC.

Next Steps:	- Complete disk imaging. - Analyze logs for lateral movement & exfiltration. - Perform initial malware analysis (sandbox). - Assess backup integrity and recovery options. - Convene IRT Sync Meeting @ 13:00 UTC.

Conclusion

This report provides a detailed framework for the initial response to Ransomware Attack incidents. By adhering to these protocols for immediate actions, case management, escalation, and communication, the organization can mount a more effective defense against this pervasive threat. The defined procedures aim to limit damage, preserve crucial evidence, ensure stakeholders are informed appropriately, and facilitate a structured transition into eradication and recovery phases. Regular training, drills, and updating of these protocols based on lessons learned and evolving threat landscape are essential for maintaining response readiness.

References

- NIST Special Publication 800-61 Revision 2: Computer Security Incident Handling Guide. (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf)
- ISO/IEC 27035: Information technology – Security techniques – Information security incident management.
- SANS Institute Incident Handler's Handbook. (https://www.sans.org/white-papers/33904/)
- [Internal Policy] Organizational Incident Response Plan (OIRP) vX.X
- [Internal Policy] Data Classification Policy
- [Internal Tool] Link to Case Management System (e.g., TheHive instance)
- [External Resource] CISA Ransomware Guide (https://www.cisa.gov/stopransomware)
