Incident Response Playbook: Malware Infection

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

1.1 Purpose

The purpose of this playbook is to provide a clear incident response plan for handling Malware Infections (excluding ransomware), 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 Malware Infection

A Malware Infection is a security incident in which malicious software is installed on a system without authorization. Unlike ransomware, which encrypts data for extortion, non-ransomware malware may include trojans, worms, spyware, adware, or rootkits. These can result in data theft, credential compromise, system instability, unauthorized access, or use of resources for botnets or cryptomining.

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 malware incident before it occurs.

- **Roles and Responsibilities:** Define roles (Incident Commander, Lead Analyst, Forensic Analyst, Communications Lead, IT Operations Lead).
- **Tools & Resources:** Ensure availability of EDR, SIEM, forensic tools, anti-malware solutions, and network monitoring systems.
- **Training:** Conduct malware awareness training and host regular incident response exercises.
- **Contact Lists:** Maintain updated contact lists for key stakeholders, vendors, and external IR partners.
- **Threat Intelligence:** Continuously monitor malware campaigns, families, and techniques relevant to the industry.

3.2 Phase 2: Identification & Analysis

Goal: To confirm malware infection and determine its scope and severity.

1. **Initial Triage:** Collect alerts, isolate suspected systems, open an incident ticket, and activate secure communications.
2. **Initial Analysis and IOC Evaluation:** Analyze logs and alerts to identify Indicators of Compromise (IOCs). Common IOCs include:

- **Network:** Unusual outbound connections, beaconing to C2 servers, abnormal traffic patterns.
- **Endpoint:** Unexpected processes, new or suspicious services, registry modifications, persistence mechanisms.
- **Account:** Unauthorized privilege escalation, unusual login attempts, credential dumping signs.

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

Level	Description	Example	MTTD	MTTR
Low	Single workstation infected, minimal impact, no sensitive data accessed.	An employee downloads adware that displays unwanted popups but does not spread further.	6-12 hours	24-48 hours
Medium	Malware infection on multiple systems with limited data exposure.	A worm spreads to several computers within a department but is contained quickly.	12-24 hours	2-4 days
High	Multiple systems compromised with credential theft or data exfiltration.	Spyware is discovered on several endpoints, capturing keystrokes and sending them to an external server.	24-48 hours	4-7 days
Critical	Organization-wide malware outbreak impacting core business systems.	Rootkit infection detected on domain controllers enabling unauthorized persistent access.	48 hours	7-14 days

Table 1: Incident Severity Matrix

4. **Alert Validation (TP vs. FP):** Correlate suspicious activity with other data points and threat intelligence.
   - **If True Positive (TP):** The activity is confirmed as malware. **Action:** Immediately proceed to the **Containment** phase, escalate to the Incident Commander, and activate the malware 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 malware incident and escalate to leadership, legal, and relevant IT teams.

3.3 Phase 3: Containment

Goal: To prevent the malware from spreading and causing further damage.

- **Short-Term Containment (Immediate Actions):**
  - Isolate infected systems from the network.
  - Disable compromised user accounts.
  - Block malicious IPs/domains to prevent further C2 communication.

- **Evidence Preservation:** Acquire disk images, memory captures, and relevant logs **before** remediation.
- **Long-Term Containment Strategy:** Enhance network segmentation to limit potential spread.

3.4 Phase 4: Eradication

Goal: To remove the malware and any associated persistence mechanisms.

- **Root Cause Analysis:** Identify the initial infection vector.
- **Malware Removal:** Remove malware and persistence mechanisms from all affected systems.
- **System Remediation:** Reimage infected systems from clean baselines.
- **Security Hardening:** Patch exploited vulnerabilities and enforce MFA and enhanced access controls.

3.5 Phase 5: Recovery

Goal: To safely restore systems and business operations.

- **System Restoration:** Restore systems to normal operation from verified backups or clean images.
- **Validation:** Validate system integrity and confirm the absence of malware before reconnecting to the network.
- **Enhanced Monitoring:** Closely monitor restored systems for any reinfection attempts.
- **Business Continuity:** Prioritize the recovery of critical business functions in coordination with leadership.

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 with all stakeholders.
- **Final Incident Report:** Prepare a detailed report including the incident scope, root cause, and remediation steps.
- **Action Plan:** Implement improved endpoint security, patch management, and user training. Share IOCs with trusted threat-sharing communities.

4 MITRE ATT&CK Framework Mapping

Malware Infection ATT&CK Mapping

- **Tactic: Initial Access**
  - *T1566 – Phishing*
  - *T1190 – Exploit Public-Facing Application*
  - *T1189 – Drive-by Compromise*
- **Tactic: Execution**
  - *T1059 – Command and Scripting Interpreter*
  - *T1204 – User Execution*
  - *T1106 – Native API*
- **Tactic: Persistence**
  - *T1547 – Boot or Logon Autostart Execution*
  - *T1053 – Scheduled Task/Job*
- **Tactic: Defense Evasion**
  - *T1562 – Impair Defenses*
  - *T1027 – Obfuscated Files or Information*
  - *T1036 – Masquerading*
- **Tactic: Credential Access**
  - *T1003 – OS Credential Dumping*
  - *T1555 – Credentials from Password Stores*
- **Tactic: Lateral Movement**
  - *T1021 – Remote Services*
  - *T1570 – Lateral Tool Transfer*
- **Tactic: Impact**
  - *T1499 – Endpoint Denial of Service*
  - *T1496 – Resource Hijacking*