Incident Response Playbook: Endpoint Beaconing (C2 Communication)

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 Endpoint Beaconing and Command-and-Control (C2) communication incidents, with the objective of minimizing attacker persistence, preventing data exfiltration, and restoring secure operations.

1.2 Scope

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

2 Overview of Endpoint Beaconing

Endpoint Beaconing is a behavior where compromised endpoints periodically attempt to connect to an external Command-and-Control (C2) server controlled by an attacker. This allows the attacker to issue commands, exfiltrate data, or move laterally within the environment. Detecting and responding quickly is essential to limit damage and eradicate attacker presence.

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 endpoint beaconing incidents before they occur.

- **Roles and Responsibilities:** Define roles (Incident Commander, Lead Analyst, Forensic Analyst, Communications Lead, Network Security Lead).
- **Tools & Resources:** Ensure availability of EDR, SIEM, IDS/IPS, network traffic analysis tools, forensic tools, and threat intelligence feeds.
- **Training:** Conduct red-team simulations and beaconing detection exercises.
- **Contact Lists:** Maintain updated contacts for executive management, legal, PR, and IR vendors.
- **Threat Intelligence:** Continuously monitor reports of C2 infrastructures and associated IOCs.

3.2 Phase 2: Identification & Analysis

Goal: To confirm C2 beaconing activity and determine its scope and severity.

1. **Initial Triage:** Collect IDS/IPS alerts, NetFlow logs, and endpoint telemetry. Open an incident ticket and activate secure comms.
2. **Initial Analysis and IOC Evaluation:** Analyze logs and alerts to identify Indicators of Compromise (IOCs). Common IOCs include:
    - **Network:** Regular outbound connections to suspicious IPs/domains, unusual ports (e.g., 8080, 8443), encrypted traffic to unknown hosts.

- **Endpoint:** Unknown processes maintaining external connections, persistence mechanisms, registry changes.
- **Account:** Use of stolen credentials for beaconing-related activity.

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 the scope of the compromise.

Level	Description	Example	MTTD	MTTR
Low	Single endpoint beaconing, no sensitive data exfiltration.	An employee workstation connects periodically to a suspicious domain but is contained quickly.	6-12 hours	24-48 hours
Medium	Multiple endpoints beaconing, limited lateral movement.	Several computers in one department show regular outbound traffic to a known malicious IP.	12-24 hours	2-4 days
High	Widespread beaconing with potential credential theft or partial data exfiltration.	EDR confirms multiple systems running a trojan that beacons to external servers, with evidence of file staging.	24-48 hours	4-7 days
Critical	Organization-wide beaconing and confirmed attacker control with data exfiltration.	Beaconing activity detected on critical servers (e.g., domain controllers) with confirmed exfiltration to attacker infrastructure.	48 hours	7-14 days

Table 1: Incident Severity Matrix

4. **Alert Validation (TP vs. FP):** Correlate suspicious network activity with threat intelligence and endpoint data.
   - **If True Positive (TP):** The activity is confirmed as C2 communication. **Action:** Immediately proceed to the **Containment** phase, escalate to the Incident Commander, and activate the C2 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 C2 incident and escalate to leadership, legal, and relevant IT teams.

3.3 Phase 3: Containment

Goal: To sever the attacker's communication channel and prevent further damage.

- **Short-Term Containment (Immediate Actions):**
  - Isolate affected endpoints from the network.
  - Block malicious IPs/domains at firewalls and proxies.
  - Disable compromised accounts and revoke active session tokens.

- **Evidence Preservation:** Acquire NetFlow, PCAPs, and forensic images of affected endpoints **before** remediation.
- **Long-Term Containment Strategy:** Implement stricter egress filtering rules and enhance network segmentation.

3.4 Phase 4: Eradication

Goal: To remove the malware and any attacker persistence.

- **Root Cause Analysis:** Identify the initial entry vector of the malware.
- **Malware Removal:** Remove the malware responsible for beaconing from all affected systems.
- **Persistence Removal:** Reimage or clean infected systems from known-good baselines and remove any persistence mechanisms.
- **Security Hardening:** Patch vulnerabilities exploited for C2 installation and harden system configurations.

3.5 Phase 5: Recovery

Goal: To safely restore systems and normal operations.

- **System Restoration:** Restore cleaned systems to the production environment.
- **Enhanced Monitoring:** Validate system and network traffic for any signs of beaconing before and after restoration.
- **Validation:** Ensure restored systems are malware-free before reconnecting to the production network.
- **Business Continuity:** Resume normal operations with stricter network segmentation and egress controls.

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

Goal: To strengthen resilience and prevent recurrence.

- **Post-Incident Meeting:** Conduct a blameless post-mortem with all stakeholders.
- **Final Incident Report:** Document the timeline, attacker TTPs, impact, and lessons learned.
- **Action Plan:** Improve detection rules (IDS/IPS signatures, EDR alerts) and share IOCs with trusted security communities.

4 MITRE ATT&CK Framework Mapping

Endpoint Beaconing ATT&CK Mapping

- **Tactic: Command and Control**
  - *T1071 – Application Layer Protocol*
  - *T1105 – Ingress Tool Transfer*
  - *T1573 – Encrypted Channel*
- **Tactic: Initial Access**
  - *T1566 – Phishing*
  - *T1190 – Exploit Public-Facing Application*
  - *T1189 – Drive-by Compromise*
- **Tactic: Persistence**
  - *T1547 – Boot or Logon Autostart Execution*
  - *T1053 – Scheduled Task/Job*
- **Tactic: Defense Evasion**
  - *T1562 – Impair Defenses*
  - *T1027 – Obfuscated Files or Information*
- **Tactic: Exfiltration**
  - *T1041 – Exfiltration Over C2 Channel*
  - *T1567 – Exfiltration Over Web Service*
- **Tactic: Impact**
  - *T1499 – Endpoint Denial of Service*
  - *T1490 – Inhibit System Recovery*