Incident Response Playbook: Suspicious USB Device Usage — (data transfer / autorun)

Team AnubisX

Version 1.0
September 23, 2025

Document Control

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

Contents

1 Introduction

1.1 Purpose

This playbook defines incident response procedures for handling "Suspicious USB Device Usage — (data transfer / autorun)". It provides roles, responsibilities, detection indicators, containment steps, and recovery guidance to minimize impact and restore services.

1.2 Scope

This playbook applies to systems, network components, cloud services, and personnel. It is intended for use by incident responders, SOC analysts, IT operations, legal, and leadership.

2 Overview of the Attack

USB devices are a common vector for malware introduction and data exfiltration. Key risks include:

- Malware introduction, data theft, unauthorized data transfer
- Potential lateral spread via removable media

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 suspicious USB incident before it occurs.

- **Roles and Responsibilities:** Define roles: Incident Commander, Lead Analyst, Forensics, IT, Communications.
- **Logging Auditing:** Ensure logging and centralized authentication audits are enabled.
- **Tools Resources:** Deploy specialized detection rules and maintain playbooks for the specific alert type.
- **Training:** Regular backups and least-privilege access models.

3.2 Phase 2: Identification & Analysis

Goal: Confirm the activity and determine scope and severity.

1. **Initial Analysis and IOC Evaluation:** Analyze logs and alerts to identify Indicators of Compromise (IOCs). Common IOCs include:
    - New removable device mounts with large file copy activity
    - Autorun entries triggering executable payloads
    - Unusual file system timestamps aligned with device connection

2. **Severity Level Assessment:** Classify the incident to ensure appropriate allocation of resources. Severity is based on: Operational Impact, Criticality of affected systems/data, Scope of attack, and Detection/Recovery timelines (MTTD/MTTR).

Level	Description	Example	MTTD	MTTR
Low	Single authorized device used for normal transfer.	Employee uses thumb drive for legitimate task.	<1 hr	<24 hrs
Medium	Unknown device used and suspicious copies observed.	USB device used to move sensitive documents across machines.	1-6 hrs	1-3 days
High	Malware introduced or sensitive data stolen via USB.	Device runs autorun malware and exfiltrates files.	6-24 hrs	3-7 days
Critical	Large-scale data exfiltration or malware spread via multiple devices.	Coordinated insider exfil using multiple USBs.	24+ hrs	7-21 days

Table 1: Incident Severity Matrix

3.3 Phase 3: Containment

Goal: Limit attacker actions and preserve evidence.

- Unplug device after forensically imaging the host, disable USB ports where appropriate.
- Collect device identifiers (VID/PID/serial) and review file copy logs.

3.4 Phase 4: Eradication

Goal: To remove malicious components and prevent reinfection.

- Remove malicious files, reimage infected hosts, disable autorun policies.
- Policy enforcement and user training on removable media.

3.5 Phase 5: Recovery

Goal: To safely restore systems and business operations.

- Restore data from backups and audit access to sensitive files.
- Implement USB control solutions and DLP.

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

Goal: To strengthen resilience and prevent recurrence.

- Conduct a blameless post-mortem and update playbooks.
- Produce final incident report and recommended mitigations.
- Implement controls to reduce recurrence.

4 MITRE ATT&CK Framework Mapping

Suspicious USB Usage ATT&CK Mapping

- **Tactic: Initial Access**
  - *T1091 – Replication Through Removable Media*
- **Tactic: Exfiltration**
  - *T1041 – Exfiltration Over C2 Channel*