# Incident Response Playbook: Suspicious Service Creation (Windows)

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 Service Creation (Windows)". 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

Attackers often create services on Windows hosts to achieve persistence and run malicious payloads with system privileges. Key risks include:

- Unauthorized persistence with SYSTEM privileges
- Service misuse to run ransomware or C2 stagers
- Evasion by hiding as legitimate services

# 3 Incident Response Phases

## 3.1 Phase 1: Preparation

- **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 service installation events with odd file paths
   - Services starting executables from user temp directories
   - Service configured to auto-start with suspicious descriptions
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 non-critical host shows new service. | User-installed service for legitimate software misclassified. | <4 hrs | <24 hrs |
| **Medium** | Multiple hosts show unusual services. | "Service installed across a department, suspected installer abuse". | 4-12 hrs | 1-3 days |
| **High** | Service used to run backdoor or credential harvester. | Service spawns reverse shell connections and persists. | 12-24 hrs | 3-7 days |
| **Critical** | Widespread malicious service creation on servers including DCs. | Service used to deploy payloads across AD. | 24+ hrs | 7-21 days |

Table 1: Incident Severity Matrix

### 3.3 Phase 3: Containment

*Goal: To limit attacker actions and preserve evidence.*

- Stop and record the service, collect binary and registry info, isolate host.
- Search for similar service artifacts across network, block source binaries.

### 3.4 Phase 4: Eradication

- Remove service entries, clean up persistence mechanisms, reimage if required.
- Harden service creation policies and use AppLocker/WDAC.

### 3.5 Phase 5: Recovery

- Restore systems from clean images and verify no reintroduction.
- Reinstate monitoring for service creation events.

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

- 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 Service Creation ATT&CK Mapping**

- **Tactic: Persistence**
  - *T1543 – Create or Modify System Process (Service)*
  - *T1050 – New Service*
- **Tactic: Defense Evasion**
  - *T1562 – Impair Defenses*
- **Tactic: Execution**
  - *T1059 – Command and Scripting Interpreter*