Incident Response Playbook: Suspicious Scheduled Task / Persistence Mechanism

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 Scheduled Task / Persistence Mechanism". 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

Scheduled tasks are frequently abused for persistence, lateral execution, and scheduled malware runs. Key risks include:

- Stealthy persistence
- Automated payload execution
- Evading detection through legitimate scheduler features

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 scheduled task 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 scheduled tasks with suspicious commands
    - Tasks created by non-admin users with elevated actions
    - Tasks invoking PowerShell or WMIC for remote commands

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 workstation task misconfiguration.	A support script created a new task with expected behavior.	<4 hrs	<24 hrs
Medium	Tasks found on multiple hosts.	Tasks used to maintain unauthorized access on several machines.	4-12 hrs	1-3 days
High	Tasks create backdoors on servers or perform credential dumps.	Scheduled tasks run malicious scripts across multiple servers.	12-24 hrs	3-7 days
Critical	Task-based automation leads to mass compromise.	Attacker uses scheduled tasks to deploy ransomware enterprise-wide.	24+ hrs	7-21 days

Table 1: Incident Severity Matrix

3.3 Phase 3: Containment

Goal: To limit attacker actions and preserve evidence.

- Disable the task, collect task XML, identify creator account and timestamp.
- Hunt for similar tasks and associated payloads across endpoints.

3.4 Phase 4: Eradication

Goal: To remove malicious components and prevent reinfection.

- Remove task entries, review scheduled task history, update policies to restrict task creation.
- Reimage when necessary and apply hardened baseline.

3.5 Phase 5: Recovery

Goal: To safely restore systems and business operations.

- Validate restored hosts and monitor for re-creation of tasks.
- Update detection rules and educate administrators on secure task management.

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 Scheduled Task ATT&CK Mapping

- **Tactic: Persistence**
  - *T1053 – Scheduled Task/Job*
  - *T1543 – Create or Modify System Process*
- **Tactic: Defense Evasion**
  - *T1070 – Indicator Removal on Host*