Incident Response Playbook: Suspicious PowerShell Activity

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 3

1.1 Purpose . . . 3

1.2 Scope . . . 3

2 Overview of the Attack 3

3 Incident Response Phases 3

3.1 Phase 1: Preparation . . . 3

3.2 Phase 2: Identification & Analysis . . . 3

3.3 Phase 3: Containment . . . 4

3.4 Phase 4: Eradication . . . 4

3.5 Phase 5: Recovery . . . 5

3.6 Phase 6: Post-Incident Activities (Lessons Learned) . . . 5

4 MITRE ATT&CK Framework Mapping 6

1 Introduction

1.1 Purpose

This playbook defines the incident response procedures for handling "Suspicious PowerShell Activity". It provides roles, responsibilities, detection indicators, containment steps, and recovery guidance to minimize impact and restore services.

1.2 Scope

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

2 Overview of the Attack

"Suspicious PowerShell Activity" typically involves using Windows PowerShell to execute scripts, download payloads, or abuse system utilities. PowerShell gives attackers powerful scripting capabilities and deep access to the operating system. Key risks include:

- Silent execution of malicious scripts
- Fileless persistence that evades traditional AV
- Credential theft via in-memory tools
- Lateral movement using PowerShell remoting or invoke-command
- Data exfiltration and launching of secondary payloads (ransomware, C2)

3 Incident Response Phases

3.1 Phase 1: Preparation

Goal: To ensure the team is prepared to detect and respond to suspicious PowerShell activity.

- **Roles and Responsibilities:** Define roles (Incident Commander, Lead Analyst, Forensics, IT, Communications).
- **Tools & Resources:** Deploy and tune EDR and PowerShell script block logging. Implement constrained language mode and execution policy where possible.
- **Training:** Conduct tabletop exercises focusing on script-based attacks.
- **Contact Lists:** Maintain secure backups and recovery playbooks.

3.2 Phase 2: Identification & Analysis

Goal: To confirm malicious PowerShell usage and determine scope and severity.

1. **Initial Triage:** Collect alerts from EDR and SIEM, isolate suspected hosts, open an official incident ticket, and assemble the incident response team.
2. **Initial Analysis and IOC Evaluation:** Analyze logs and alerts to identify Indicators of Compromise (IOCs). Common IOCs include:
   - **Process:** PowerShell spawning child processes (e.g., mshta, rundll32).

- **Command Line:** EncodedCommand usage or long obfuscated commands.
- **Logs:** Script block logging showing suspicious download/execution patterns.
- **Network:** Unusual network connections initiated by powershell.exe to external IPs/domains.
- **Behavior:** Commands invoking credential harvesting tools (mimikatz) or bypassing AMSI.

3. **Severity Level Assessment:** The severity is determined by operational impact, criticality of affected systems and data, scope of the attack, and detection/recovery timelines.

Level	Description	Example	MTTD	MTTR
Low	Single host; no sensitive data; script stopped quickly.	An analyst killed a malicious PS process on a laptop.	1-4 hrs	<24 hrs
Medium	Multiple hosts with non-critical impact.	Malicious scripts executed on a department file server but backups intact.	4-12 hrs	1-3 days
High	Credential access, lateral movement, partial service disruption.	PowerShell used to dump credentials and move laterally to several servers.	12-48 hrs	3-7 days
Critical	Widespread execution including domain controllers or data exfil.	Encoded PowerShell deploys ransomware payloads across AD.	48+ hrs	7-14 days

Table 1: Incident Severity Matrix

4. **Incident Declaration:** If malicious activity is confirmed, formally declare an incident and escalate to leadership and relevant stakeholders.

3.3 Phase 3: Containment

Goal: To limit attacker actions and preserve evidence.

- Isolate affected hosts from the network.
- Terminate suspicious powershell.exe processes after capturing memory and logs.
- Block identified malicious domains/IPs at the perimeter and in the EDR.
- Force password resets for compromised accounts and revoke tokens.
- Enable enhanced logging across endpoints to track lateral movement.

3.4 Phase 4: Eradication

Goal: To remove malicious artifacts and prevent reinfection.

- Collect forensic images and memory dumps before remediation.
- Remove malicious scripts, scheduled tasks, and services introduced by the attacker.
- Restore affected systems from known-good backups where necessary.
- Patch exploited vulnerabilities and harden PowerShell scripting settings.

3.5 Phase 5: Recovery

Goal: To safely restore systems and business operations.

- Validate backups and perform controlled restores.
- Monitor restored systems for signs of re-infection.
- Gradually reconnect systems to production with increased monitoring.
- Communicate status to leadership and stakeholders.

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

Goal: To analyze the incident and improve security posture.

- Conduct a blameless post-mortem and update playbooks.
- Tune detection rules to reduce false positives and improve coverage.
- Implement additional controls such as AppLocker and Constrained Language Mode.
- Train staff on phishing and suspicious script reporting.

4 MITRE ATT&CK Framework Mapping

Suspicious PowerShell Activity ATT&CK Mapping

- **Tactic: Initial Access**
  - *T1566 – Phishing.*
  - *T1190 – Exploit Public-Facing Application.*
- **Tactic: Execution**
  - *T1059 – Command and Scripting Interpreter (PowerShell).*
  - *T1204 – User Execution.*
- **Tactic: Persistence**
  - *T1547.001 – Registry Run Keys / Startup Folder.*
  - *T1053 – Scheduled Task/Job.*
- **Tactic: Privilege Escalation**
  - *T1068 – Exploitation for Privilege Escalation.*
  - *T1078 – Valid Accounts.*
- **Tactic: Defense Evasion**
  - *T1562 – Impair Defenses.*
  - *T1027 – Obfuscated Files or Information.*
- **Tactic: Credential Access**
  - *T1003 – OS Credential Dumping (LSASS).*
- **Tactic: Lateral Movement**
  - *T1021.001 – Remote Desktop Protocol (RDP).*
  - *T1021.002 – SMB/Windows Admin Shares.*
- **Tactic: Impact**
  - *T1486 – Data Encrypted for Impact.*
  - *T1490 – Inhibit System Recovery.*