Incident Handling: Suspicious Use of PowerShell Script by Internal Host

---

Scenario

You are a level one security operations center (SOC) analyst at a healthcare organisation. You have received an alert from the endpoint detection and response (EDR) system about unusual PowerShell activity initiated by an internal host.

You investigate the alert and discover that a user executed a PowerShell command that connected to an external IP address and downloaded a script via Invoke-WebRequest. This script was saved locally with a .ps1 extension and then executed. The downloaded script is heavily obfuscated and attempts to establish persistence by modifying registry keys.

Hashing is used to identify the file and compare it across threat intelligence sources. Now that you have the file hash, you will use **VirusTotal** to uncover additional Indicators of Compromise (IoCs) and understand the broader threat.

Date:
July 16th, 2024

Entry:
#1

Description:
This incident occurred in the **Detection and Analysis** phase.

The scenario allows me to investigate suspicious use of PowerShell, a common technique in post-exploitation activity.

I identified a potential LOLBin attack and used the hash to look for existing threat intel.

SHA256 file hash:
f8f9ac66dc72e8c5a74ec6b5790e8f7df2376f86e9399b6f9c39c1099f282d32

Tool(s) used:

- **VirusTotal**: To analyse the file hash and identify known threat patterns.
- **EDR platform (e.g., Microsoft Defender ATP)**: For endpoint visibility and command line capture.
- **Sysmon logs via SIEM**: To trace registry and network activity.

The 5 W's

- **Who caused the incident?**
  Malicious actor leveraging compromised employee account or insider threat.

- **What happened?**
  Obfuscated PowerShell script was downloaded from an external server, saved, and executed on an endpoint.

- **When did the incident occur?**
  3:47 p.m. - EDR flagged suspicious Invoke-WebRequest activity followed by script execution.

- **Where did the incident happen?**
  Internal host within the healthcare company's main office in the Finance department.

- **Why did the incident happen?**
  Either an attacker gained access via phishing or poor credentials, or the employee downloaded the file unknowingly.

Additional notes:

- **How to prevent this from happening?**
  Implement application control, block PowerShell for non-admin users, and educate staff on suspicious scripts.

- **Should this be escalated?**
  Yes. This behavior may indicate **Command and Control** (C2) or the beginning of lateral movement. It should be escalated to a **Level 2 SOC Analyst** for deeper forensic investigation.

Date:
September 16th, 2024

Entry:
#2

Description:
This entry involves the application of a **playbook for suspicious script execution**. Though playbooks are written during the **Preparation** phase, they are actively used during Detection, Containment, and Eradication.

Tool(s) used:

- Playbook for suspicious scripting activity
- Ticketing system (Jira)

The 5 W's

- **Who caused the incident?**
  Attacker using LOLBin to maintain stealth.

- **What happened?**
  Ticket ID A-PS44ZT created. Alert confirmed use of obfuscated PowerShell. EDR flagged attempts to modify registry keys for persistence.

- **When did the incident occur?**
  September 16th, 2024 - initial detection at 3:47 p.m., follow-up investigation at 4:30 p.m.

- **Where did the incident happen?**
  Healthcare organisation, Finance department workstation.

- **Why did the incident happen?**
  Endpoint allowed unmonitored script execution and access to PowerShell.

Ticketing:

Ticket ID	Alert Message	Severity	Details	Ticket Status
A-PS44ZT	Suspicious PowerShell activity with potential persistence technique.	High.	Potential malware download and execution with registry persistence attempt.	Escalated

---

Ticket comments:

The user workstation was observed executing PowerShell commands with obfuscated content.

The script fetched content from hxxp://45.129.248.102/init.ps1 and attempted to modify the Run registry key under HKCU\Software\Microsoft\Windows\CurrentVersion\Run.
The behavior mimics known tactics associated with initial access or foothold establishment. Escalated for deeper memory and network analysis.

Reflections/Notes for Scenario 3:

- **How many entries are there so far?**
  Two entries.

- **What type of security incident was it?**
  Living off the Land Binary (LOLBin) abuse.

- **What was the attack vector?**
  Script download using PowerShell from a remote server.

- **Recommendation:**
  Enforce strict PowerShell logging (ScriptBlockLogging), restrict script execution policies, and alert on outbound traffic to suspicious IPs.