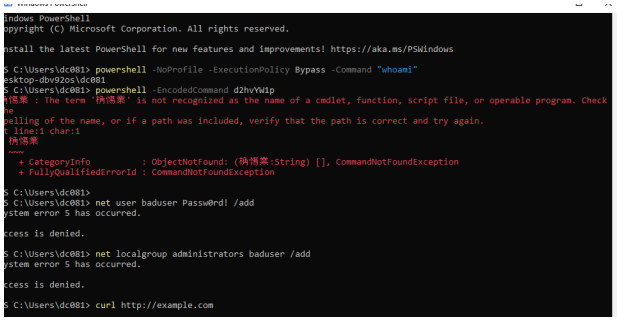
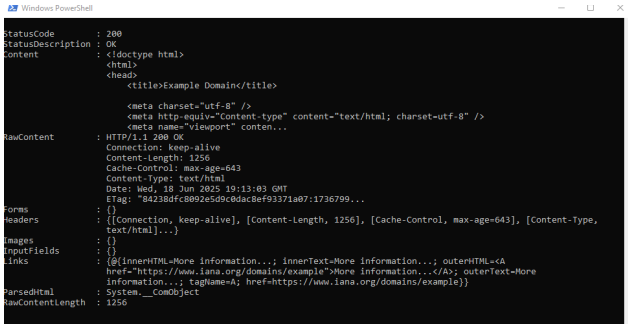
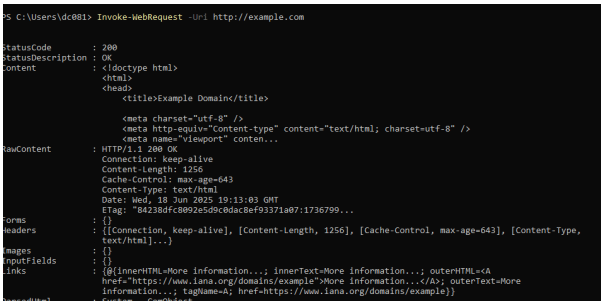
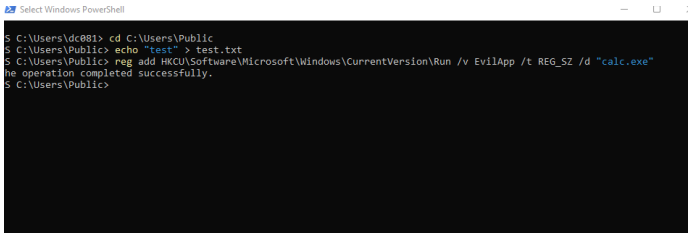
Windows Log Analysis Report
Analyst: Daniel Cruz
Date: June 18, 2025

## Simulated Suspicious Activity




## Logged in event viewer

| | | | | |
|---|---|---|---|---|
| Information | 6/18/2025 3:07:12 PM | Sysmon | 1 | Process Create (rule: Pro... |
| Information | 6/18/2025 3:11:39 PM | Sysmon | 8 | CreateRemoteThread de... |
| Information | 6/18/2025 3:11:42 PM | Sysmon | 1 | Process Create (rule: Pro... |
| Information | 6/18/2025 3:11:43 PM | Sysmon | 11 | File created (rule: FileCre... |
| Information | 6/18/2025 3:11:45 PM | Sysmon | 1 | Process Create (rule: Pro... |
| Information | 6/18/2025 3:11:45 PM | Sysmon | 11 | File created (rule: FileCre... |
| Information | 6/18/2025 3:11:45 PM | Sysmon | 1 | Process Create (rule: Pro... |
| Information | 6/18/2025 3:11:55 PM | Sysmon | 1 | Process Create (rule: Pro... |
| Information | 6/18/2025 3:11:55 PM | Sysmon | 11 | File created (rule: FileCre... |
| Information | 6/18/2025 3:12:46 PM | Sysmon | 1 | Process Create (rule: Pro... |
| Information | 6/18/2025 3:12:47 PM | Sysmon | 1 | Process Create (rule: Pro... |
| Information | 6/18/2025 3:12:47 PM | Sysmon | 1 | Process Create (rule: Pro... |
| Information | 6/18/2025 3:12:51 PM | Sysmon | 1 | Process Create (rule: Pro... |
| Information | 6/18/2025 3:12:51 PM | Sysmon | 1 | Process Create (rule: Pro... |
| Information | 6/18/2025 3:13:21 PM | Sysmon | 1 | Process Create (rule: Pro... |
| Information | 6/18/2025 3:13:21 PM | Sysmon | 11 | File created (rule: FileCre... |
| Information | 6/18/2025 3:13:46 PM | Sysmon | 1 | Process Create (rule: Pro... |
| Information | 6/18/2025 3:13:46 PM | Sysmon | 13 | Registry value set (rule: ... |
| Information | 6/18/2025 3:13:56 PM | Sysmon | 13 | Registry value set (rule: ... |
| Information | 6/18/2025 3:14:51 PM | Sysmon | 1 | Process Create (rule: Pro... |
| Information | 6/18/2025 3:14:51 PM | Sysmon | 1 | Process Create (rule: Pro... |
| Information | 6/18/2025 3:14:51 PM | Sysmon | 1 | Process Create (rule: Pro... |

## Suspicious Activity Simulation and Analysis

### Event ID 1 — Malicious Scheduled Task Creation

Image: schtasks.exe
Command Line:
"C:\Windows\system32\schtasks.exe" /create /tn MaliciousTask /tr "cmd.exe /c whoami" /sc hourly
Parent Image: powershell.exe
Parent Command Line:
"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"

Analysis:
Upon reviewing Event ID 11, I checked the surrounding Event ID 1 logs and found a schtasks.exe process creating the same malicious task. The parent process was PowerShell, indicating script based persistence.

Actions Taken:

Verified the task using schtasks

Confirmed the hourly schedule and command

Validated that whoami.exe was a legitimate system binary

Removed the task using schtasks

Escalated to Tier 2 or IR and recommended detection logic for schtasks.exe spawned by PowerShell

Event ID 1 — Registry Persistence via reg.exe
Image: reg.exe
Command Line:
reg add HKCU\Software\Microsoft\Windows\CurrentVersion\Run /v EvilApp /t REG_SZ /d calc.exe /f
Parent Image: powershell.exe
Parent Command Line: powershell.exe

Analysis:
Event ID 13 showed registry key persistence. Correlated Event ID 1 logs revealed that reg.exe set the same key with PowerShell as the parent, confirming a script-based technique.

Actions Taken:

Validated calc.exe integrity

Removed the persistence key

Escalated to Tier 2 or IR team

Event ID 11 — Suspicious File Creation in System32
Target Filename: C:\Windows\System32\Tasks\MaliciousTask
Image: svchost.exe
User: NT AUTHORITY\SYSTEM

Analysis:
A system process created a file in a protected directory. This is suspicious, in combination with the task name.

Actions Taken:

Retrieved file hash using PowerShell

Verified the hash on VirusTotal

Quarantined the file (simulated)

Correlated with Event ID 1 for full context

Escalated to Tier 2 SOC Analyst

Event ID 11 — File Creation in Temp Directory
Target Filename: C:\Users\Daniel\AppData\Local\Temp__PSScriptPolicyTest_rnh5dnnq.sjw.ps1
Image: powershell.exe
User: Daniel (local)

Analysis:
A PowerShell process dropped a script in the Temp directory. This is common with initial access payloads or post-exploitation tools.

Actions Taken:

Verified file origin and execution context

Collected hash and submitted to VirusTotal

Quarantined the file

Investigated surrounding Event ID 1 logs

Escalated to Tier 2

Event ID 13 — Registry Key Creation (EvilApp)
Rule Name: T1060 (RunKey)

Event Type: SetValue

Image: reg.exe

Target Object:
HKCU\Software\Microsoft\Windows\CurrentVersion\Run\EvilApp
Details: calc.exe

Analysis:
A persistence key was added via reg.exe, instructing calc.exe to run at login. While calc.exe is benign, attackers commonly replace or abuse trusted binaries in this manner. Actions Taken: Manually reviewed the registry key Confirmed calc.exe legitimacy Removed the key Investigated related event IDs (1, 11, and 4720)