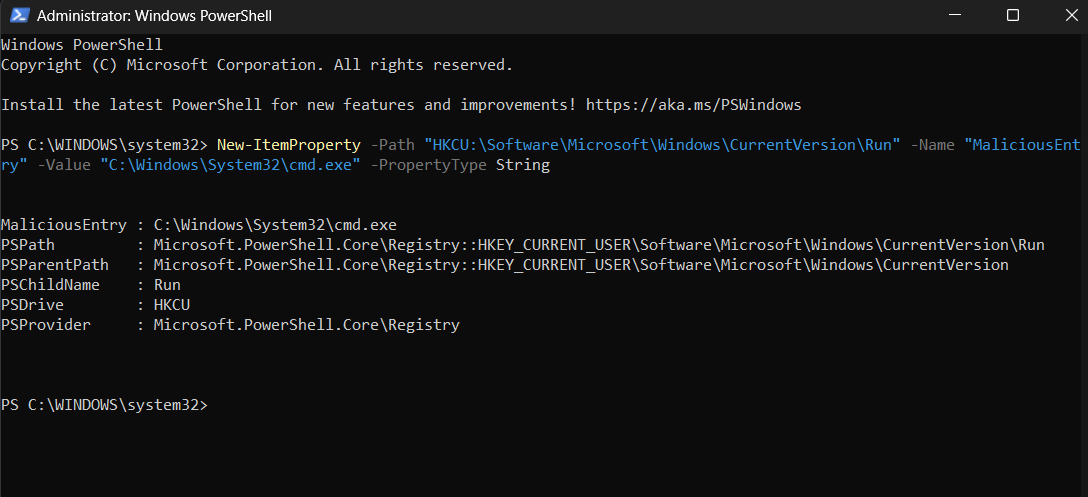
**Step 1:**

1. Open PowerShell (Run as Administrator).
2. Run the following command to modify the Windows Run Key (often used for persistence by malware):

New-ItemProperty -Path "HKCU:\Software\Microsoft\Windows\CurrentVersion\Run" -Name "MaliciousEntry" -Value "C:\Windows\System32\cmd.exe" -PropertyType String

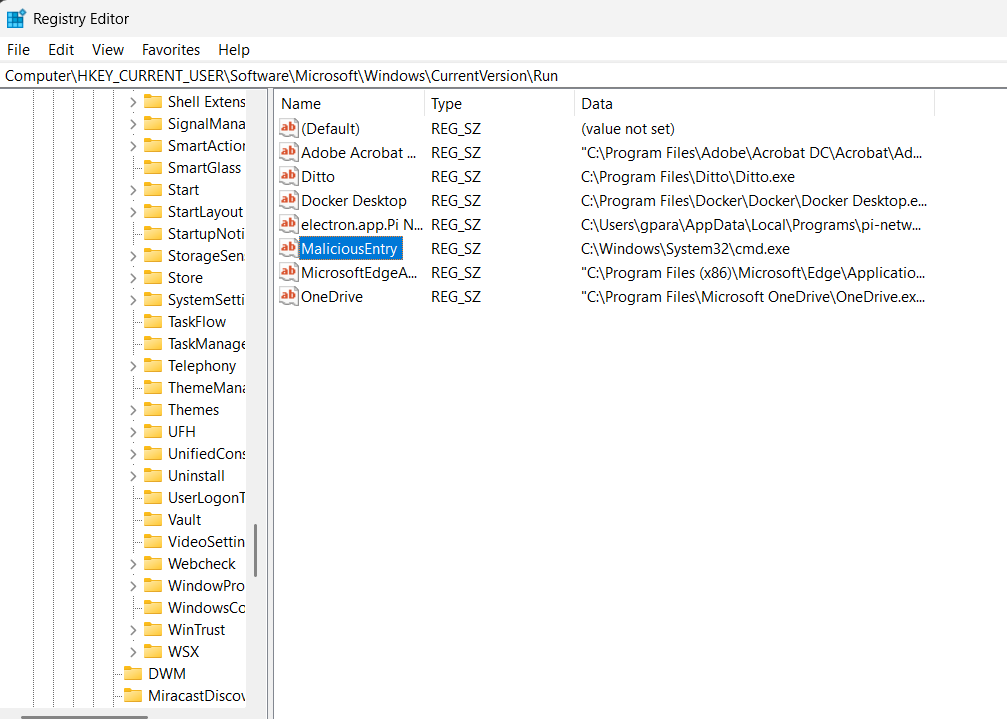


* Attackers often use this technique to maintain persistence on compromised machines. Step 2: Detect the Registry Modification Using Registry Editor

1. Open Registry Editor (Win + R, type regedit, press Enter).
2. Navigate to:

HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Run

1. Look for the "MaliciousEntry" key and verify that its value is set to cmd.exe.



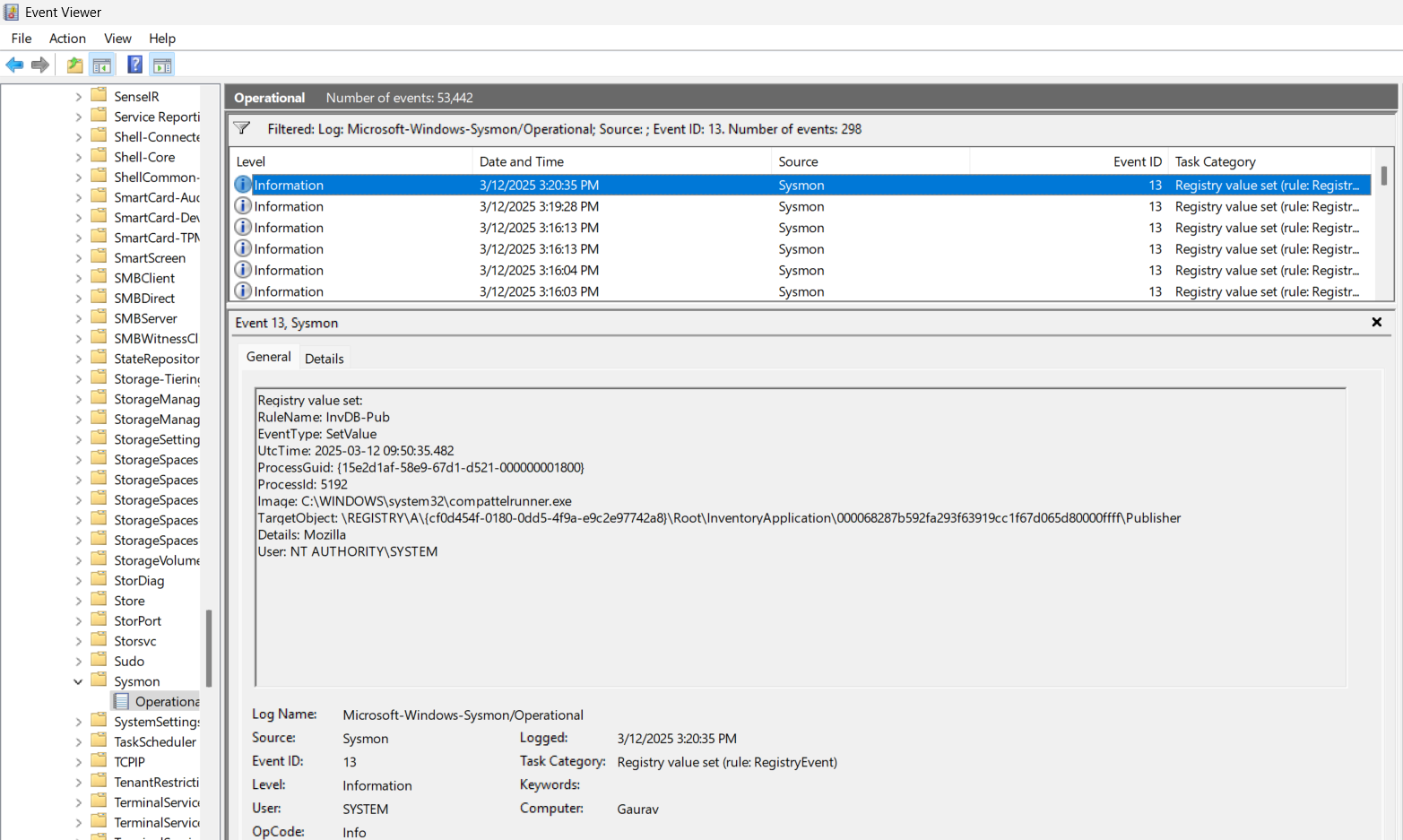
**Step 3: Detect Registry Changes Using Sysmon Logs**

1. Open Event Viewer (Win + R, type eventvwr.msc, press Enter).
2. Navigate to:

Applications and Services Logs → Microsoft → Windows → Sysmon → Operational

1. Click Filter Current Log and enter Event ID 13 (Registry Value Set).
2. Look for:

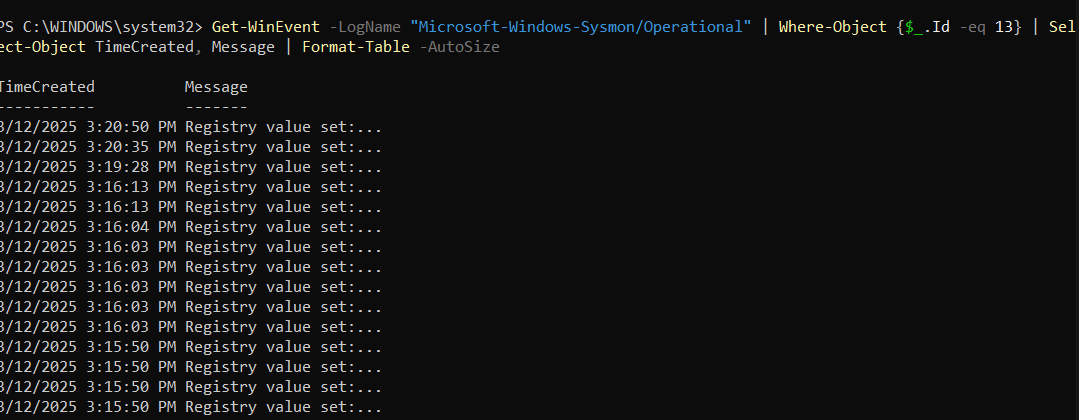
* Registry Key Path: HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Run
* Value Name: MaliciousEntry
* Value Data: C:\Windows\System32\cmd.exe
* Process Responsible: powershell.exe



**Step 4: Retrieve Registry Modification Logs Using PowerShell**

Instead of using Event Viewer, use PowerShell to extract Sysmon registry modification logs:

Get-WinEvent -LogName "Microsoft-Windows-Sysmon/Operational" | Where-Object {$\_.Id -eq 13} | Select-Object TimeCreated, Message | Format-Table -AutoSize



**Step 5: Remove the Suspicious Registry Entry**

To clean up the simulated registry modification, run:

Remove-ItemProperty -Path "HKCU:\Software\Microsoft\Windows\CurrentVersion\Run" -Name "MaliciousEntry"

* This removes the persistence entry from the registry.