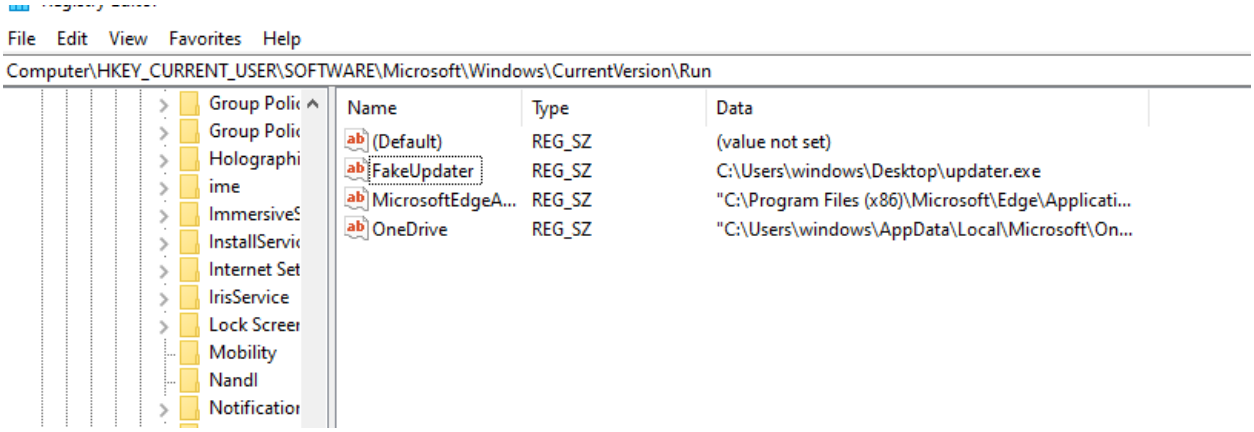
Scenario 3: Persistence via Registry Run Keys

Objective:

Simulate a threat actor establishing **persistence** on a Windows system by adding a **malicious script or executable** to a **Registry Run key**, ensuring it executes upon system reboot or user login.

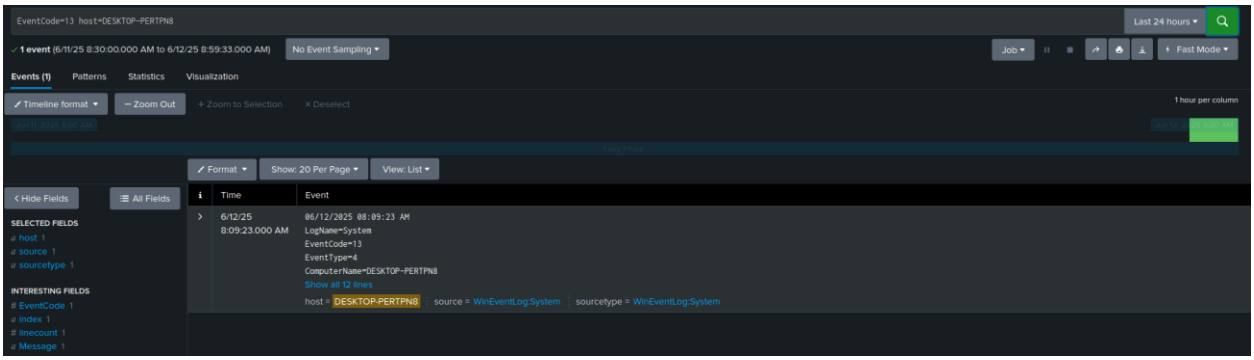
Step 1: Simulate Registry Persistence on Windows

- We'll add a fake malicious entry manually to simulate persistence.

- Set-ItemProperty -Path "HKCU:\Software\Microsoft\Windows\CurrentVersion\Run" -Name "FakeUpdater" -Value "C:\Users\<USERNAME>\Desktop\updater.exe"
- 

Event Type	**Event ID**	**Source**
Registry modification	**13**	Sysmon
Process creation (later)	**1**	Sysmon

Step 2: Monitor Registry Modification Logs in Splunk



Step 3: Set Up Detection Alert for Registry Persistence