

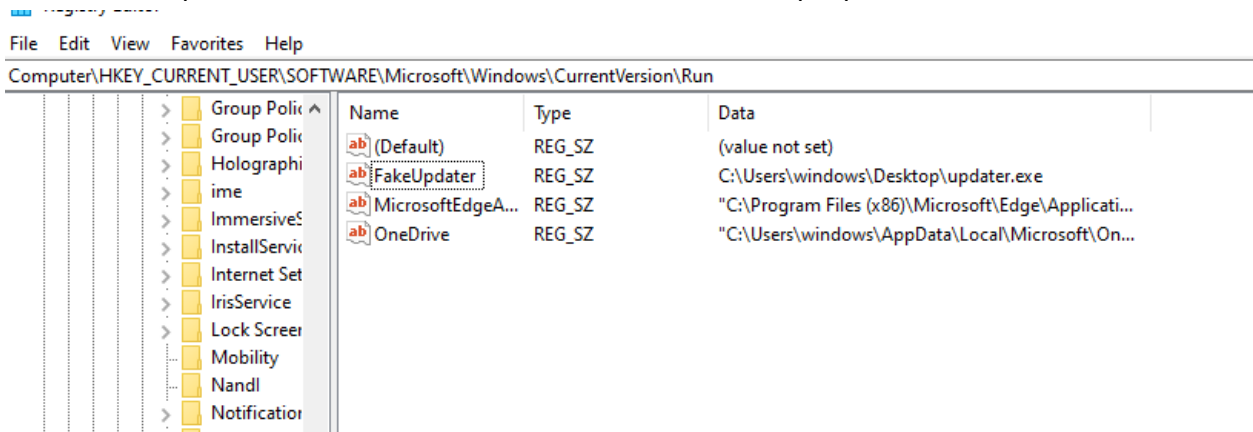
Scenario 3: Persistence via Registry Run Keys

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

EventCode=13 host=DESKTOP-PERTPN8

Last 24 hours

✓ 1 event (6/12/25 8:30:00.000 AM to 6/12/25 8:59:33.000 AM) No Event Sampling

Job

Fast Mode

Events (1) Patterns Statistics Visualization

Timeline format Zoom Out Zoom to Selection Deselect

1 hour per column

6/12/25 8:30:00 AM

Format Show: 20 Per Page View: List

Time	Event
6/12/25 8:09:23.000 AM	LogName=System EventCode=13 ComputerName=DESKTOP-PERTPN8 Show all 12 lines host = DESKTOP-PERTPN8 source = WinEventLogSystem sourcetype = WinEventLog:System

SELECTED FIELDS

- # host: 1
- # source: 1
- # sourcetype: 1

INTERESTING FIELDS

- # EventCode: 1
- # index: 1
- # linecount: 1
- # Message: 1

Step 3: Set Up Detection Alert for Registry Persistence

splunk-enterprise Apps

Administrator Messages Settings Activity Help Find

Search Analytics Datasets Reports Alerts Dashboards

Search & Reporting

Alert for Registry Persistence

Edit

Enabled: Yes [Disable](#)

App: search

Permissions: Private, Owned by splunk_admin, [Edit](#)

Modified: Jun 12, 2025 9:14:37 AM

Alert Type: Scheduled, Weekly, Monday at 6:00, [Edit](#)

Trigger Condition: Number of Results is > 5, [Edit](#)

Actions: 1 Action [Add to Triggered Alerts](#)

There are no fired events for this alert.