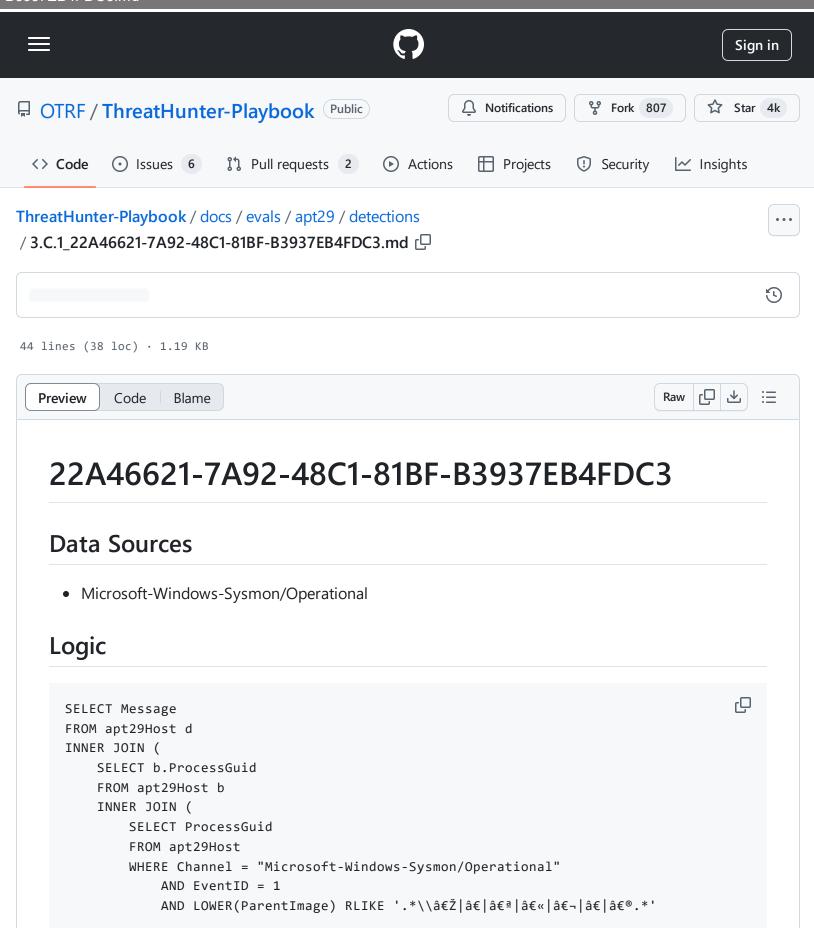
ThreatHunter-Playbook/docs/evals/apt29/detections/3.C.1\_22A46621-7A92-48C1-81BF-B3937EB4FDC3.md at 2d4257f630f4c9770f78d0c1df059f891ffc3fec · OTRF/ThreatHunter-Playbook · GitHub - 31/10/2024 19:55 https://github.com/OTRF/ThreatHunter-

Playbook/blob/2d4257f630f4c9770f78d0c1df059f891ffc3fec/docs/evals/apt29/detections/3.C.1\_22A46621-7A92-48C1-81BF-B3937EB4FDC3.md



ThreatHunter-Playbook/docs/evals/apt29/detections/3.C.1\_22A46621-7A92-48C1-81BF-B3937EB4FDC3.md at 2d4257f630f4c9770f78d0c1df059f891ffc3fec · OTRF/ThreatHunter-Playbook · GitHub - 31/10/2024 19:55 https://github.com/OTRF/ThreatHunter-

Playbook/blob/2d4257f630f4c9770f78d0c1df059f891ffc3fec/docs/evals/apt29/detections/3.C.1\_22A46621-7A92-48C1-81BF-B3937EB4FDC3.md

```
    ON b.ParentProcessGuid = a.ProcessGuid
    WHERE b.Channel = "Microsoft-Windows-Sysmon/Operational"
        AND b.EventID = 1
) c
ON d.ProcessGuid = c.ProcessGuid
WHERE d.Channel = "Microsoft-Windows-Sysmon/Operational"
    AND d.EventID = 12
AND LOWER(d.TargetObject) RLIKE '.*\\\\\\folder\\\\\\shell\\\\\\open\\\\\\
AND d.Message RLIKE '.*EventType: DeleteKey.*'
```

## Output

```
Registry object added or deleted:
RuleName: -
EventType: DeleteKey
UtcTime: 2020-05-02 02:59:15.911
ProcessGuid: {47ab858c-e1f8-5eac-bc03-000000000400}
ProcessId: 3832
Image: C:\windows\System32\WindowsPowerShell\v1.0\powershell.exe
TargetObject: HKU\S-1-5-21-1830255721-3727074217-2423397540-1107_Classes\Folder\sho
```