22A46621-7A92-48C1-81BF-B3937EB4FDC3

Data Sources

- Microsoft-Windows-Sysmon/Operational

Logic

```
SELECT Message
FROM apt29Host d
INNER JOIN (
    SELECT b.ProcessGuid
    FROM apt29Host b
    INNER JOIN (
        SELECT ProcessGuid
        FROM apt29Host
        WHERE Channel = "Microsoft-Windows-Sysmon/Operational"
            AND EventID = 1
            AND LOWER(ParentImage) RLIKE '.*\\â€Ž|â€|â€ª|â€«|â€¬|â€|â€®.*'
```

```
    ) a
    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\sh
```