53 lines (47 loc) · 1.48 KB

Preview Code Blame Raw

611FCA99-97D0-4873-9E51-1C1BA2DBB40D

Data Sources

- Microsoft-Windows-Sysmon/Operational

Logic

```
SELECT Message
FROM apt29Host f
INNER JOIN (
    SELECT d.ProcessGuid
    FROM apt29Host d
    INNER JOIN (
      SELECT a.ProcessGuid, a.ParentProcessGuid
      FROM apt29Host a
      INNER JOIN (
        SELECT ProcessGuid
        FROM apt29Host
        WHERE Channel = "Microsoft-Windows-Sysmon/Operational"
            AND EventID = 1
            AND LOWER(Image) LIKE "%control.exe"
            AND LOWER(ParentImage) LIKE "%sdclt.exe"
      ) b
      ON a.ParentProcessGuid = b.ProcessGuid
      WHERE a.Channel = "Microsoft-Windows-Sysmon/Operational"
        AND a.EventID = 1
        AND a.IntegrityLevel = "High"
    ) c
    ON d.ParentProcessGuid= c.ProcessGuid
    WHERE d.Channel = "Microsoft-Windows-Sysmon/Operational"
      AND d.EventID = 1
      AND d.Image LIKE '%powershell.exe'
) e
ON f.ProcessGuid = e.ProcessGuid
WHERE f.Channel = "Microsoft-Windows-Sysmon/Operational"
    AND f.EventID = 11
    AND f.TargetFilename RLIKE '.*\\\\\\\\ProgramData\\\\\\\\Microsoft\\\\\\\\Wind
```

Output

```
File created:
RuleName: -
UtcTime: 2020-05-02 03:04:23.681
ProcessGuid: {47ab858c-e23d-5eac-c603-000000000400}
ProcessId: 3876
Image: C:\windows\system32\WindowsPowerShell\v1.0\powershell.exe
TargetFilename: C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp\hostu
CreationUtcTime: 2020-05-02 03:04:23.681
```