Sign in

OTRF / ThreatHunter-Playbook Public

Notifications Fork 807 Star 4k

Code Issues 6 Pull requests 2 Actions Projects Security Insights

ThreatHunter-Playbook / docs / evals / apt29 / detections / 4.B.4_83D62033-105A-4A02-8B75-DAB52D8D51EC.md

66 lines (59 loc) · 2.01 KB

Preview Code Blame Raw

83D62033-105A-4A02-8B75-DAB52D8D51EC

Data Sources

- Microsoft-Windows-Sysmon/Operational

Logic

```
SELECT Message, g.CommandLine
FROM apt29Host h
INNER JOIN (
  SELECT f.ProcessGuid, f.CommandLine
  FROM apt29Host f
  INNER JOIN (
    SELECT d.ProcessId, 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.ParentProcessGuid = e.ProcessGuid
  WHERE f.Channel = "Microsoft-Windows-Sysmon/Operational"
    AND f.EventID = 1
    AND LOWER(f.Image) LIKE '%sdelete%'
    AND LOWER(f.CommandLine) LIKE '%sysinternalssuite.zip%'
) g
ON h.ProcessGuid = g.ProcessGuid
WHERE h.Channel = "Microsoft-Windows-Sysmon/Operational"
  AND h.EventID = 23
```

Output

```
Message     | File Delete:
RuleName: -
UtcTime: 2020-05-02 03:03:37.794
ProcessGuid: {47ab858c-e305-5eac-d303-000000000400}
ProcessId: 8848
User: DMEVALS\pbeesly
Image: C:\Program Files\SysinternalsSuite\sdelete64.exe
TargetFilename: C:\Users\pbeesZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZ.ZZZ
Hashes: SHA1=A51DE96F19B0314067CCDD2D2A08C316367DC313,MD5=F86BF68DB45C99EDEBBB554A
IsExecutable: false
Archived: true
```

```
  CommandLine | "C:\Program Files\SysinternalsSuite\sdelete64.exe" /accepteula C:\U
```