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.A.3_09F29912-8E93-461E-9E89-3F06F6763383.md

50 lines (42 loc) · 1.35 KB

Preview Code Blame Raw

09F29912-8E93-461E-9E89-3F06F6763383

Data Sources

- Microsoft-Windows-Sysmon/Operational
  * Microsoft-Windows-PowerShell/Operational

Logic

```
SELECT Message
FROM apt29Host f
INNER JOIN (
    SELECT d.ProcessId
    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.ExecutionProcessID = e.ProcessId
WHERE f.Channel = "Microsoft-Windows-PowerShell/Operational"
    AND f.EventID = 4104
    AND LOWER(f.ScriptBlockText) LIKE "%expand-archive%"
```

Output

```
Creating Scriptblock text (1 of 1):
Expand-Archive -LiteralPath "$env:USERPROFILE\Downloads\SysinternalsSuite.zip" -De

ScriptBlock ID: 63fc6cf4-cd9f-4134-9231-51ccb5c7d247
```