






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](#) / [1.A.1_DFD6A782-9BDB-4550-AB6B-525E825B095E.md](#) 






29 lines (23 loc) · 760 Bytes


Preview


Code

Blame

Raw







DFD6A782-9BDB-4550-AB6B-525E825B095E

Data Sources

- Microsoft-Windows-Sysmon/Operational

Logic

```
SELECT Message
FROM apt29Host
WHERE Channel = "Microsoft-Windows-Sysmon/Operational"
      AND EventID = 13
      AND TargetObject RLIKE '.*\\\\\\\\\\\\\\AppCompatFlags\\\\\\\\\\\\\\\\Compatibility Assistant\\'
```

Output

Registry value set:

RuleName: -

EventType: SetValue

UtcTime: 2020-05-02 03:01:29.278

ProcessGuid: {47ab858c-cc06-5eac-9402-000000000400}

ProcessId: 1144

Image: C:\windows\system32\svchost.exe

TargetObject: HKU\S-1-5-21-1830255721-3727074217-2423397540-1107\Software\Microsoft

Details: Binary Data

