






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](#) / [3.B.2_C36B49B5-DF58-4A34-9FE9-56189B9DEFEA.md](#) 






45 lines (35 loc) · 917 Bytes


Preview


Code

Blame

Raw








C36B49B5-DF58-4A34-9FE9-56189B9DEFEA

Data Sources

- Security

Logic

```
SELECT Message
FROM apt29Host
WHERE LOWER(Channel) = "security"
      AND EventID = 4688
      AND LOWER(NewProcessName) LIKE "%sdclt.exe"
      AND MandatoryLabel = "S-1-16-12288"
      AND TokenElevationType = "%1937"
```



Output

A new process has been created.



Creator Subject:

Security ID: S-1-5-18
Account Name: SCRANTON\$
Account Domain: DMEVALS
Logon ID: 0x3E7

Target Subject:

Security ID: S-1-5-21-1830255721-3727074217-2423397540-1107
Account Name: pbeesly
Account Domain: DMEVALS
Logon ID: 0x372E81

Process Information:

New Process ID: 0x195c
New Process Name: C:\Windows\System32\sdclt.exe
Token Elevation Type: %%1937
Mandatory Label: S-1-16-12288
Creator Process ID: 0xd98
Creator Process Name: C:\Windows\System32\cmd.exe
Process Command Line: "C:\windows\system32\sdclt.exe"