C10730EA-6345-4934-AA0F-B0EFCA0C4BA6

Data Sources

- Microsoft-Windows-Sysmon/Operational

Logic

```
SELECT Message
FROM apt29Host
WHERE Channel = "Microsoft-Windows-Sysmon/Operational"
    AND EventID = 1
    AND CommandLine RLIKE '.*rundll32.exe.*\\\\\\\\windows\\\\\\\\system32\\\\\\\\
```

Output

```
Process Create:
RuleName: -
UtcTime: 2020-05-02 03:08:50.846
ProcessGuid: {47ab858c-e442-5eac-ec03-000000000400}
ProcessId: 3268
Image: C:\Windows\System32\rundll32.exe
FileVersion: 10.0.18362.1 (WinBuild.160101.0800)
Description: Windows host process (Rundll32)
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: RUNDLL32.EXE
CommandLine: rundll32.exe C:\windows\system32\davclnt.dll,DavSetCookie 192.168.0.4
CurrentDirectory: C:\windows\system32\
User: DMEVALS\pbeesly
LogonGuid: {47ab858c-dabe-5eac-812e-370000000000}
LogonId: 0x372E81
TerminalSessionId: 2
IntegrityLevel: High
Hashes: SHA1=7662A8D2F23C3474DEC6EF8E2B0365B0B86714EE,MD5=F68AF942FD7CCC0E7BAB1A23
ParentProcessGuid: {47ab858c-e43f-5eac-eb03-000000000400}
ParentProcessId: 8984
ParentImage: C:\Windows\System32\svchost.exe
ParentCommandLine: C:\windows\system32\svchost.exe -k LocalService -p -s WebClient
```