Product Solutions Resources Open Source Enterprise Pricing

Sign in Sign up

OTRF / ThreatHunter-Playbook Public

Notifications Fork 807 Star 4k

<> Code Issues 6 Pull requests 2 Actions Projects Security Insights

Files

2d4257f

Go to file

- docs
  - _build
  - evals
    - apt29
      - data
      - detections
        - 1.A.1_204B00B6-A92B-4EF...
        - 1.A.1_52540C1E-DD76-41B...
        - 1.A.1_DFD6A782-9BDB-45...
        - 1.A.2_D94222A0-72F9-4F1...
        - 1.A.2_F4C71BF4-E068-493...
        - 1.A.3_1BAC5645-83CD-4D...
        - 1.A.3_B53A710B-43AB-4B5...
        - 1.A.4_E12B701E-1222-413...
        - 1.B.1_4799C203-573A-49C...
        - 1.B.1_C8D664CD-48EE-466...
        - 1.B.2_43B46661-3407-430...
        - 1.B.2_C1DBF5F2-21D5-45E...
        - 10.A.1_4DABE602-E648-4C...
        - 10.A.1_CB9F90C0-93EA-46...
        - 2.A.1_10C87900-CC2F-4EE...
        - 2.A.1_26F6963D-00D5-466...
        - 2.A.2_EAD989D4-8886-46...
        - 2.A.2_F96EA21C-1EB4-498...
        - 2.A.4_621F8EE7-E9D8-417...
        - 2.A.4_6CDEBEBF-387F-4A4...
        - 2.A.5_76154CEC-1E01-4D3...
        - 3.A.1_64249901-ADF8-4E5...
        - 3.A.2_0F10E1D1-EDF8-4B9...
        - 3.A.2_94F9B4F2-1C52-4A4...
        - 3.B.1_04EB334D-A304-40D...
        - 3.B.2_6C8780E9-E6AF-421...
        - 3.B.2_7a4a8c7e-4238-4db3...
        - 3.B.2_C36B49B5-DF58-4A3...
        - 3.B.2_EE34D18C-0549-4AF...
        - 3.B.2_F7E315BA-6A66-44D...

ThreatHunter-Playbook / docs / evals / apt29 / detections
/ 7.B.4_C10730EA-6345-4934-AA0F-B0EFCA0C4BA6.md

Cyb3rWard0g OTRF reference updates   a5db220 · 4 years ago History

Preview Code Blame   43 lines (37 loc) · 1.39 KB   Raw

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\\\\\\\\system
```

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 1
CurrentDirectory: C:\windows\system32\
User: DMEVALS\pbeesly
LogonGuid: {47ab858c-dabe-5eac-812e-370000000000}
LogonId: 0x372E81
TerminalSessionId: 2
IntegrityLevel: High
Hashes: SHA1=7662A8D2F23C3474DEC6EF8E2B0365B0B86714EE,MD5=F68AF942FD7CCC
ParentProcessGuid: {47ab858c-e43f-5eac-eb03-000000000400}
ParentProcessId: 8984
ParentImage: C:\Windows\System32\svchost.exe
ParentCommandLine: C:\windows\system32\svchost.exe -k LocalService -p -s
```