

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 / 3.C.1_22A46621-7A92-48C1-81BF-B3937EB4FDC3.md

History

Preview

Code

Blame

44 lines (38 loc) · 1.19 KB

Raw

22A46621-7A92-48C1-81BF-B3937EB4FDC3

Data Sources

Microsoft-Windows-Sysmon/Operational

Logic

SELECT Message
FROM apt29Host d
INNER JOIN (
 SELECT b.ProcessGuid
 FROM apt29Host b
 INNER JOIN (
 SELECT ProcessGuid
 FROM apt29Host
 WHERE Channel = "Microsoft-Windows-Sysmon/Operational"
 AND EventID = 1
 AND LOWER(ParentImage) RLIKE '.*\\â€Ž|â€|â€³|â€«|â€-|â€|â€®.
) a
 ON b.ParentProcessGuid = a.ProcessGuid
 WHERE b.Channel = "Microsoft-Windows-Sysmon/Operational"
 AND b.EventID = 1
) c
 ON d.ProcessGuid = c.ProcessGuid
 WHERE d.Channel = "Microsoft-Windows-Sysmon/Operational"
 AND d.EventID = 12
 AND LOWER(d.TargetObject) RLIKE '.*\\\\\\\\\\\\\\\\folder\\\\\\\\\\\\\\\\shell\\\\\\\\\\\\\\\\\\\\\\.
 AND d.Message RLIKE '.*EventType: DeleteKey.*'

Output

Registry object added or deleted:
RuleName: -
EventType: DeleteKey
UtcTime: 2020-05-02 02:59:15.911
ProcessGuid: {47ab858c-e1f8-5eac-bc03-000000000400}
ProcessId: 3832
Image: C:\windows\System32\WindowsPowerShell\v1.0\powershell.exe
TargetObject: HKU\S-1-5-21-1830255721-3727074217-2423397540-1107_Classes

Page 1 of 2

3.B.2_d52fe669-55da-49e1...

3.B.3_2E9B9ADC-2426-419...

3.B.3_E209D0C5-5A2B-4AE...

3.C.1_22A46621-7A92-48C...

4.A.1_337EA65D-55A7-489...

4.A.2 B86F90BD-716C-443...