

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 / 6.B.1\_6392C9F1-D975-4F75-8A70-433DEDD7F622.md

Cyb3rWard0g

OTRF reference updates

a5db220 · 4 years ago

History

Preview

Code

Blame

53 lines (47 loc) · 1.35 KB

Raw

6392C9F1-D975-4F75-8A70-433DEDD7F622

Data Sources

Microsoft-Windows-Sysmon/Operational

Logic

SELECT Message  
FROM apt29Host f  
INNER JOIN (  
    SELECT d.ProcessGuid  
    FROM apt29Host d  
    INNER JOIN (  
        SELECT a.ProcessGuid, a.ParentProcessGuid  
        FROM apt29Host a  
        INNER JOIN (  
            SELECT ProcessGuid  
            FROM apt29Host  
            WHERE Channel = "Microsoft-Windows-Sysmon/Operational"  
            AND EventID = 1  
            AND LOWER(Image) LIKE "%control.exe"  
            AND LOWER(ParentImage) LIKE "%sdclt.exe"  
        ) b  
        ON a.ParentProcessGuid = b.ProcessGuid  
        WHERE a.Channel = "Microsoft-Windows-Sysmon/Operational"  
        AND a.EventID = 1  
        AND a.IntegrityLevel = "High"  
    ) c  
    ON d.ParentProcessGuid= c.ProcessGuid  
    WHERE d.Channel = "Microsoft-Windows-Sysmon/Operational"  
    AND d.EventID = 1  
    AND d.Image LIKE '%powershell.exe'  
    ) e  
ON f.ProcessGuid = e.ProcessGuid  
WHERE f.Channel = "Microsoft-Windows-Sysmon/Operational"  
AND f.EventID = 11  
AND LOWER(f.TargetFilename) LIKE "%.pfx"

Output

File created:  
RuleName: -  
UtcTime: 2020-05-02 03:04:57.460  
ProcessGuid: {47ab858c-e23d-5eac-c603-000000000400}  
ProcessId: 3876

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...

Image: C:\windows\system32\WindowsPowerShell\v1.0\powershell.exe  
TargetFilename: C:\Users\pbeesly\Downloads\coyn5igj.3io.pfx  
CreationUtcTime: 2020-05-02 03:04:57.460