



Sign in

vadim-hunter / Detection-Ideas-Rules

Public

Notifications

Fork 28

Star 178

Code

Issues

Pull requests

Actions

Projects

Security

Insights

Detection-Ideas-Rules / TTPs / Defense Evasion / T1218 - Signed Binary Proxy Execution
/ T1218.003 - CMSTP
/ Procedures.yaml

...



64 lines (64 loc) · 3.32 KB

Code

Blame

Raw



```
1  tactics:
2    - TA0005 - Defense Evasion
3  techniques:
4    - T1218 - Signed Binary Proxy execution
5  subtechniques:
6    - T1218.003 - CMSTP
7  description: >
8    Adversaries may abuse CMSTP to proxy execution of malicious code.
9    The Microsoft Connection Manager Profile Installer (CMSTP.exe) is a command-line program used to
10   CMSTP.exe accepts an installation information file (INF) as a parameter and installs a service pr
11  links:
12    - https://attack.mitre.org/techniques/T1218/003/
13    - https://msitpros.com/?p=3960
14  procedures:
15    procedure T1218.003.001:
16      description: >
17        CMSTP can be abused to run malicious code from specially prepared INF files.
18      detection:
19        ideas:
20          - monitor unusual CMSTP parent processes (office apps, browsers, server apps etc).
21      telemetry:
22        process_create:
23          - Windows EID 4688
```

```
24         - Sysmon EID 1
25         - EDR (PsSetCreateProcessNotifyRoutine)
26     rules: >
27         - Channel:Windows-Security AND EventID:4688 AND NewProcessName:"\\cmstp.exe" AND CommandLin
28           AND ParentProcessName:("\\chrome.exe" OR "\\iexplore.exe" OR "\\winword.exe" OR "\\visio.
29         - Channel:Sysmon AND EventID:1 AND (CommandLine:"*cmstp *" OR Image:"\\csmtmp.exe" OR Origin
30           AND CommandLine:*/s* AND ParentImage:("\\chrome.exe" OR "iexplore.exe" OR "\\winword.exe"
31     ideas:
32         - monitor CMSTP.exe process creation with specific parameters and "bad" folders in command
33     telemetry:
34         process_create:
35             - Windows EID 4688
36             - Sysmon EID 1
37             - EDR (PsSetCreateProcessNotifyRoutine)
38     rules:
39         - Channel:Windows-Security AND EventID:4688 AND NewProcessName:"\\cmstp.exe" AND CommandLin
40           AND CommandLine:("\\Users\\" OR "\\Temp\\" OR "\\ProgramData\\")
41         - Channel:Sysmon AND EventID:1 AND (CommandLine:"*cmstp *" OR Image:"\\csmtmp.exe" OR Origin
42           AND CommandLine:*/s* AND CommandLine:("\\Users\\" OR "\\Temp\\" OR "\\ProgramData\\")
43     ideas:
44         - monitor suspicious images loading by CMSTP.
45     telemetry:
46         image_load:
47             - Sysmon EID 7
48             - EDR (PsSetLoadImageNotifyRoutine)
49     rules:
50         - Channel:Sysmon AND EventID:7 AND Image:"\\cmstp.exe" AND (NOT ImageLoaded:(*.dll OR *.ocx)
51 procedure T1218.003.002:
52     description: >
53         CMSTP.exe may be abused to load and execute DLLs and/or COM scriptlets (SCT) from remote serv
54     detection:
55         ideas:
56             - monitor for outbound network connections initiated by CMSTP.
57     telemetry:
58         network_connection:
59             - Windows EID 5156
60             - Sysmon EID 3
61             - EDR (WFP)
62     rules: >
63         - Channel:Sysmon AND EventID:3 AND Image:"\\cmstp.exe" AND Initiated:true AND DestinationIp
64         - Channel:Windows-Security AND EventID:5156 AND ApplicationName:"\\cmstp.exe" AND Direction
```