Files

02bcbfc

Go to file

KB
TTPs
Command and Control
Credential Access
Defense Evasion
T1070 - Indicator Removal on ...
T1197 - BITS Jobs
T1218 - Signed Binary Proxy E...
Procedures.yaml
T1564 - Hide Artifacts
Discovery
Persistence
Threat Intelligence
Tools
README.md

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

vadim-hunter Update Procedures.yaml 121d74a · 3 years ago History

Code Blame 64 lines (64 loc) · 3.32 KB Raw

```yaml
tactics:
  - TA0005 - Defense Evasion
techniques:
  - T1218 - Signed Binary Proxy execution
subtechniques:
  - T1218.003 - CMSTP
description: >
  Adversaries may abuse CMSTP to proxy execution of malicious code.
  The Microsoft Connection Manager Profile Installer (CMSTP.exe) is a command-line prog
  CMSTP.exe accepts an installation information file (INF) as a parameter and installs
links:
  - https://attack.mitre.org/techniques/T1218/003/
  - https://msitpros.com/?p=3960
procedures:
  procedure T1218.003.001:
    description: >
      CMSTP can be abused to run malicious code from specially prepared INF files.
    detection:
      ideas:
        - monitor unusual CMSTP parent processes (office apps, browsers, server apps et
      telemetry:
        process_create:
          - Windows EID 4688
          - Sysmon EID 1
          - EDR (PsSetCreateProcessNotifyRoutine)
      rules: >
        - Channel:Windows-Security AND EventID:4688 AND NewProcessName:"\\cmstp.exe" AN
          AND ParentProcessName:("\\chrome.exe" OR "\\iexplore.exe" OR "\\winword.exe"
        - Channel:Sysmon AND EventID:1 AND (CommandLine:"*cmstp *" OR Image:"\\csmtp.ex
          AND CommandLine:*/s* AND ParentImage:("\\chrome.exe" OR "iexplore.exe" OR "\\
      ideas:
        - monitor CMSTP.exe process creation with specific parameters and "bad" folders
      telemetry:
        process_create:
          - Windows EID 4688
          - Sysmon EID 1
          - EDR (PsSetCreateProcessNotifyRoutine)
      rules:
        - Channel:Windows-Security AND EventID:4688 AND NewProcessName:"\\cmstp.exe" AN
          AND CommandLine:("\\Users\\" OR "\\Temp\\" OR "\\ProgramData\\")
        - Channel:Sysmon AND EventID:1 AND (CommandLine:"*cmstp *" OR Image:"\\csmtp.ex
          AND CommandLine:*/s* AND CommandLine:("\\Users\\" OR "\\Temp\\" OR "\\Program
      ideas:
        - monitor suspicious images loading by CMSTP.
      telemetry:
        image_load:
          - Sysmon EID 7
          - EDR (PsSetLoadImageNotifyRoutine)
      rules:
        - Channel:Sysmon AND EventID:7 AND Image:"\\cmstp.exe" AND (NOT ImageLoaded:(*.
  procedure T1218.003.002:
    description: >
      CMSTP.exe may be abused to load and execute DLLs and/or COM scriptlets (SCT) from
    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 D
64            - Channel:Windows-Security AND EventID:5156 AND ApplicationName:"\\cmstp.exe" A
```