64 lines (64 loc) · 3.32 KB

Code | Blame | 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 program used to
  CMSTP.exe accepts an installation information file (INF) as a parameter and installs a service pr
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 etc).
      telemetry:
        process_create:
          - Windows EID 4688
```

```
            - Sysmon EID 1
            - EDR (PsSetCreateProcessNotifyRoutine)
        rules: >
          - Channel:Windows-Security AND EventID:4688 AND NewProcessName:"\\cmstp.exe" AND CommandLir
            AND ParentProcessName:("\\chrome.exe" OR "\\iexplore.exe" OR "\\winword.exe" OR "\\visio.
          - Channel:Sysmon AND EventID:1 AND (CommandLine:"*cmstp *" OR Image:"\\csmtp.exe" OR Origir
            AND CommandLine:*/s* AND ParentImage:("\\chrome.exe" OR "iexplore.exe" OR "\\winword.exe"
        ideas:
          - monitor CMSTP.exe process creation with specific parameters and "bad" folders in command
        telemetry:
          process_create:
            - Windows EID 4688
            - Sysmon EID 1
            - EDR (PsSetCreateProcessNotifyRoutine)
        rules:
          - Channel:Windows-Security AND EventID:4688 AND NewProcessName:"\\cmstp.exe" AND CommandLir
            AND CommandLine:("\\Users\\" OR "\\Temp\\" OR "\\ProgramData\\")
          - Channel:Sysmon AND EventID:1 AND (CommandLine:"*cmstp *" OR Image:"\\csmtp.exe" OR Origir
            AND CommandLine:*/s* AND CommandLine:("\\Users\\" OR "\\Temp\\" OR "\\ProgramData\\")
        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:(*.dll OR *.ocx
    procedure T1218.003.002:
      description: >
        CMSTP.exe may be abused to load and execute DLLs and/or COM scriptlets (SCT) from remote serv
      detection:
        ideas:
          - monitor for outbound network connections initiated by CMSTP.
        telemetry:
          network_connection:
            - Windows EID 5156
            - Sysmon EID 3
            - EDR (WFP)
        rules: >
          - Channel:Sysmon AND EventID:3 AND Image:"\\cmstp.exe" AND Initiated:true AND DestinationIp
          - Channel:Windows-Security AND EventID:5156 AND ApplicationName:"\\cmstp.exe" AND Direction
```