README

NetshHelperBeacon

DLL to load from Windows NetShell. Will pop calc and execute shellcode.

Background

It turns out Windows NetShell (netsh) allows loading of external DLLs. But you cant just load any regular DLL. For successful loading netsh requires the InitHelperDll entry point

to exist. Once loaded, the DLL will be execute every time netsh is executed.

I got the idea after reading a blogpost(1) and wanted to verify and test its usefulness by making a PoC that executes Cobalt Strike beacon code.

How to use

- *Yolo mode*: load (x64)Release\NetshHelperBeacon.dll on your production machine
- Fire up Visual studio and import the project
- Read code, modify shellcode, build for your architecture
- Copy (x64)Release\NetshHelpderBeacon.dll to your desired location (c:\windows\system32 is the regular path for netsh DLLs)
- run netsh add helper $PathToYourDll - should return OK and pop calc, but shellcode not yet executed
- run netsh - should pop calc and run your shellcode

Drawbacks

- Currently spawns a new thread (so netsh remains useful) but will not spawn new process. This means your shellcode will be killed once the netsh process is stopped.
- Only loosely compliant to Microsoft netsh DLL rules. For example the DLL is not registered with a GUID.
- To make it useful for persistence you need to find a way for netsh to run after reboot.

1: http://www.adaptforward.com/2016/09/using-netshell-to-execute-evil-dlls-and-persist-on-a-host/