Files

master

Go to file

- AppLockerBypass
- CERTPL2Hosts
- CopyEAs
- DFIR
- DNS
- ETW
- EnableAllParentPrivileges
- FMAPI
- FakeAMSI
- FakeCmdLine
- GPO
- GetWindowFlag
- HashSrv
- HideSnapshot
- IFilter
- IOCTL_VOLSNAP_SET_MAX_DIFF...
- LSASecretDumper
- LoLBIN
- Locker
- MSI_Payload
- Misc
- Misc2
- NLA
- NTDSdiff
- NTFSObjectID
- NetShRun
- NetstatWithTimestamps
- NoDLP
- NoRebootSvc
- NoRunDll
- NtPowerInformation
- NtRights
- OfflineSAM
- PasswordStealing
  - DHCP
  - NPPSpy

PSBits / PasswordStealing / NPPSpy /

gtworek Update README.md 0cdc4ec · 3 years ago History

Name	Last commit message	Last commit date
..		
ConfigureRegistrySettings.ps1	PowerShell script by @LadhaAleem added	4 years ago
Get-NetworkProviders.ps1	Update Get-NetworkProviders.ps1	4 years ago
NPPSPY.dll	DLL added	4 years ago
NPPSPy.c	TEXT macro instead of hardcoded unicode.	4 years ago
README.md	Update README.md	3 years ago

README.md

Simple (but fully working) code for `NPLogonNotify()`. The function obtains logon data, including cleartext password.

The DLL is detected by AV engines as a "potentially unwanted software" for obvious reason.
You have been warned. And if you want to run it anyway, you can re-compile it (instructions below) after introducing some changes in the source code, or just add an AV exclusion.

Installation:

1. Copy NPPSpy.dll to the System32 folder
2. Add `"NPPSpy"` at the end of the `"ProviderOrder"` in `HKLM\SYSTEM\CurrentControlSet\Control\NetworkProvider\Order`
3. Create `HKLM\SYSTEM\CurrentControlSet\Services\NPPSpy\NetworkProvider` and set following values:
   - `"Class" = [REG_DWORD]2`
   - `"ProviderPath" = [REG_EXPAND_SZ]"%SystemRoot%\System32\NPPSPY.dll"`
   - `"Name" = [REG_SZ]"NPPSpy"`

OR

Use the ConfigureRegistrySettings.ps1 script (by @LadhaAleem)

Re-logon is required, reboot is not required.

Build it at home

1. From the Start Menu run Visual Studio 2019 -> x64 Native Tools Command Prompt for VS 2019
2. Browse to the folder with your NPPSpy.c
3. Run cl.exe /LD NPPSpy.c

Documentation:

The idea is somewhat documented at https://docs.microsoft.com/en-us/windows/win32/api/npapi/nf-npapi-nplogonnotify

Video

I did my best to explain the flow on a short video: https://youtu.be/ggY3srD9dYs