

Product

Solutions

Resources

Open Source

Enterprise

Pricing

Sign in

Sign up

gtworek / PSBits

Public

Notifications

Fork

525

Star

3.2k

<> Code

Issues

Pull requests

Actions

Projects

Security

Insights

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

ProcessMitigations

ProjFS

PSBits / SIP

gtworek

Add files via upload

2aa885c · 3 years ago

History

Name	Last commit message	Last commit date
..		
GTSIPProvider.c	Create GTSIPProvider.c	3 years ago
GTSIPProvider.dll	Add files via upload	3 years ago
README.md	Create README.md	3 years ago

README.md

The flow of signature checking "asks" for the DLL willing to do the actual job for the specified file. Just out of curiosity I have created a simple DLL reporting who is asking and about which file. And I am sharing the source file and the compiled DLL if you want to play as well.

[DebugView](#) for displaying the result.


And the documentation: [https://docs.microsoft.com/en-us/windows/win32/api/mssip/ns-mssip-sip\\_add\\_newprovider](https://docs.microsoft.com/en-us/windows/win32/api/mssip/ns-mssip-sip_add_newprovider)

Registering with `Regsvr32.exe GTSIPProvider.dll` , unregistering with `Regsvr32.exe /u GTSIPProvider.dll`


Effect visible in the registry under `HKLM\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CryptSIPDllIsMyFileType2`

Page 1 of 2

>


 RDPHoneyPot

>


 RegExport

▼


 SIP



GTSIPProvider.c



GTSIPProvider.dll



README.md