Cn33liz/StarFighters: A JavaScript and VBScript Based Empire Launcher, which runs within their own embedded PowerShell Host.

github.com/Cn33liz/StarFighters

Cn33liz

Cn33liz/
StarFighters

A JavaScript and VBScript Based Empire Launcher, which runs within their own embedded PowerShell Host.

1 Contributor | 4 Issues | 305 Stars | 67 Forks

```
 _________ __                 _____________.__        .__      __
 /   _____//  |_____ ______\_   _____/|__| ____ |  |___/  |_ _____________  ______
 \_____  \\   __\__  \\_  __ \    __)  |  |/ ___\|  |  \   __\/ __ \_  __ \/  ___/
 /        \|  |  / __ \|  | \/     \   |  / /_/  >   Y  \  | \  ___/|  | \/\___ \
/_______  /|__| (____  /__|  \___  /   |__\___  /|___|  /__|  \___  >__|  /____  >
        \/           \/          \/      /_____/      \/          \/           \/
```

A JavaScript and VBScript Based Empire Launcher - by Cn33liz 2017

Both Launchers run within their own embedded PowerShell Host, so we don't need PowerShell.exe. This might be usefull when a company is blocking PowerShell.exe and/or is using a Application Whitelisting solution, but does not block running JS/VBS files.

Empire PowerShell Host build by Cn33liz and embedded within JavaScript using DotNetToJScript from James Forshaw https://github.com/tyranid/DotNetToJScript

```
Usage:

* Setup a new Listener within PowerShell Empire.

* Use the Launcher command to Generate a PowerShell launcher for this listener.

* Copy and Replace the Base64 encoded Launcher Payload within the StarFighter
JavaScript or VBScript file.

* For the JavaScript version use the following Variable:

  var EncodedPayload = "<Paste Encoded Launcher Payload Here>"

* For the VBScript version use the following Variable:

  Dim EncodedPayload: EncodedPayload = "<Paste Encoded Launcher Payload Here>"

* Then run: wscript.exe StarFighter.js or StarFighter.vbs on Target, or DoubleClick
the launchers within Explorer.
```

BlueTeam Advice

- Instead of Blocking PowerShell.exe, make sure you enable PowerShell Constrained Language to all of your users that do not need to use PowerShell for their daily work.
- Use Device Guard and make sure you only allow signed Java, VBS and PowerShell Scripts to prevent Malicious use.