

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

🔍

Sign in

Sign up

📄 mdsecactivebreach / CACTUSTORCH Public

🔔 Notifications

🍴 Fork 224

★ Star 994

<> Code

🔗 Issues 2

🔗 Pull requests 1

🎬 Actions

📁 Projects

🛡 Security

📈 Insights

🔗 master ▾

🔗

📁

🔍 Go to file

<> Code ▾

vysec Merge pull request #5 from Meatballs1/Meatball... 🗨 d663c60 · 7 years ago 🕒 15 Commits

| | | |
|-------------------|------------------------|-------------|
| 📁 CACTUSTORCH.cs | Update TestClass.cs | 7 years ago |
| 📄 CACTUSTORCH.cna | Changes | 7 years ago |
| 📄 CACTUSTORCH.hta | Update CACTUSTORCH.hta | 7 years ago |
| 📄 CACTUSTORCH.js | Update CACTUSTORCH.js | 7 years ago |
| 📄 CACTUSTORCH.jse | Update CACTUSTORCH.jse | 7 years ago |
| 📄 CACTUSTORCH.vba | Changes | 7 years ago |
| 📄 CACTUSTORCH.vbe | Update CACTUSTORCH.vbe | 7 years ago |
| 📄 CACTUSTORCH.vbs | Update CACTUSTORCH.vbs | 7 years ago |
| 📄 README.md | Update README.md | 7 years ago |
| 📄 banner.txt | Initial | 7 years ago |
| 📄 splitvba.py | Initial | 7 years ago |

📖 README

```
( ( ( * ) ) \ ) * ) ( / ( ) \ ) ( ( / (
) \ ) \ ) \ ` ) / ( ( ( ) / ( ` ) / ( ) \ ( ) ( ) / ( ) \ ) \ ( )
(( _ | ( ( _ ) ( ( ( _ ) ( ) _ ) ) \ / ( _ ) ( ) _ | ( _ ) \ / ( _ | ( _ ) ( _ ) \
) \ _ _ ) \ _ ) \ ) \ _ _ ( _ ( ) ) _ ( _ | _ ) ( _ ( ) ) ( _ ) ( _ ) ) \ _ _ _ ( _ )
( / _ _ ( _ ) \ _ ( | / _ _ | _ _ | | / _ _ | | _ _ | / _ _ \ | _ ( / _ _ | | |
| ( _ / _ \ \ | ( _ | | | | | | \ _ \ \ | | | | ( _ ) | / | ( _ | _ _ |
\ _ / / \ \ \ _ | | | \ _ / | _ / | | \ _ / | | \ \ _ | | | |
```

Author and Credits

Author: Vincent Yiu (@vysecurity)

Credits:

- @cn33liz: Inspiration with StarFighters
- @tiraniddo: James Forshaw for DotNet2JScript
- @armitagehacker: Raphael Mudge for idea of selecting 32 bit version on 64 bit architecture machines for injection into
- @_RastaMouse: Testing and giving recommendations around README
- @bspence7337: Testing

Description

About

CACTUSTORCH: Payload Generation for Adversary Simulations

📖 Readme

📈 Activity

★ 994 stars

👁 43 watching

🍴 224 forks

Report repository

Releases

No releases published

Packages

No packages published

Contributors 3

vysecurity Vincent Yiu

Meatballs1 Ben Campbell

rasta-mouse Rasta Mouse

Languages

Visual Basic .NET 61.3%

JavaScript 21.2%

C# 16.2%

Python 1.3%

Page 1 of 2

A JavaScript and VBScript shellcode launcher. This will spawn a 32 bit version of the binary specified and inject shellcode into it.

DotNetToJScript can be found here: <https://github.com/tyranid/DotNetToJScript>

Usage:

- Choose a binary you want to inject into, default "rundll32.exe", you can use notepad.exe, calc.exe for example...
- Generate a 32 bit raw shellcode in whatever framework you want. Tested: Cobalt Strike, Metasploit Framework
- Run: cat payload.bin | base64 -w 0
- For JavaScript: Copy the base64 encoded payload into the code variable below

```
var code = "<base64 encoded 32 bit raw shellcode>";
```

- For VBScript: Copy the base64 encoded payload into the code variable below

```
Dim code: code = "<base64 encoded 32 bit raw shellcode>"
```

- Then run:

wscript.exe CACTUSTORCH.js or wscript.exe CACTUSTORCH.vbs via command line on the target, or double click on the files within Explorer.

- For VBA: Copy the base64 encoded payload into a file such as code.txt
- Run python splitvba.py code.txt output.txt
- Copy output.txt under the following bit so it looks like:

```
code = ""
code = code & "<base64 code in 100 byte chunk"
code = code & "<base64 code in 100 byte chunk"
```



- Copy and paste the whole payload into Word Macro
- Save Word Doc and send off or run it.

CobaltStrike

- Load CACTUSTORCH.cna
- Go to Attack -> Host CACTUSTORCH Payload
- Fill in fields
- File hosted and ready to go!

