

mdsecactivebreach/CACTUSTORCH: CACTUSTORCH: Payload Generation for Adversary Simulations

 github.com/mdsecactivebreach/CACTUSTORCH

mdsecactivebreach

mdsecactivebreach/ CACTUSTORCH



CACTUSTORCH: Payload Generation for Adversary Simulations

 3

Contributors

 2

Issues

 902

Stars

 233

Forks



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

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

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!