

We're continuing to fight for universal access to quality information—and you can help as we continue to make improvements. Will you join in?

https://gist.github.com/code-scrap/d7f152ffcdb3e0b02f7f394f5187f008 Go SEP OCT NOV 2021 26 2022 2023 About this capture

3 captures
16 Oct 2022 - 30 Nov 2022

GitHub Gist Search... All gists Back to GitHub

Instantly share code, notes, and snippets.

code-scrap / README.md Last active 2 days ago

☆ Star 15 Fork 9

<> Code Revisions 7 ☆ Stars 15 Forks 9 Download ZIP

Table Top With Teeth - Training Exercise

README.md Raw

Instructions

The following script is designed to create artifacts that teams can use to hunt, new or interesting capabilities.

The following table top is based on the code here: <https://github.com/code-scrap/DynamicWrapperDotNet>

This script is self-contained. It should dynamically write a DLL to disk and load it in to cscript.exe

To Invoke `cscript.exe stranger_things.js` This example expects a 64bit system. You can modify that if you wat ARM or x86 etc..

Ideas of what to hunt/test:

1. Did the anti-malware engine detect a malicious script
2. Did you observe the DLL written to disk?

4. What artifacts does this approach leave behind?

16 Oct 2022 - 30 Nov 2022

SEP

OCT

NOV

26

2022

2023

▼ About this capture

```
<> stranger things.js
```


Raw



Sign up for free to join this conversation on GitHub. Already have an account? [Sign in to comment](#)

[Terms](#) [Privacy](#) [Security](#) [Status](#) [Docs](#) [Contact GitHub](#) [Pricing](#) [API](#) [Trainin](#)

[3 captures](#)
16 Oct 2022 - 30 Nov 2022

 © 2022 GitHub, Inc.



SEPT2021



◀

OCT
26
2022

▶

NOV2023

▼ About this capture