https://gist.github.com/code-scrap/d7f152ffcdb3e0b02f7f394f5187f008 | Go

SEP | **OCT** | NOV
◀ | **26** | ▶
2021 | **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?

3. Did you observe the DLL/ Module Load

4. What artifacts does this approach leave behind?

5. How might an attacker change this script to evade detection? hint : that 'base....ell'

stranger_things.js

Raw

```javascript
1    var scriptdir = WScript.ScriptFullName.substring(0,WScript.ScriptFullName.lastIndexOf(WScript.ScriptName
2    new ActiveXObject('WScript.Shell').Environment('Process')('TMP') = scriptdir;
3
4
5    // Create Base64 Object, supports encode, decode
6    var Base64={characters:"ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/=",encode:funct
7    //Magic is just a cool way to decode to byte array ;
8    function Magic(r){if(!/^[a-z0-9+/]+={0,2}$/i.test(r)||r.length%4!=0)throw Error("Not base64 string");fo
9    function binaryWriter(res,filename)
10   {var base64decoded=Magic(res);var TextStream=new ActiveXObject('ADODB.Stream');TextStream.Type=2;TextSt
11   // x64 dynwrapx.dll v 2.2.0 http://dynwrapx.script-coding.com/dwx/pages/dynwrapx.php?lang=en
12   var dynwrapX = 'T' +'V'+ 'qQAAMAAAAEAAAA//8AALgAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
13
14   binaryWriter(dynwrapX,scriptdir+"\\export.dll");
15
16
17
18   // You could add a way to drop this dynamically
19   var manifest = '<?xml version="1.0" encoding="UTF-16" standalone="yes"?> <assembly xmlns="urn:schemas-m
20   var ax = new ActiveXObject("Microsoft.Windows.ActCtx");
21   ax.ManifestText = manifest;
22
23   var mdo = ax.CreateObject("DynamicWrapperDotNet");
24   var s = mdo.getValue1("a");
25   WScript.StdOut.WriteLine(s);
26   var t = mdo.getValue1("b");
27   var s = mdo.getValue2();
28   mdo.getValue3();
29   WScript.StdOut.WriteLine(s);
30   WScript.StdOut.WriteLine(t);
```

Terms   Privacy   Security   Status   Docs   Contact GitHub   Pricing   API   Training

© 2022 GitHub, Inc.

3 captures
16 Oct 2022 - 30 Nov 2022

SEP   OCT   NOV
26
2021   2022   2023

About this capture