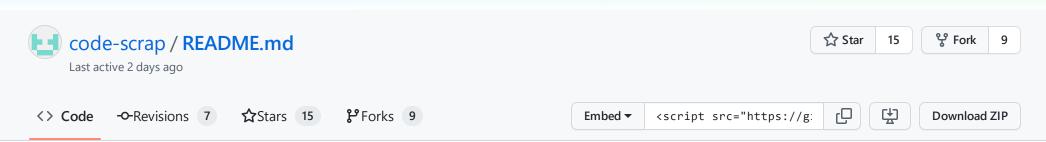


Instantly share code, notes, and snippets.



Raw

Table Top With Teeth - Training Exercise



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 'base64 blob lol'

```
⇔ stranger_things.js
                                                                                                            Raw
   var scriptdir = WScript.ScriptFullName.substring(0,WScript.ScriptFullName.lastIndexOf(WScript.ScriptName)-1)
   new ActiveXObject('WScript.Shell').Environment('Process')('TMP') = scriptdir;
3
4
   // Create Base64 Object, supports encode, decode
    var Base64={characters:"ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/=",encode:function(a){Base64.characters;var
    //Magic is just a cool way to decode to byte array ;
7
   8
   function binaryWriter(res,filename)
9
    {var base64decoded=Magic(res);var TextStream=new ActiveXObject('ADODB.Stream');TextStream.Type=2;TextStream.charSet='iso-8859-1';TextStream'
10
    // x64 dynwrapx.dll v 2.2.0 http://dynwrapx.script-coding.com/dwx/pages/dynwrapx.php?lang=en
11
    12
13
    binaryWriter(dynwrapX,scriptdir+"\\export.dll");
14
15
16
17
   // You could add a way to drop this dynamically
18
    var manifest = '<?xml version="1.0" encoding="UTF-16" standalone="yes"?> <assembly xmlns="urn:schemas-microsoft-com:asm.v1" manifes</pre>
19
    var ax = new ActiveXObject("Microsoft.Windows.ActCtx");
20
    ax.ManifestText = manifest;
21
22
    var mdo = ax.CreateObject("DynamicWrapperDotNet");
23
    var s = mdo.getValue1("a");
24
   WScript.StdOut.WriteLine(s);
25
```

© 2022 GitHub, Inc. Terms Privacy Security Status Docs Contact GitHub Pricing API Training Blog About