7h3w4lk3r/pyback: cross-platform C2 framework in python 2

github.com/7h3w4lk3r/pyback

7h3w4lk3r

7h3w4lk3r/**pyback**

cross-platform C2 framework in python 2

1 Contributor 0 Issues 33 Stars 15 Forks

PYBACK 2.1.0

Object-oriented FUD (if you keep it that way) cross-platform backdoor and CNC written in python 2 with post exploitation modules and encrypted communication.

Features

. Automated obfuscation and packing with pyarmor and pyinstaller
. Cross-platform modules (of course)
. Direct shell access (no need to type extra garbage)
. AES encrypted communication
. Command and Control center
. Can execute commands on all sessions at the same time (AKA Botnet)
. Download/upload files
. Detect virtual machine and sandbox
. Take screenshots
. Dump clipboard
. Keylogger
. Spawn a separate powershell session

. Enable/disable RDP
. Enable/disable UAC
. Easy session interaction and handling
. Windows persistence using registry entries

Installation

you can use python native installation or wine

requirements:

python 2 ,version 2.7.15 or later

to install pyback simply run the setup.py

```
python setup.py
```

or use wine:

```
wine /root/.wine/drive_c/Python27/python.exe setup.py
```

Usage

run the generator script and follow the steps, you can choose to pack and obfuscate the backdoor automatically during the config operation.

```
python generate.py
```

using wine:

```
wine /root/.wine/drive_c/Python27/python.exe generate.py
```

the generated backdoor will be saved in the `output` directory inside pyback folder.

send the backdoor, start the c2 and wait for connections.

```
python cnc.py
```

Usage Tips

. DO NOT USE QUOTES in path names, for example use `file name` instead of `"file name"` when changing directories with `cd`
. If you want to upload a file it should be placed in the same directory as the cnc.py file.
. spawn module will spawn a separate shell using powershell for windows, catch it with netcat.
. While using the CNC shell your prompt will be like this: `[ CNC ] >>>` and it can run local

system commands.
. To get a list of all available commands in CNC or backdoor prompt simply type `help` .
. ANY COMMAND not included in the help banners will be executed as system shell commands so be carefull with that.

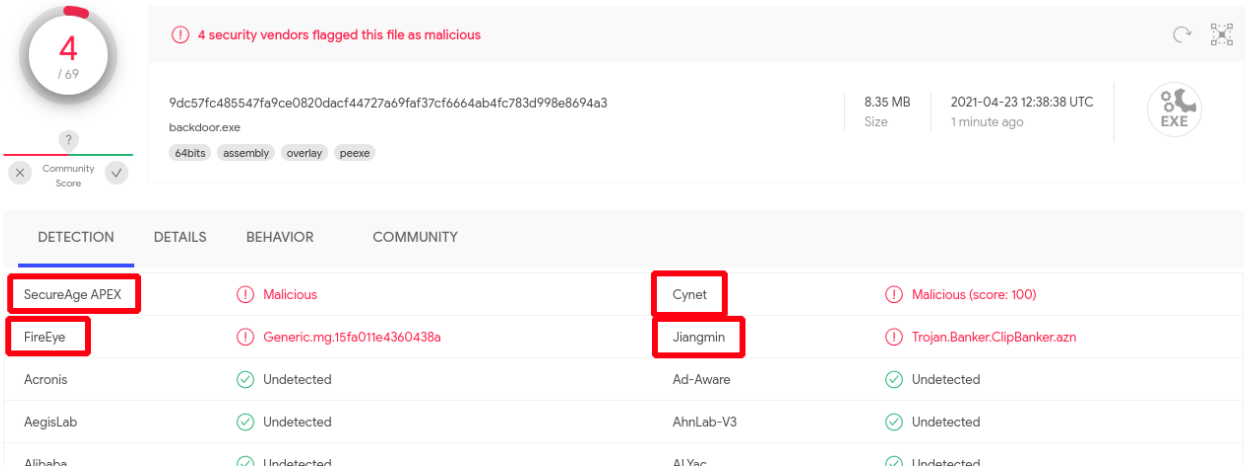
Changelog

see changelogs for different versions here

POC

❗ DO NOT upload this on VirusTotal or anywhere else, I DID IT FOR YOU ❗

Updated in 23 Apr 2021:



Contact

Email: bl4ckr4z3r@gmail.com