

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

By 7h3w4lk3r

Archived: 2026-04-05 16:31:32 UTC

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.

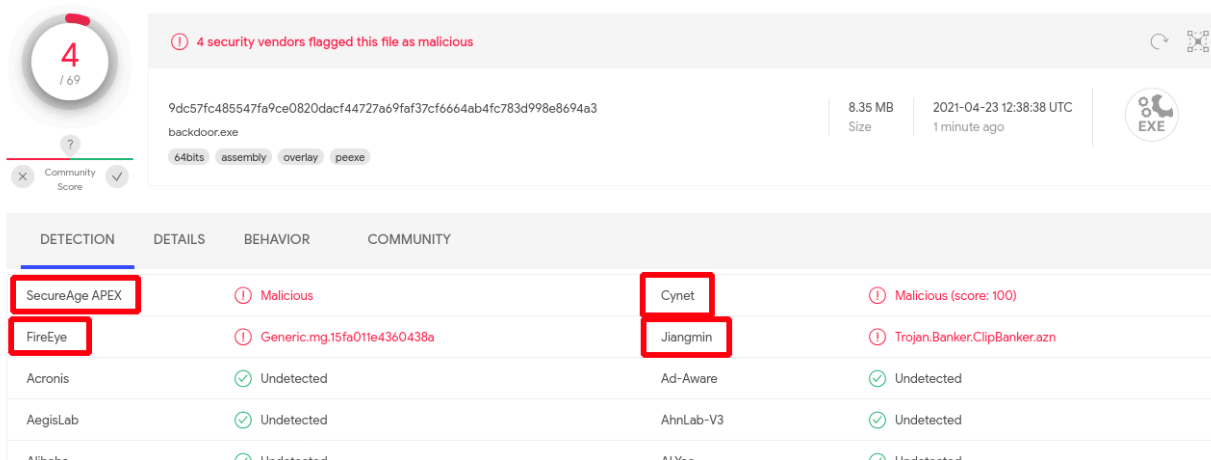
Changelog

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:



The image shows a VirusShare file analysis interface. At the top left, a circular badge displays the number '4' with a red outline, indicating the number of security vendors that flagged the file as malicious. Below this, the file name 'backdoor.exe' is shown along with its SHA-256 hash: '9dc57fc485547fa9ce0820dacf44727a69faf37cf6664ab4fc783d998e8694a3'. The file size is listed as '8.35 MB' and the upload time as '2021-04-23 12:38:38 UTC'. A 'Community Score' of '1/69' is also visible. The interface includes tabs for '64bits', 'assembly', 'overlay', and 'peexe'. Below the header, there are four tabs: 'DETECTION', 'DETAILS', 'BEHAVIOR', and 'COMMUNITY'. The 'DETECTION' tab is active, showing a table of security vendor detections. The table has four columns: 'Vendor', 'Status', 'Signature', and 'Score'. The first two rows are highlighted with red boxes: 'SecureAge APEX' (Malicious) and 'FireEye' (Generic.mg.15fa011e4360438a). Other vendors listed include Acronis, AegisLab, and Alihaha, all marked as 'Undetected'.

DETECTION	DETAILS	BEHAVIOR	COMMUNITY
SecureAge APEX	Malicious	Cynet	Malicious (score: 100)
FireEye	Generic.mg.15fa011e4360438a	Jiangmin	Trojan.Banker.ClipBanker.azn
Acronis	Undetected	Ad-Aware	Undetected
AegisLab	Undetected	AhnLab-V3	Undetected
Alihaha	Undetected	AliYar	Undetected

Contact

Email: bl4ckr4z3r@gmail.com

Source: <https://github.com/7h3w4lk3r/pyback>