nathanlopez/Stitch: Python Remote Administration Tool (RAT)

github.com/nathanlopez/Stitch

nathanlopez

nathanlopez/**Stitch**

Python Remote Administration Tool (RAT)

3 Contributors | 39 Issues | 2k Stars | 567 Forks

DISCLAIMER

Stitch is for education/research purposes only. The author takes NO responsibility and/or liability for how you choose to use any of the tools/source code/any files provided. The author and anyone affiliated with will not be liable for any losses and/or damages in connection with use of ANY files provided with Stitch. By using Stitch or any files included, you understand that you are AGREEING TO USE AT YOUR OWN RISK. Once again Stitch and ALL files included are for EDUCATION and/or RESEARCH purposes ONLY. Stitch is ONLY intended to be used on your own pentesting labs, or with explicit consent from the owner of the property being tested.

About Stitch

A Cross Platform Python Remote Administration Tool:

This is a cross platform python framework which allows you to build custom payloads for Windows, Mac OSX and Linux as well. You are able to select whether the payload binds to a specific IP and port, listens for a connection on a port, option to send an email of system info when the system boots, and option to start keylogger on boot. Payloads created can only run on the OS that they were created on.

Features

Cross Platform Support

- Command and file auto-completion
- Antivirus detection
- Able to turn off/on display monitors
- Hide/unhide files and directories
- View/edit the hosts file
- View all the systems environment variables
- Keylogger with options to view status, start, stop and dump the logs onto your host system
- View the location and other information of the target machine
- Execute custom python scripts which return whatever you print to screen
- Screenshots
- Virtual machine detection
- Download/Upload files to and from the target system
- Attempt to dump the systems password hashes
- Payloads' properties are "disguised" as other known programs

Windows Specific

- Display a user/password dialog box to obtain user password
- Dump passwords saved via Chrome
- Clear the System, Security, and Application logs
- Enable/Disable services such as RDP,UAC, and Windows Defender
- Edit the accessed, created, and modified properties of files
- Create a custom popup box
- View connected webcam and take snapshots
- View past connected wifi connections along with their passwords
- View information about drives connected
- View summary of registry values such as DEP

Mac OSX Specific

- Display a user/password dialog box to obtain user password
- Change the login text at the user's login screen
- Webcam snapshots

Mac OSX/Linux Specific

- SSH from the target machine into another host
- Run sudo commands
- Attempt to bruteforce the user's password using the passwords list found in Tools/

- Webcam snapshots? (untested on Linux)

Implemented Transports

All communication between the host and target is AES encrypted. Every Stitch program generates an AES key which is then put into all payloads. To access a payload the AES keys must match. To connect from a different system running Stitch you must add the key by using the showkey command from the original system and the addkey command on the new system.

Implemented Payload Installers

The "stitchgen" command gives the user the option to create NSIS installers on Windows and Makeself installers on posix machines. For Windows, the installer packages the payload and an elevation exe ,which prevents the firewall prompt and adds persistence, and places the payload on the system. For Mac OSX and Linux, the installer places the payload and attempts to add persistence. To create NSIS installers you must download and install NSIS.

Wiki

> Crash Course of Stitch

Requirements

> Python 2.7

For easy installation run the following command that corresponds to your OS:

```
# for Windows
pip install -r win_requirements.txt

# for Mac OSX
pip install -r osx_requirements.txt

# for Linux
pip install -r lnx_requirements.txt
```

- Pycrypto
- Requests
- Colorama
- PIL

Windows Specific

- Py2exe
- pywin32

Mac OSX Specific

PyObjC

Mac OSX/Linux Specific

- PyInstaller
- pexpect

To Run

```
python main.py
or
./main.py
```

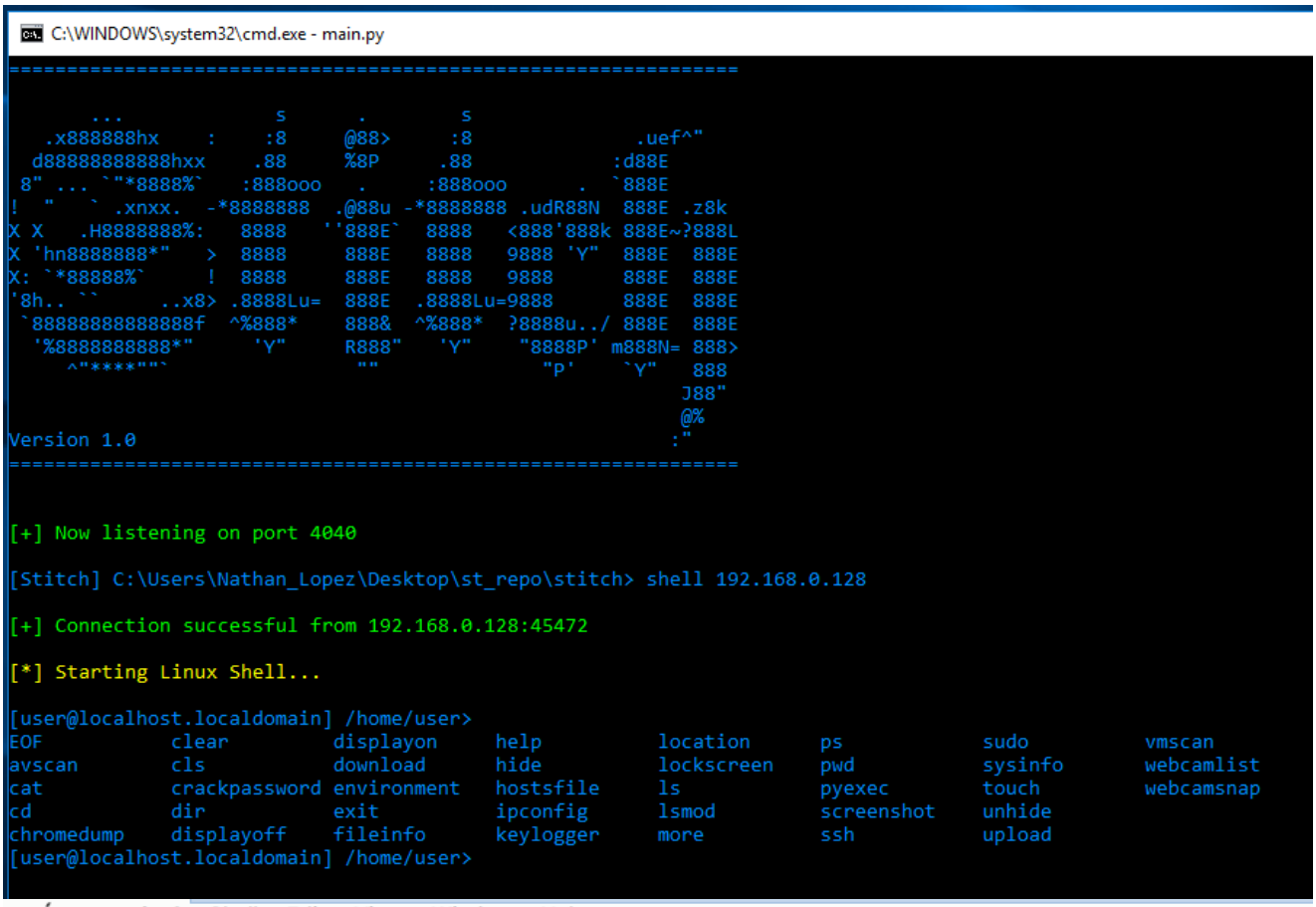
Motivation

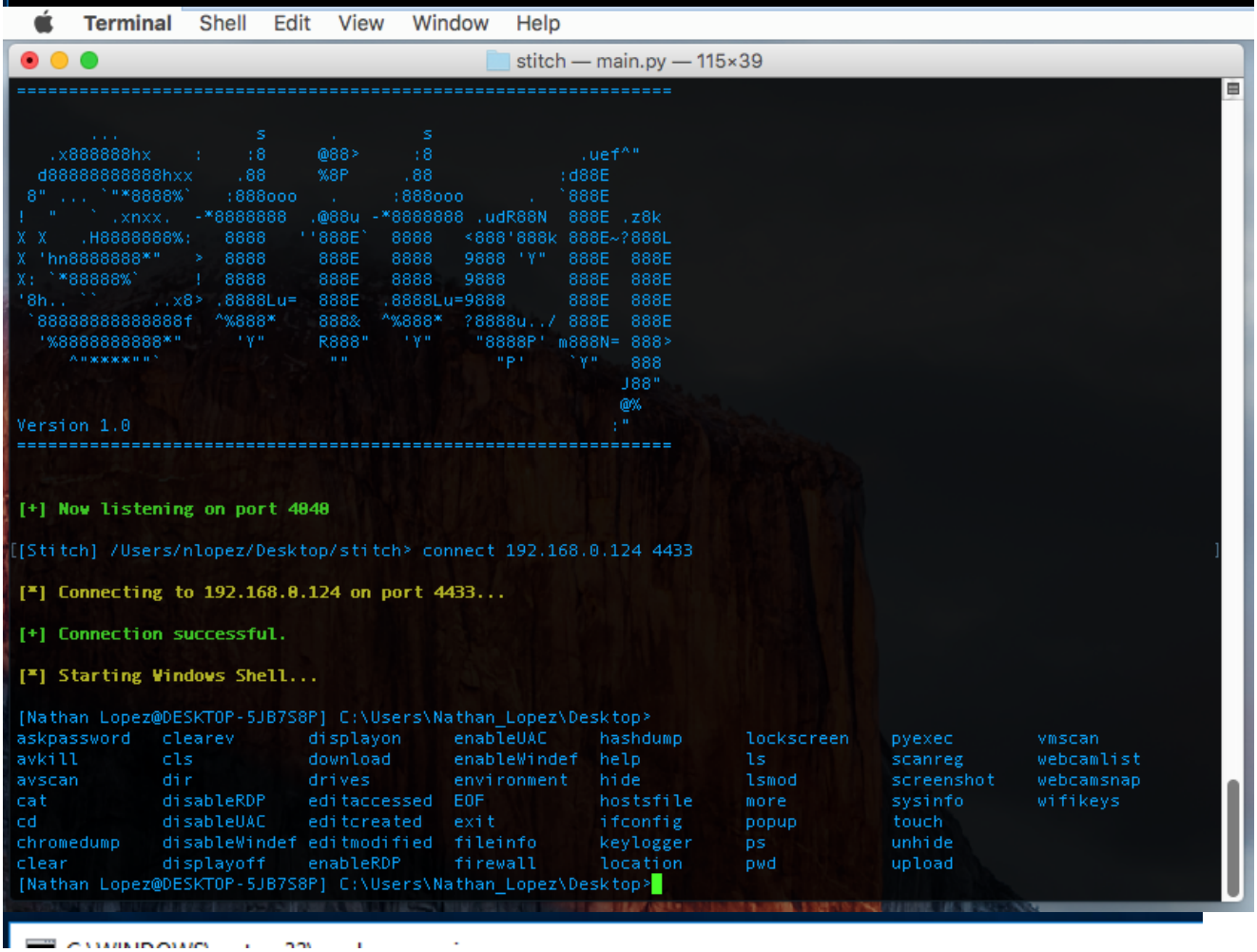
My motivation behind this was to advance my knowledge of python, hacking, and just to see what I could accomplish. Was somewhat discouraged and almost abandoned this project when I found the amazing work done by n1nj4sec, but still decided to put this up since I had already come so far.

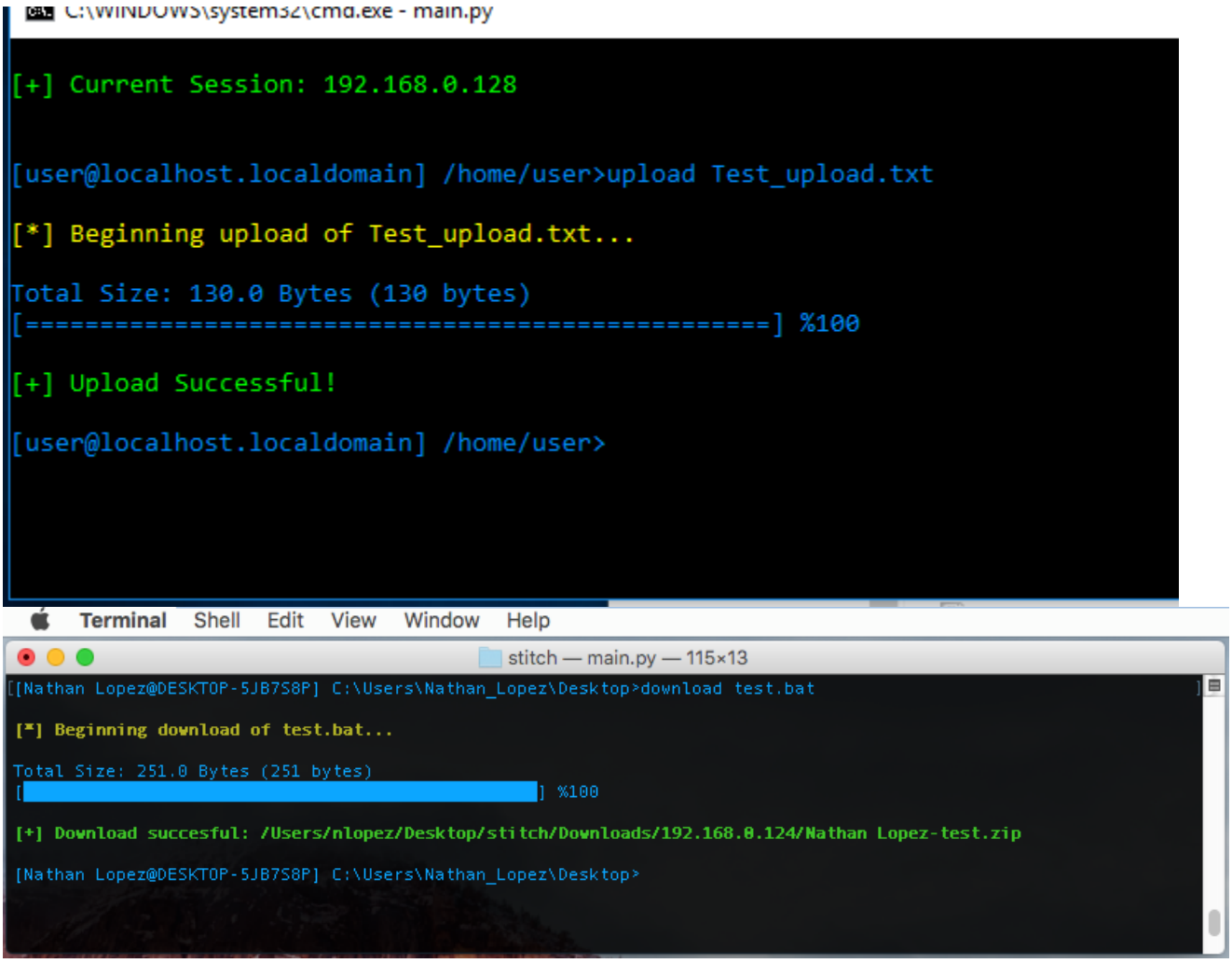
Other open-source Python RATs for Reference

- vesche/basicRAT
- n1nj4sec/pupy

Screenshots


C:\WINDOWS\system32\cmd.exe - main.py
Version 1.0
[+] Now listening on port 4040
[Stitch] C:\Users\Nathan_Lopez\Desktop\st_repo\stitch> shell 192.168.0.128
[+] Connection successful from 192.168.0.128:45472
[*] Starting Linux Shell...
[user@localhost.localdomain] /home/user>
EOF clear displayon help location ps sudo vmscan
avscan cls download hide lockscreen pwd sysinfo webcamlist
cat crackpassword environment hostsfile ls pyexec touch webcamsnap
cd dir exit ipconfig lsmod screenshot unhide
chromedump displayoff fileinfo keylogger more ssh upload
[user@localhost.localdomain] /home/user>


Terminal Shell Edit View Window Help
stitch — main.py — 115×39
Version 1.0
[+] Now listening on port 4040
[[Stitch] /Users/nlopez/Desktop/stitch> connect 192.168.0.124 4433
[*] Connecting to 192.168.8.124 on port 4433...
[+] Connection successful.
[*] Starting Windows Shell...
[Nathan Lopez@DESKTOP-5JB7S8P] C:\Users\Nathan_Lopez\Desktop>
askpassword clearev displayon enableUAC hashdump lockscreen pyexec vmscan
avkill cls download enableWindef help ls scanreg webcamlist
avscan dir drives environment hide lsmod screenshot webcamsnap
cat disableRDP editaccessed EOF hostsfile more sysinfo wifikeys
cd disableUAC editcreated exit ifconfig popup touch
chromedump disableWindef editmodified fileinfo keylogger ps unhide
clear displayoff enableRDP firewall location pwd upload
[Nathan Lopez@DESKTOP-5JB7S8P] C:\Users\Nathan_Lopez\Desktop>



License

See LICENSE