TROJARK USER GUIDE

Table of Contents

Introduction

Trojark is a Python-based, multi-platform, remote-access trojan. Python **does not** have to be installed on the machine as the client is built to a standalone executable with PyInstaller.

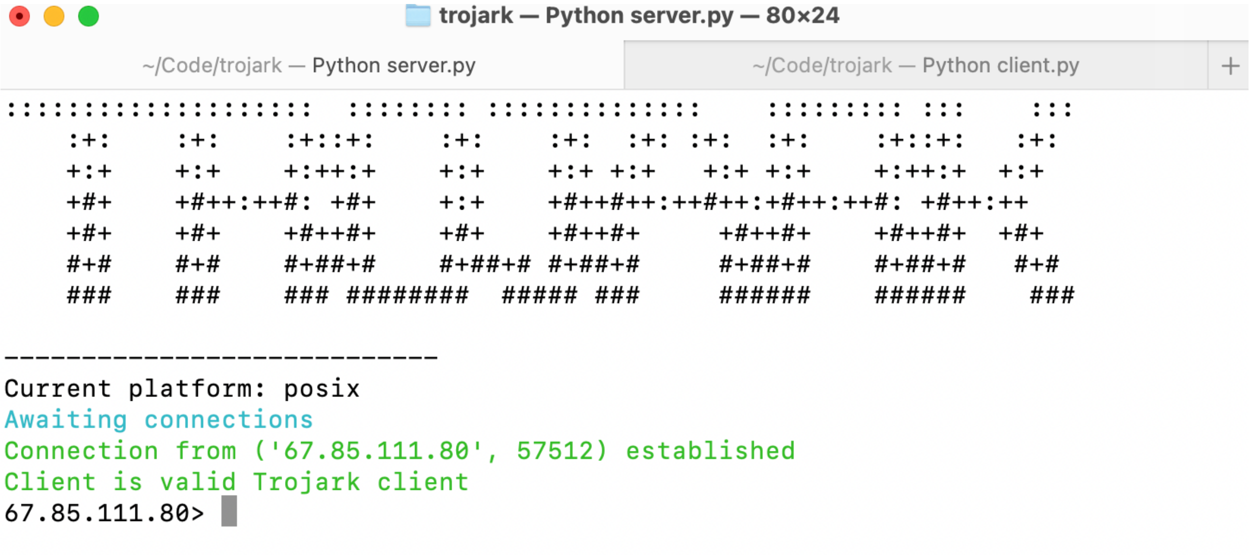
When the client executable is run on the victim's machine, a socket stream is created to a server (with a hard-coded IP address) on port 9258. There is no authentication, but the client must send the message "`trojark`" as its first message to verify that it is a valid client. An algorithm to generate a valid string is planned.

Usage

On the attacker machine, install the requirements with `pip install -r requirements.txt`. Now, make sure that port 9258 is exposed. This can be done through port-forwarding, with a service such as ngrok, or running the server on a VPS and exposing it there. Just make sure that the ngrok URL does not change, because the server is hard coded in the client. If the domain changes, the client will be unable to connect. Therefore, using a VPS with a static IP is recommended.

To build the client into an executable, run `make`. It will be built into the “dist” folder. The server does not have to be an executable; it can just be run with `python server.py`.

Now, the client executable has to be run on the target machine. It is a silent program, so no console will appear. You can make the look less suspicious by hiding it inside of another program that does something.


trojark — Python server.py — 80×24
~/Code/trojark — Python server.py
~/Code/trojark — Python client.py

```
::::::::::::::::::::  :::::::: ::::::::::::::    ::::::::: :::    :::
    :+:    :+:    :+::+:    :+:    :+:  :+: :+:  :+:    :+::+:   :+:
    +:+    +:+    +:++:+    +:+    +:+ +:+   +:+ +:+    +:++:+  +:+
    +#+    +#++:++#: +#+    +:+    +#++#++:++#++:+#++:++#: +#++:++
    +#+    +#+    +#++#+    +#+    +#++#+     +#++#+    +#++#+  +#+
    #+#    #+#    #+##+#    #+##+# #+##+#     #+##+#    #+##+#   #+#
    ###    ###    ### ########  ##### ###     ######    ######    ###

----------------------------
Current platform: posix
Awaiting connections
Connection from ('67.85.111.80', 57512) established
Client is valid Trojark client
67.85.111.80> 
```

IP is blurred out.

Any command you enter will be executed on the machine. If your command is part of the scripts, it will execute it instead.

Scripts

ip	Get public IP address of machine (even though it tells you)
scare	Creates a file called **TROJARK_WAS_HERE** and, if on MacOS, uses text-to-speech to say “Trojark has taken over your computer.”