**Covert Delivery + Building an Undetectable Payload Bundle**

**Project Jackcryptor:**

**Objective**

Create a stealthy malware bundle by hiding a RAT inside a legitimate software installer using AES-256 encryption and PyInstaller packaging.

**Tools Used**

Python 3 + PyInstaller

PyCryptoDome (AES encryption)

NjRAT (or any RAT)

**Legitimate software (Notepad++, VLC, etc.)**

**Steps Executed**

1. Install Python → Added to PATH

2. Install Requirements:

cmd

pip install pyinstaller pycryptodome requests

3. Run Builder Script:

cmd

python Jackcryptor.py client.exe

4. Select Software (e.g., VLC)

5. Add Icon (e.g., Bitcoin.ico for disguise)

6. Build Bundle → Output: VLC\_Installer.exe

**Key Features**

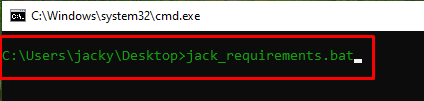
1. AES-256 Encryption
2. Silent Payload Execution
3. Icon + Name Spoofing
4. VM Detection + UAC Bypass Attempt

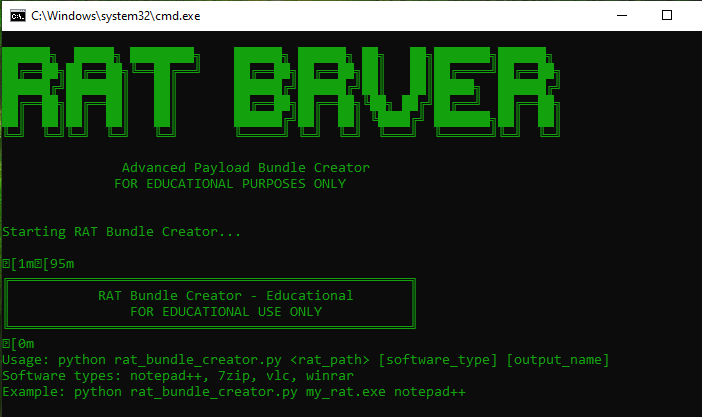
**Result**

1. Legitimate software installs visibly
2. RAT runs hidden in background
3. Evades basic detection
4. Appears trustworthy to user

**Important Steps:**

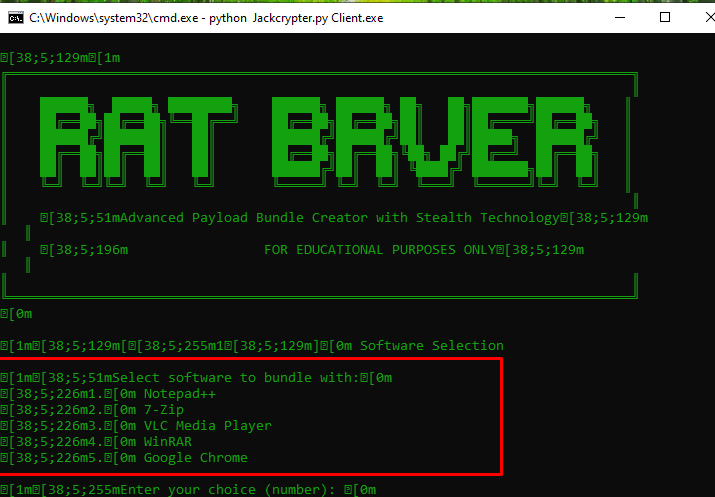
**Legal Notice You can follow these under on Ethical Laws on Testing Environment:**



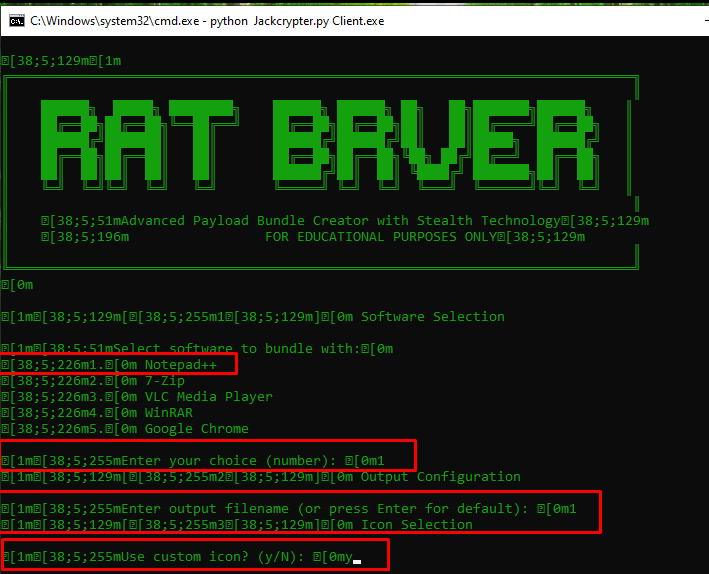
 **Press Enter**



**Press Enter:**



**Choose options:**



**It Ask you to choose options**

**Like 1 , 2 , 3 , 4, according to as per user choice**

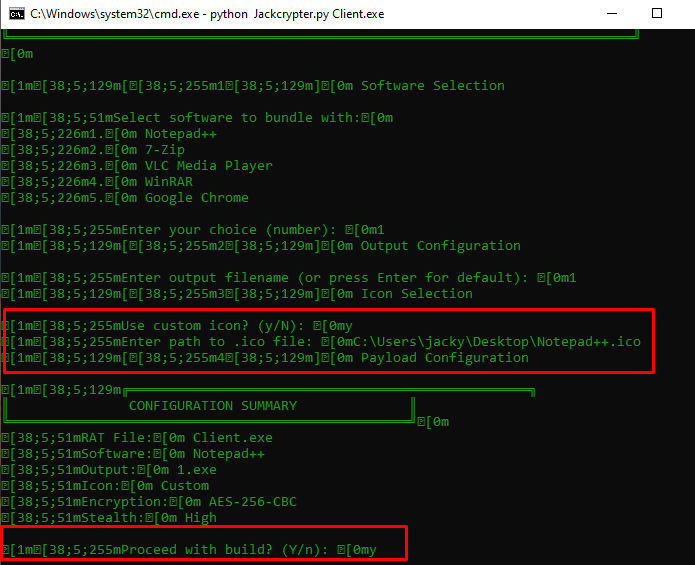
**Than it ask you choose custom icon if yes so press y**

**After so have to select the path of your icon that I mentioned below**

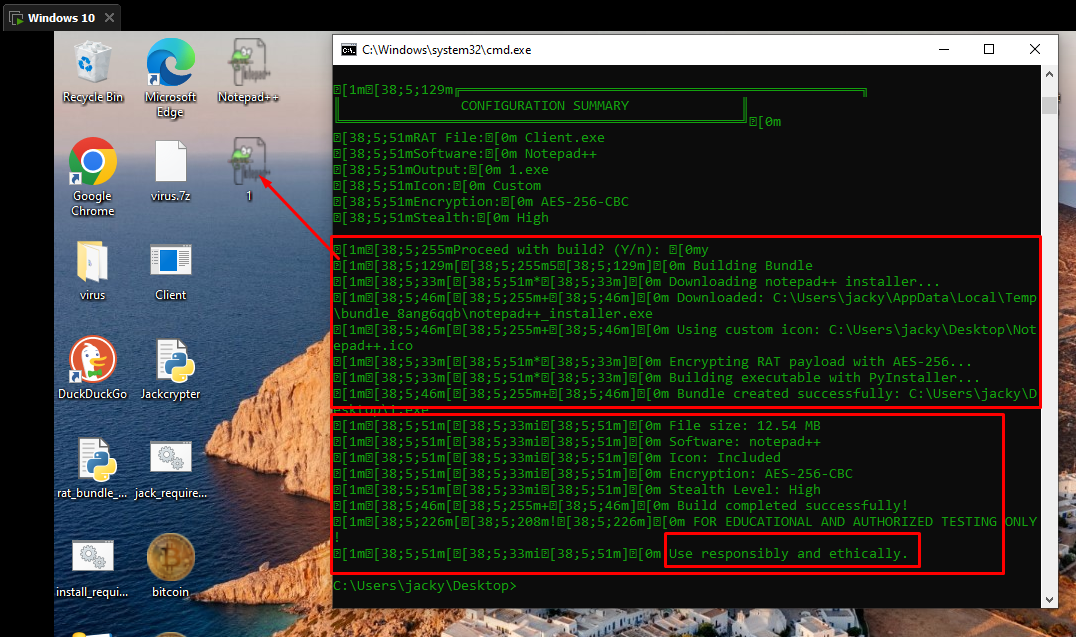
**Follow all steps:**

**Here I provide the path of my icon you choose yours:**

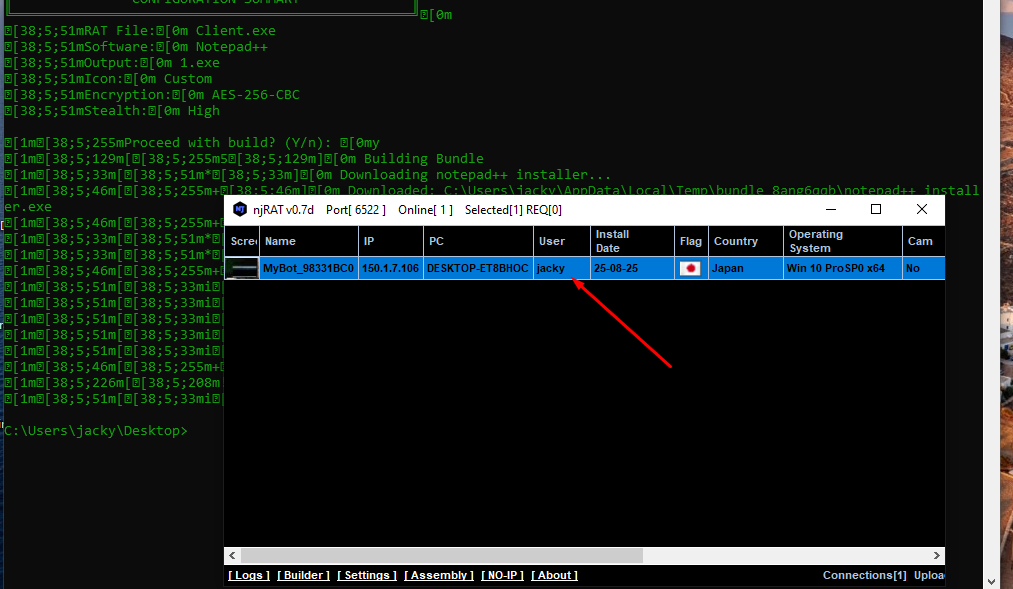
**Enter**



**Select y and hit enter**



**Finally It Create So Let’s check your Client on NJ rat:**



**It’s done**

**Github repo:**

**Note**

**For educational use only. Conducted in a controlled lab environment for cybersecurity training.**