DevilCatCommander Trojan

Before start:

Server:

- When you run a server part – you need to install PyQt6. (If it doesn't work - use python interpreter version 3.9)
- When GUI is running and you click "start" for listening in windows it can write "not responding" – it is ok.
- There is also a GUI.exe file of server

Client:

- Source code in plain text you can find in client.pdf (Because I had some issue with detection by ESET)
- ***You have 2 versions of client payload:***
    - ***Version of packer with client.exe file for persistence (can be detectable)***
    - ***Version of packer with one more packer inside for persistence (need install packages)***

- You need to install pycryptodome (different from pycryptodomex)
- You need to install pynput
- By default, it connects to 127.0.0.1 port 4444. I used ddns but decided to change it for localhost for you. When you start server-side program you need to enter port number.

About program:

Server-client(trojan)

Server GUI with PyQt6 and has both buttons and command line control

Client obfuscated with pyarmor

Client compressed with IExpress and inside it has another IExpress package for persistence

Then target execute the payload, it copies the files to *c:\users\%user%\document* directory and creates a register key in runs to create persistence. After that it uses hybrid encryption for traffic – it creates RSA public key and send it to server, then server creates symmetric AES key and encrypt it with client public key and send it back to client. Both (client and server) start connection.

Files:

Server:

- Devil_Cat_Commander.py, DevilCatCommander.py (GUI version – 2 files)
- DevilCatCommander.exe (GUI exe version)
- CLI_DevilCatCommander.py (CLI version)
- README.pdf (this file)

Client:

- client.pdf (plain text source code)
- cat.exe (main payload) compressed with IExpress following files:
  - cat.jpg (cat pic)
  - cl.bat
  - backd.exe (compressed with iexpress persistence files)
  - client_obfuscated.py, pytransform.py, _pytransform.dll (3 obfuscated from 1 source file with pyarmor)

Functionality:

- *Basic shell functionality*
- *Download and Upload files*
- *Search for file*
- *Scanning hosts/network*
- *Persistence functionality*
- *Clipboard capture, Keylogger*
- *Chrome password stealer*
- *Encryption*

Modules:

Server side:

os, socket, pyqt6, cryptodomex, string, random

Client side:

os, json, base64, sqlite3, threading, pycryptodome, pycryptodomex, pypiwin32, shutil, datetime, socket, subprocess, time, pynput, winreg