

Challenge SSTIC 2026 - Step 1 : vibe malwaring

nebucca

A cette étape on va se concentrer sur ce qu'on a pu récupérer à l'étape précédente : les sources du malware.

Après un nouveau travail de mise en forme il apparait que le module *config* est chiffré lors du transport.

1 Déchiffrement du module *config*

Comment le client le déchiffre t il ?

```
mod_code_bytes = b64decode(mod_code)
self.crypto.decrypt(self.session_key, mod_code_bytes).decode()
```

D'où vient cette clef de session ?

```
self.session_key = self.crypto.compute_session_key()
```

```
def compute_session_key(self) -> bytes:
    rand = Random(int(time.time()))
    key = rand.randbytes(n=32)
    return key
```

Autrement dit, la clef de session est calculée à partir de la date courante. Il est ainsi possible de retrouver la clef de session à partir de sa date de création. Grâce aux traces réseaux nous avons un horodatage précis de l'événement *set_session_key*.

Avec un script python, petit brute force sur la date à partir de "1771542017" qui nous permet de trouver la clef et de déchiffrer le module de configuration.

2 Domain Generation Algorithm

Dans la configuration on trouve en particulier tout ce qui sert à initialiser la partie DGA (Domain Generation Algorithm) du malware afin de lui permettre de déterminer à quelle adresse retrouver le C2.

Il suffit de lancer l'algorithme de calcul du domaine sur la bonne période (là encore la date dans wireshark). On trouve : <http://51.15.164.185/aoxgulmpgdvaagd/>

Il n'y a plus qu'à récupérer le flag et se rendre à l'étape suivante.