HACK'OSINT CTF – OFFICIEL WRITEUP

Table des matières

Date de la compétition	21 juin 2024 au 23 Juin 2024
Nombre d'équipe inscrite	220
Nombre d'équipes participantes	145
Nombre d'équipes ayant terminé la mission	0

I. Rappel de la mission

Lien vers le trailer officiel : TRAILER - HACK'OSINT CTF 2024

Charlotte, une jeune femme, a été victime d'une arnaque en ligne. Tout a commencé lorsqu'elle a reçu un email frauduleux prétendument de sa banque, l'incitant à cliquer sur un lien et à saisir ses informations personnelles. Après avoir suivi ces instructions, rien ne s'est produit immédiatement. Cependant, quelques heures plus tard, elle reçoit une notification de sa banque concernant un transfert de 10 000 euros vers un compte étranger. Surprise, elle appelle immédiatement sa banque pour faire opposition, mais il était déjà trop tard.

Déterminée à retrouver les responsables, Charlotte, aidée par une amie, découvre que l'email était en fait une tentative de phishing ciblée. Décidée à récupérer son argent et à traduire en justice les cybercriminels responsables, Charlotte se rend aux autorités pour porter plainte. Parallèlement, elle engage des enquêteurs privés pour renforcer ses efforts.

C'est dans ce contexte que vous avez accepté la mission de retrouver et de démanteler le réseau de cybercriminels responsable de l'arnaque subie par Charlotte, avant qu'ils ne puissent nuire à d'autres victimes.

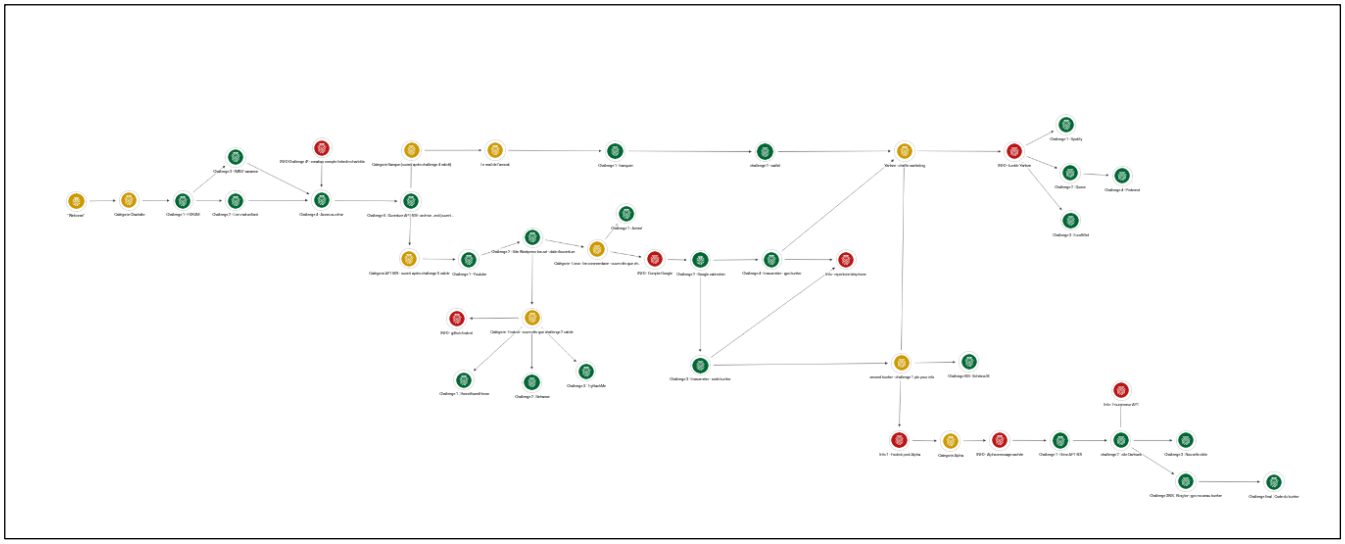
❗ **Pour rappel, ne faites jamais justice par vous-même. Rapprochez-vous toujours des autorités compétentes :** PHAROS

II. WU OFFICIEL

A. OSINT TRACKER

Pour mener à bien cette enquête et démanteler APT509, vous avez dû relever 33 défis.

Voici l'OSINT TRACKER de l'enquête :



B. Challenges

Acte 1 : Charlotte

Challenge : Le fil conducteur

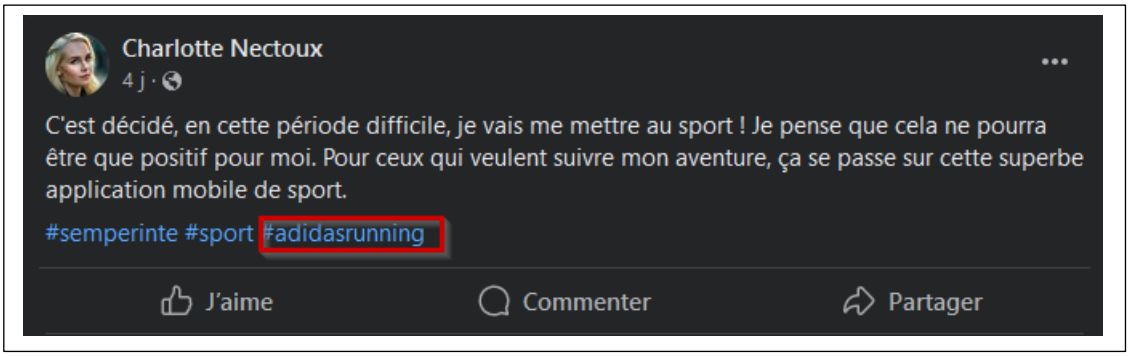
Grâce à l'énoncé de ce challenge, nous en savons maintenant un peu plus sur Charlotte. Après une recherche sur Google, nous avons trouvé son profil LinkedIn :

https://www.linkedin.com/in/charlotte-nectoux

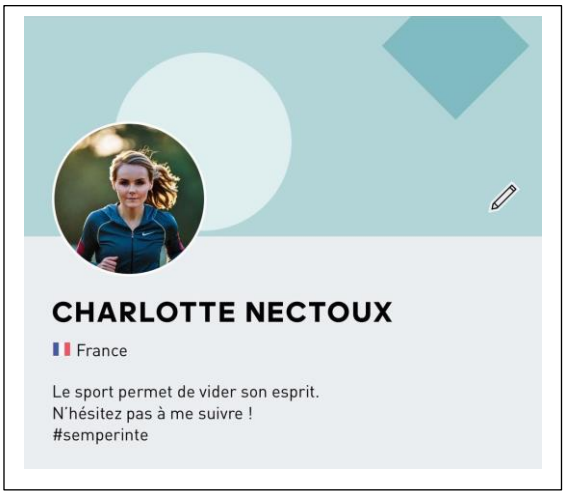
En effectuant une recherche manuelle, nous avons trouvé son compte Facebook :

https://www.facebook.com/profile.php?id=61556792931249

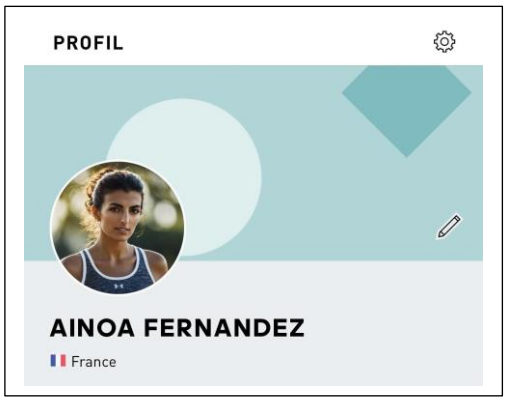
Sur son Facebook, nous trouvons un post de Charlotte intéressant :



Par conséquent, Charlotte utilise l'application mobile Adidas Running. En téléchargeant cette application, nous trouvons le profil sportif de Charlotte. Sur l'une de ses activités, nous trouvons un commentaire d'une certaine Ainoa F.



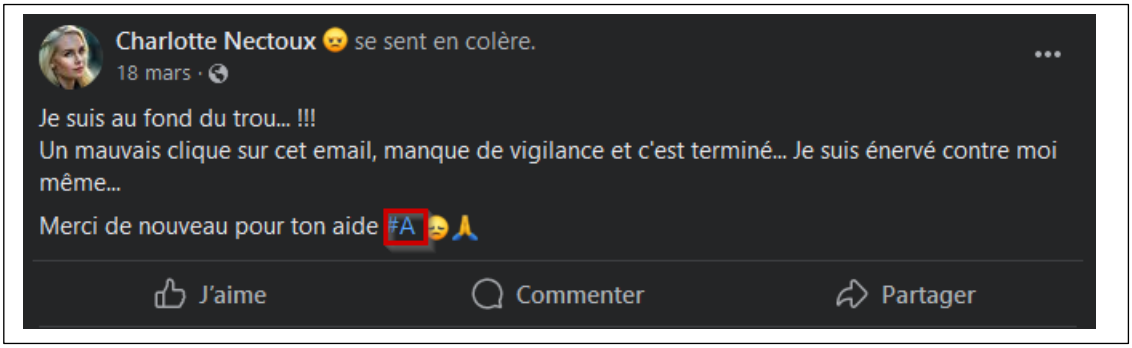
On apprend alors que c'est cette personne qui a aidé Charlotte.



De plus, grâce à leur discussion sur Adidas Running, nous savons qu'Ainoa Fernandez a un compte Facebook :

https://www.facebook.com/profile.php?id=61559173776963

Pour confirmer qu'il s'agit bien d'Ainoa qui a aidé Charlotte, nous trouvons un post sur Facebook de Charlotte la remerciant :



Le flag est donc : hacko{ainoa_fernandez}

Challenge : Lien malveillant

Nous savons que c'est Ainoa qui a aidé Charlotte. Pour retrouver le lien de phishing sur lequel Charlotte a cliqué, tout se passe sur le profil d'Ainoa. Sur son profil Facebook, nous retrouvons plein d'informations intéressantes :

Grâce à ces informations, nous retrouvons son profil CCM :

https://forums.commentcamarche.net/profile/user/AinoaHelp

Nous découvrons également sa demande d'aide concernant un drôle de mail que son amie a reçu :

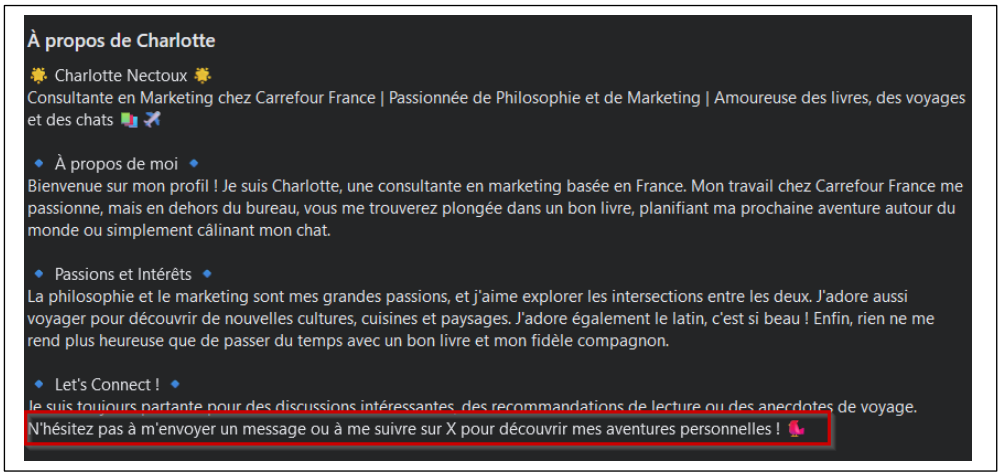
https://forums.commentcamarche.net/forum/affich-38016367-drole-d-email

```
<a href="https://zdzadzad.ra"
    style="display: none;"></a>
<a href="https://olpma.it"
    style="display: none;"></a><a
    href='https://d0cum3nts-clc.we3bly.com/'>https
</p>
<a href="https://zdzadzad.ra"
```

Nous retrouvons alors l'URL du lien malveillant sur lequel Charlotte a cliqué : hacko{https://d0cum3nts-clc.we3bly.com}

Challenge : « Oh soleil ! »

Grâce au profil Facebook de Charlotte, nous savons qu'elle utilise également Twitter.

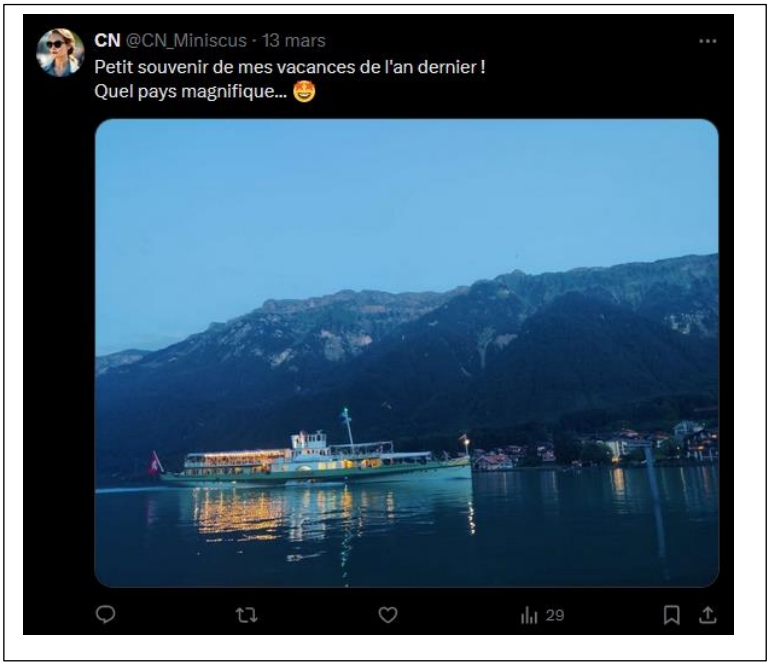


Pour retrouver son compte Twitter, nous remarquons sur son compte Facebook qu'elle utilise souvent des hashtags dans ses publications.

Après une recherche sur Twitter avec l'un des hashtags utilisés par Charlotte, nous retrouvons son compte :

https://twitter.com/CN_CumSpe

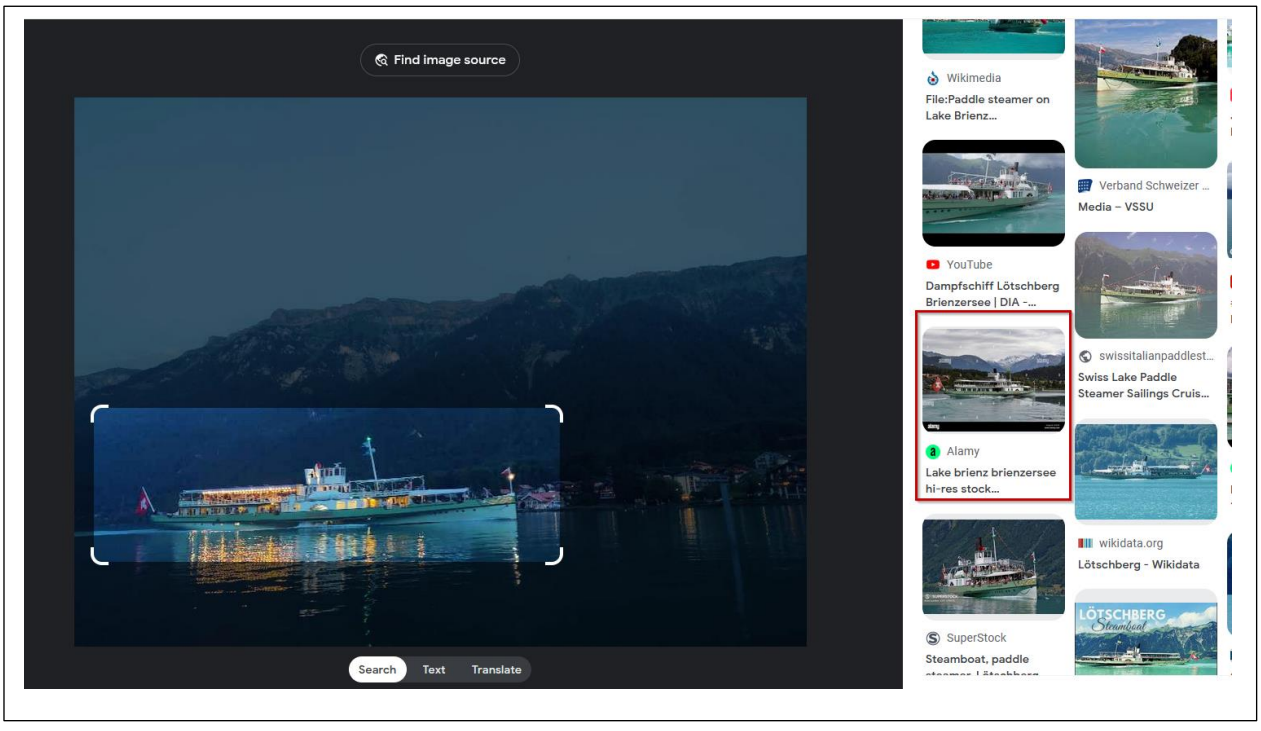
Nous trouvons alors un post de Charlotte évoquant ses vacances de l'an dernier :



Place au GEOINT, nous avons une photo des dernières vacances de Charlotte. Les données EXIF de l'image ne sont pas utiles. En analysant l'image, nous pouvons voir les informations suivantes

- Un bateau sur l'eau avec un drapeau suisse.
- La présence d'une zone montagneuse.
- Une ville en arrière-plan.

Nous allons alors effectuer une recherche inversée de l'image (utilisant https://lens.google/).



Nous retrouvons alors facilement des informations sur le bateau et son emplacement. Nous sommes sur le lac « Lake Brienz » (Brienzersee), et le bateau que nous voyons est un bateau de croisière. Sur Google, nous trouvons des informations sur cette croisière : Croisières sur le lac de Brienz.

En effectuant une recherche sur Google, nous pouvons retrouver les différents points où le bateau fait escale :

Plus qu'à retrouver, grâce aux informations disponibles sur la photo, dans quelle ville celle-ci a été prise.

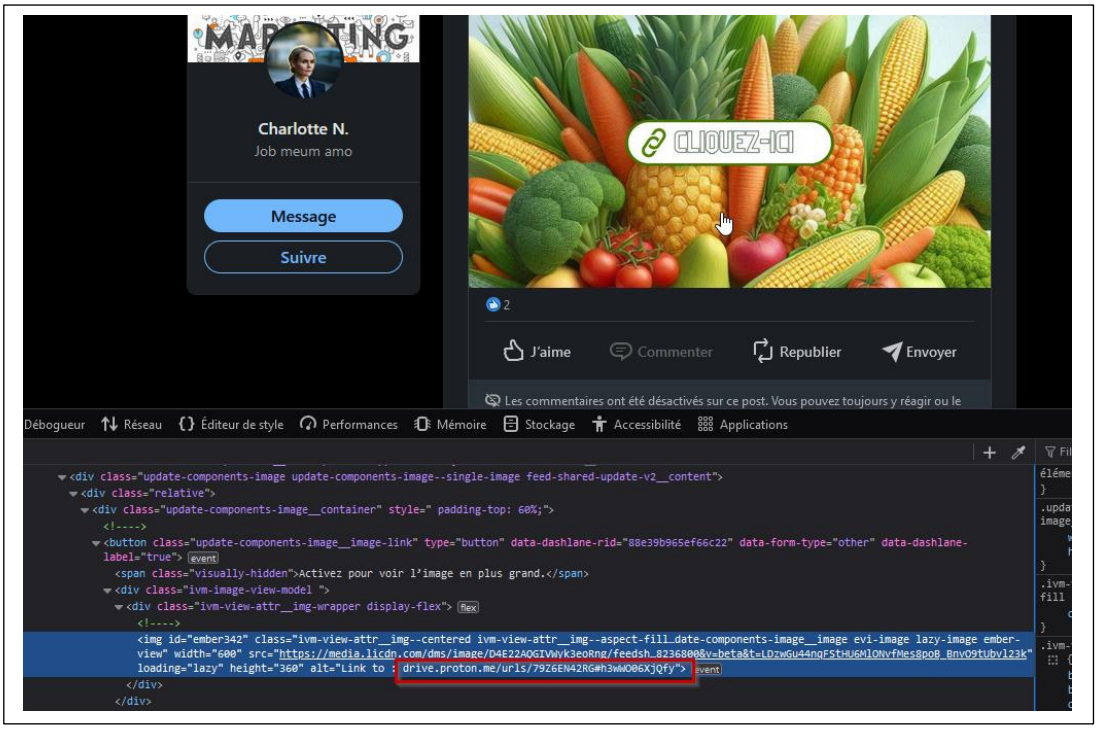
Après une recherche, nous retrouvons le lieu exact où la photo a été prise :

Charlotte était alors en vacances à **Bönigen en Suisse.**

Flag du challenge : hacko{bonigen}

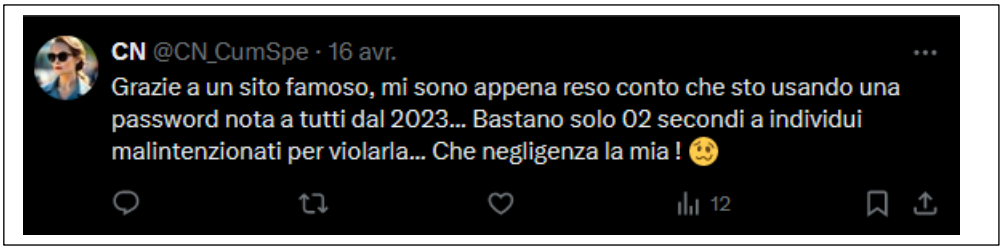
Challenge : Intimité

Pour ce challenge, sur le Facebook de Charlotte, nous retrouvons une de ses publications parlant de son projet en marketing. Celle-ci nous incite à cliquer sur la photo du post pour en savoir plus. Cependant, la photo n'est pas cliquable. En regardant le code source de la page, nous retrouvons le lien que Charlotte voulait rendre cliquable.



Nous retrouvons alors un lien vers un drive :
https://drive.proton.me/urls/79Z6EN42RG#h3wWO06XjQfy

Pour trouver le mot de passe du drive de Charlotte, nous savons grâce à l'un de ses tweets qu'elle utilise un mot de passe faible.

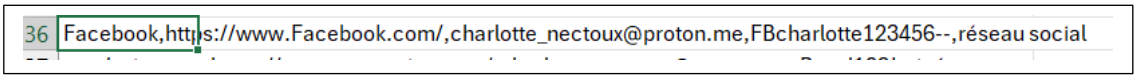


Après une recherche sur Google, nous retrouvons le site qu'elle évoque :

https://nordpass.com/most-common-passwords-list/

Son tweet étant en italien, nous retrouvons alors dans le tableau "Italie" le mot de passe évoqué par Charlotte, qui est : ciaociao

Une fois dans son drive, nous trouvons dans un dossier un fichier contenant l'historique de ses mots de passe (Archives -> Nav -> CHROME_HISTORY_MMXIX.xlsx).



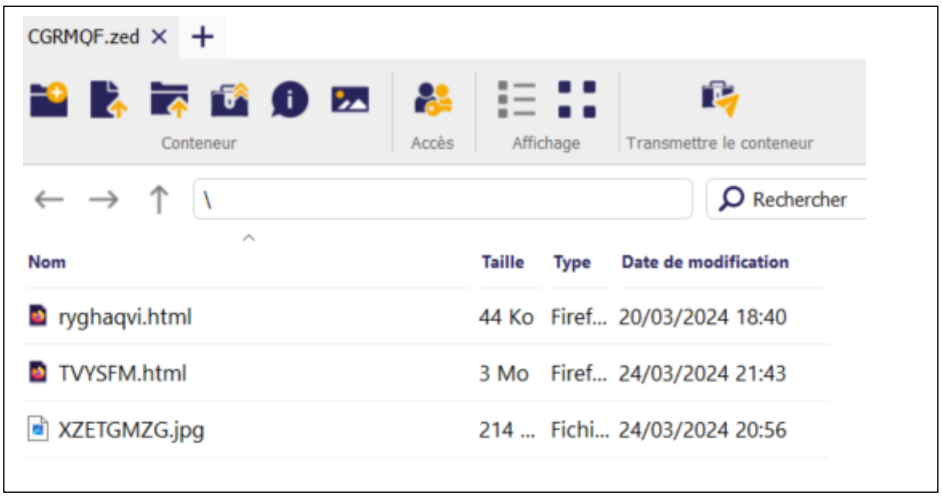
La réponse à ce challenge était : hacko{FBcharlotte123456--}

Challenge : Revendication

Sur le drive de Charlotte, dans le dossier Archives, nous retrouvons un fichier .zed (CGRMQF.zed). Dans le même dossier, nous trouvons un fichier (ofrsxxiujcsnnqeygtkhmf.txt) avec une phrase nous indiquant le mot de passe pour ouvrir ce fichier.

En comprenant cette phrase, on réalise alors que le mot de passe pour ouvrir le fichier .zed est le nom du fichier .zed lui-même : CGRMQF.

Une fois l'archive ouverte grâce à l'application Zed! (https://www.zedencrypt.com/download), nous retrouvons plusieurs fichiers :



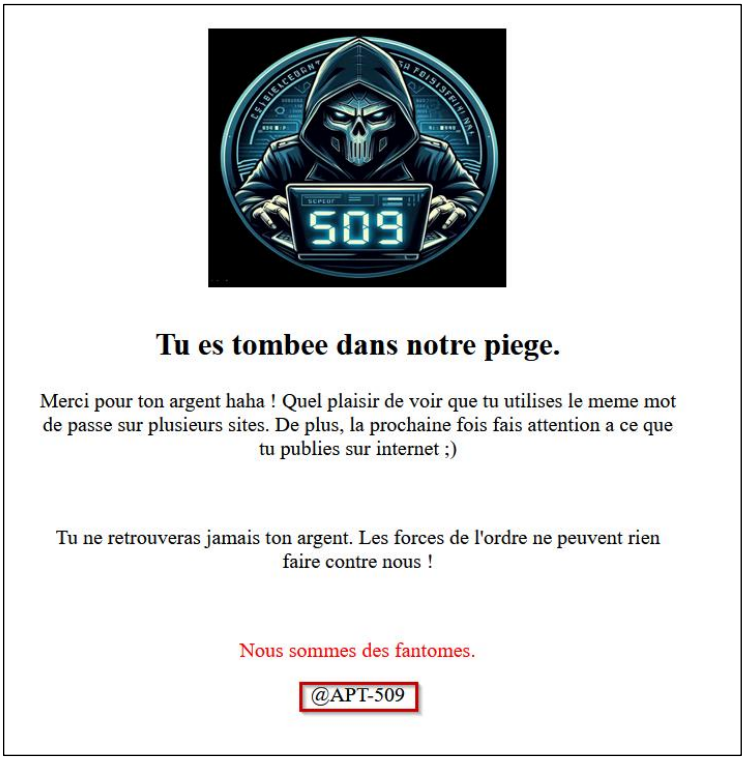
Parmi les fichiers, nous trouvons un fichier nommé TVYSFM.html, qui semble être la revendication d'APT-509 :

La réponse à ce challenge était : hacko{apt-509}

Acte 2 : APT-509

Challenge : Site vitrine

Grâce à la revendication trouvée sur le drive de Charlotte, nous trouvons également un pseudonyme :



Nous retrouvons alors leur chaîne YouTube : https://www.youtube.com/@APT-509

La vidéo d'une heure sur leur chaîne tourne en boucle, indiquant le message suivant : "VIDEOS ARE NOT JUST PUBLIC".

Cependant, en utilisant le site « unlistedvideos.com » (un outil pour publier des vidéos non répertoriées sur YouTube), nous retrouvons alors une vidéo publiée par APT-509 :

https://unlistedvideos.com/v.php?youtube-mCwcEL8jpP0

En observant attentivement les informations sur la vidéo, nous trouvons alors l'URL du site WordPress utilisé par APT-509 :

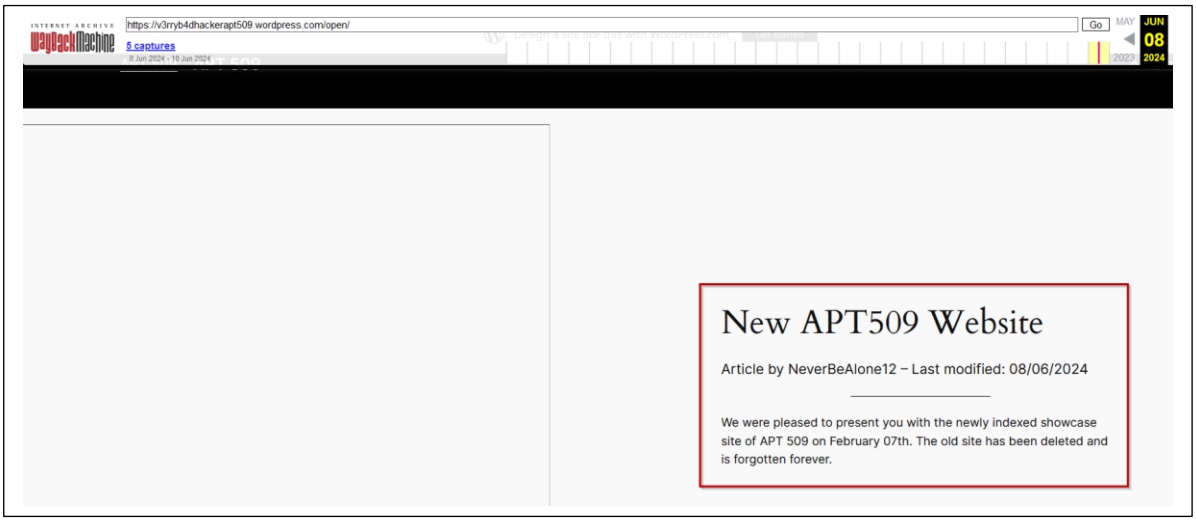
https://v3rryb4dhackerapt509.wordpress.com/

La réponse au challenge était donc : hacko{https://v3rryb4dhackerapt509.wordpress.com}

Challenge : Ghosts really ?!

Grâ à l'extension de navigateur « WAYBACK MACHINE », nous savons qu'il existe des sauvegardes de ce site.

Nous retrouvons alors un historique de scan wayback de la page « open » intéressant (https://web.archive.org/web/20240608184829/https://v3rryb4dhackerapt509.wordpress.com/open/) comprenant des informations personnelles d'un des membres d'APT-509 ainsi que la date d'ouverture du site :



La réponse au challenge était : hacko{2024-02-07}

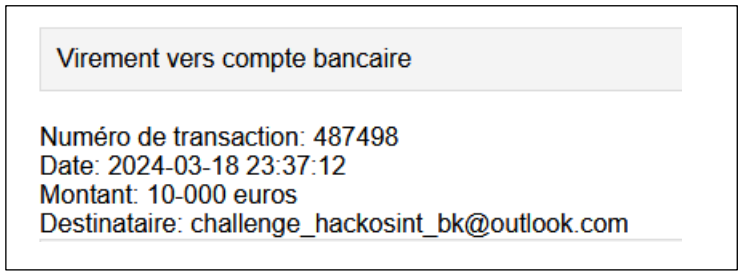
Par la même occasion, nous trouvons un pseudo qui nous servira plus tard : NeverBeAlone12.

Acte 3 : Fortune

Challenge : Banker

Comme nous l'indique l'énoncé de ce challenge, nous devons nous concentrer sur la transaction frauduleuse dont Charlotte a été victime. En inspectant de nouveau son drive (drive.proton.me/urls/79Z6EN42RG#h3wWO06XjQfy), nous retrouvons des relevés bancaires (ARCHIVES -> PRO -> ARGENTARIA). Sur les deux virements disponibles, seul celui de mars est intéressant. Pour rappel, c'est sur le compte Facebook de Charlotte que nous apprenons qu'elle a été arnaquée en mars dernier.

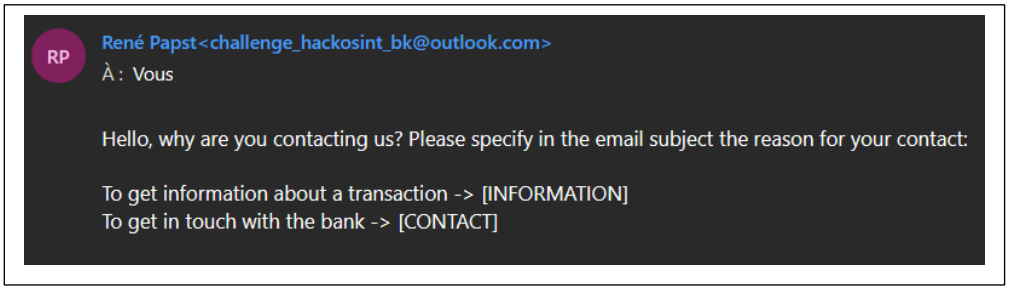
En ouvrant le fichier .html (RELEVE-BANCAIRE-03-2024.html), nous retrouvons la trace du virement de 10 000 euros.



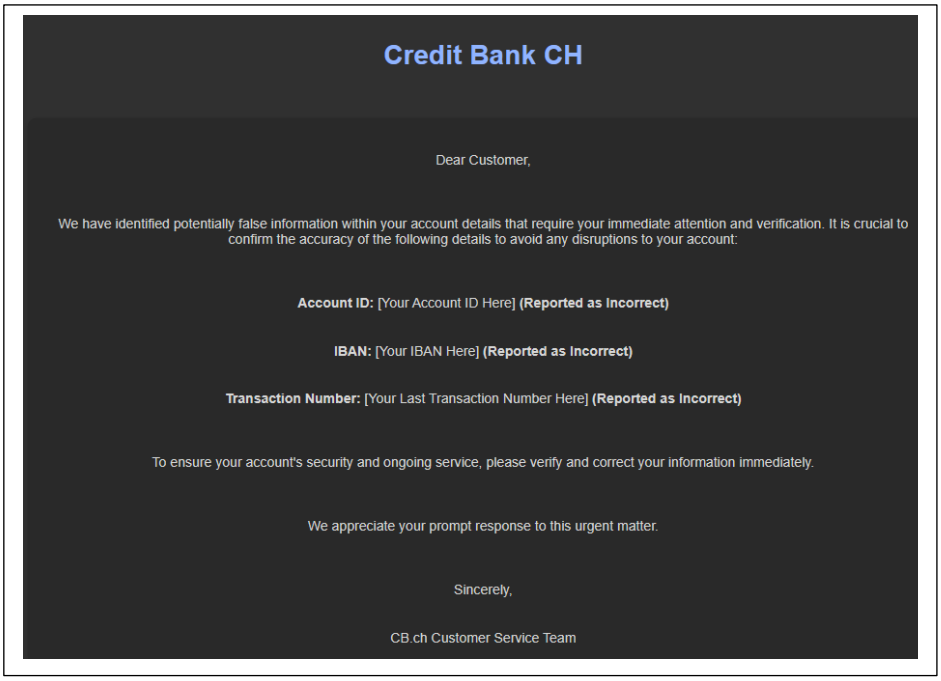
Nous trouvons également une adresse mail : challenge_hackosint_bk@outlook.com

Comme l'indique l'énoncé du challenge, nous savons qu'il faut faire une interaction pour résoudre ce challenge. Par conséquent, nous envoyons un e-mail à cette adresse.

Une véritable conversation commence alors entre nous et la banque utilisée par APT-509.



Après le premier mail envoyé, nous recevons une réponse nous indiquant qu'il faut utiliser un objet précis dans notre mail. Nous choisissons alors d'utiliser "[INFORMATION]", car nous souhaitons obtenir des informations sur un virement.

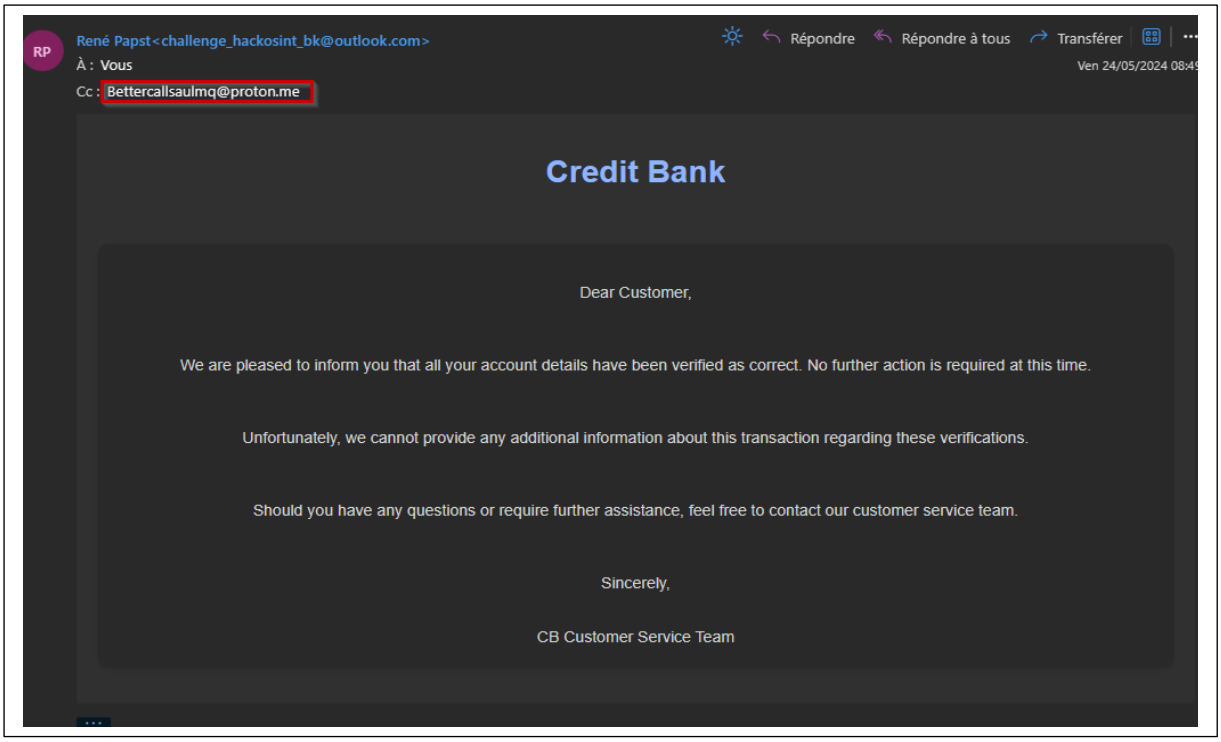


Nous recevons alors une nouvelle réponse nous demandant de fournir des informations précises sur le virement dont nous souhaitons obtenir des détails.

Pour retrouver toutes ces informations, il suffit alors de lire le fichier RELEVE-BANCAIRE-03-2024.html :

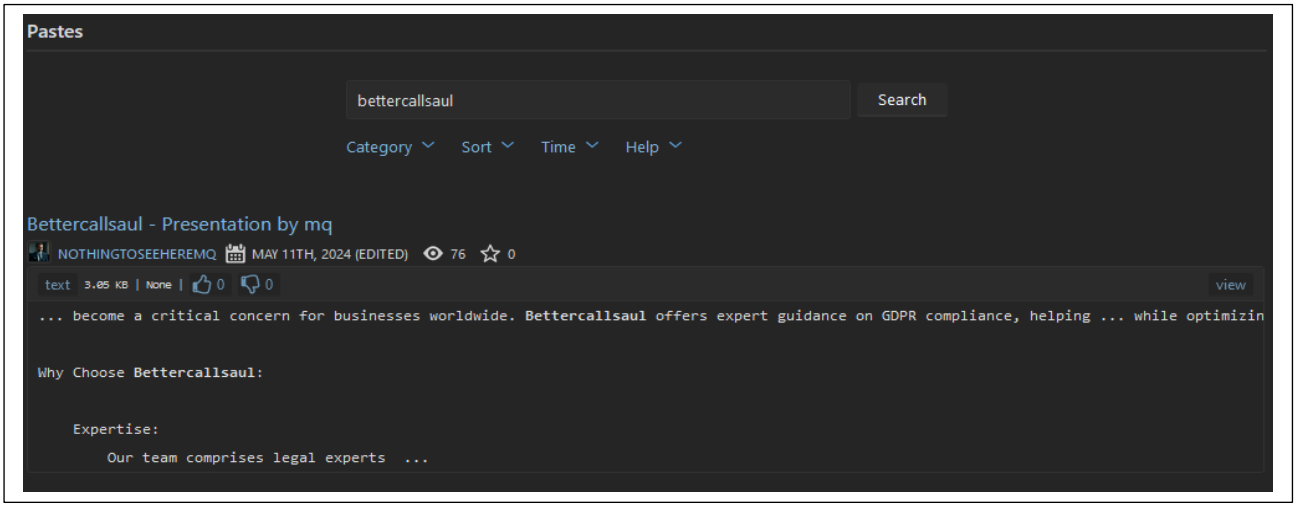
- Account ID : 18984158 (ID de Charlotte)
- IBAN : FR6230003000505569161492F54
- Numéro de transaction : 487498

Nous répondons alors au mail reçu en incluant dans le corps de notre réponse toutes ces informations.

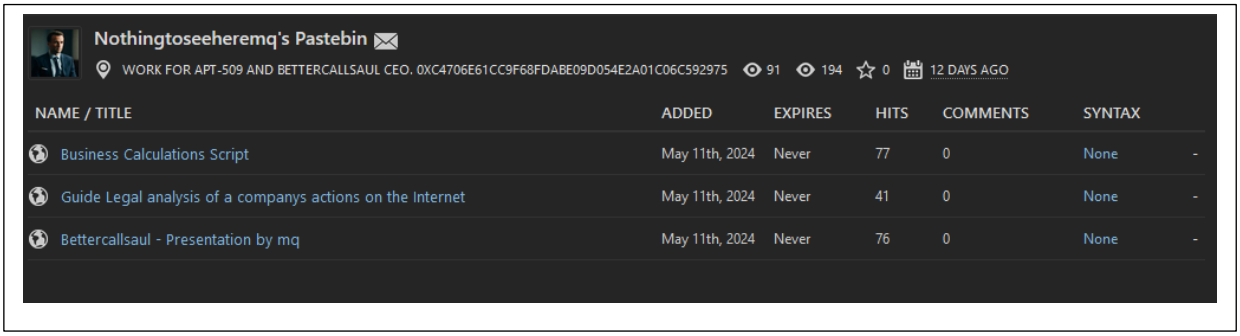


Nous recevons alors un courriel indiquant qu'il n'est pas possible d'obtenir des informations sur ce virement. Cependant, en étant observateur, nous remarquons une adresse e-mail en copie du courriel reçu : bettercallsaulmq@proton.me

Pour la seconde partie de ce challenge, nous pouvons déduire que l'adresse e-mail trouvée est probablement celle du trésorier d'APT-509. Nous savons qu'il communique avec APT-509 en utilisant des notes en ligne. Nous allons donc sur https://pastebin.com/ et nous cherchons dans la barre de recherche : bettercallsaul.

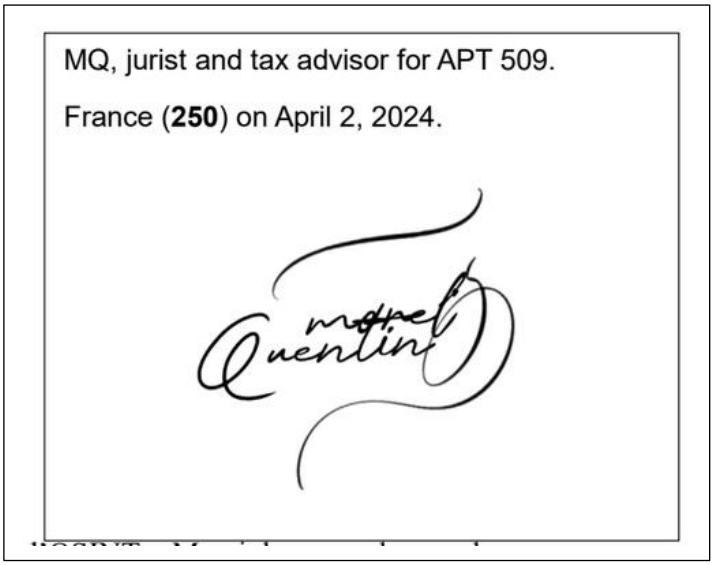


Nous trouvons alors un post présentant l'entreprise "Better Call Saul". Ce post a été créé par un certain "Nothingtoseeheremq" (https://pastebin.com/u/nothingtoseeheremq). En cliquant sur son profil, nous apprenons qu'il travaille pour APT-509. Nous avons alors trouvé le potentiel trésorier d'APT-509.



Nous retrouvons également une adresse de portefeuille (wallet) dans la description de son profil : 0xc4706e61cc9F68fdaBe09D054E2A01c06c592975.

Nous nous concentrons alors sur ses posts. Dans le post "Guide Legal analysis of a company's actions on the Internet", nous trouvons un lien bit.ly menant vers un Dropbox (bit.ly/5a0p9t). Sur ce Dropbox, nous trouvons un fichier PDF. En nous rendant à la fin du fichier, nous trouvons grâce à sa signature des informations sur cette personne :



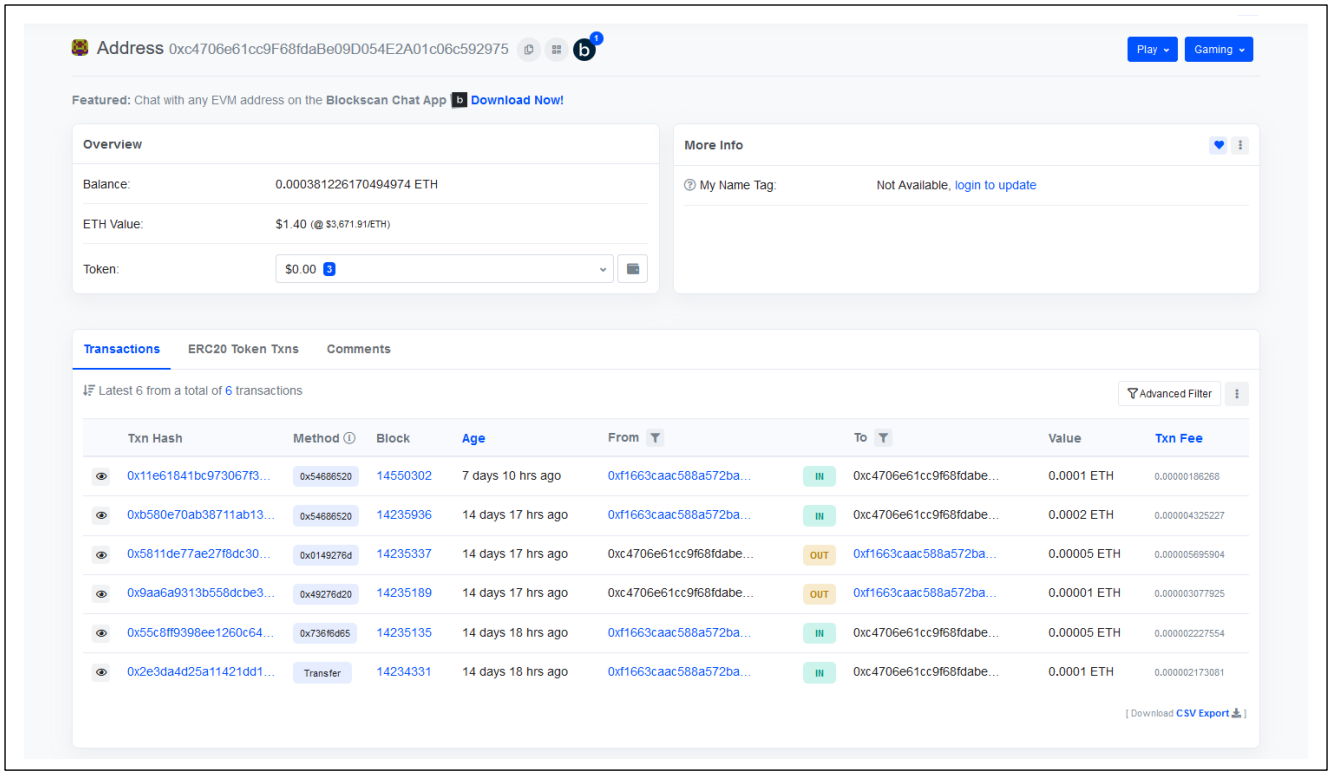
- MQ : Morel Quentin
- Jusrist and tax advisor for APT-509

La réponse à ce challenge était : hacko{juriste_conseiller_fiscal}

Challenge : La transaction

Pour ce défi, nous avions trouvé précédemment un portefeuille. Nous enquêtons alors sur celui-ci : https://basescan.org/address/0xc4706e61cc9F68fdaBe09D054E2A01c06c592975.

Nous retrouvons alors toutes les transactions de ce wallet :



En examinant les différentes informations (INPUT DATA) dans les transactions, nous nous apercevons alors d'une conversation entre deux membres d'APT-509.

Finalement, sur la transaction : https://basescan.org/tx/0xb580e70ab38711ab1367b642721b2d536eb7ae0d9beb4f7afafb0b540b97adf9

Nous savons alors que le virement de Charlotte serait fait 5:09pm soit à 17h09.

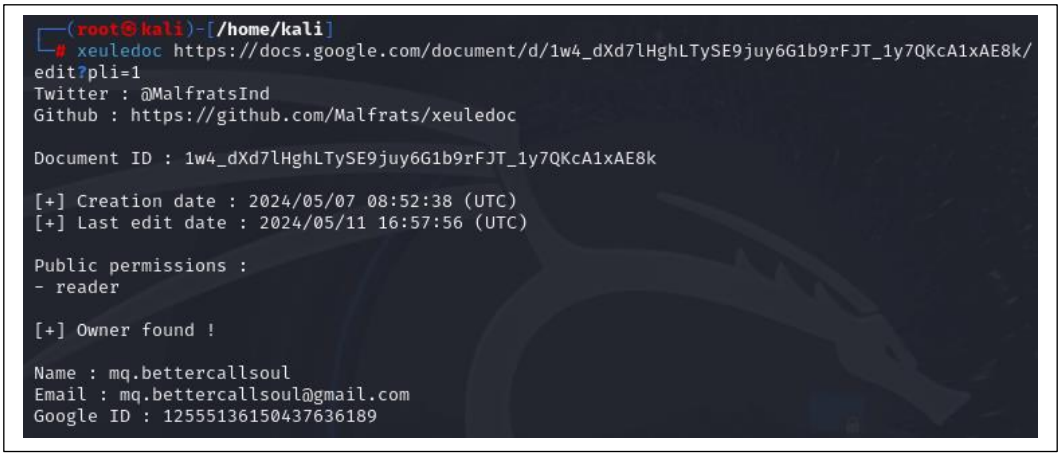
La réponse à ce challenge est donc : hacko{17h09}

Challenge : Welcome back !

Comme l'indique l'énoncé du challenge, nous devons nous concentrer sur le document de l'entreprise "Better Call Saul". Pour information, nous retrouvons ce document dans l'un des pastes de Quentin Morel (https://pastebin.com/Btj06h3F), ainsi que sur le lien suivant : https://docs.google.com/document/d/1w4_dXd7lHghLTySE9juy6G1b9rFJT_1y7QKcA1xAE8k/edit?usp=sharing.

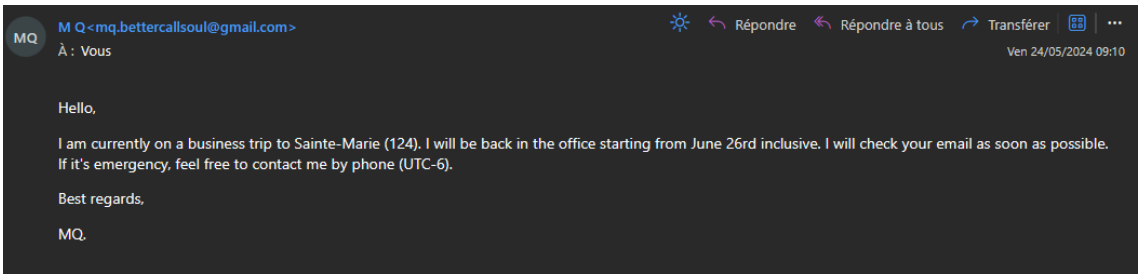
La fiche que nous avons trouvée nous invite à envoyer un e-mail à cette entreprise. Cependant, nous n'avons pas l'adresse e-mail professionnelle de cette entreprise. L'adresse e-mail bettercallsaulmq@proton.me est l'adresse e-mail personnelle de Quentin Morel et n'est donc pas pertinente pour résoudre ce défi.

Grâce à un outil (https://github.com/Malfrats/xeuledoc), nous parvenons à retrouver l'adresse e-mail associée à ce partage Google Doc.



mq.bettercallsoul@gmail.com

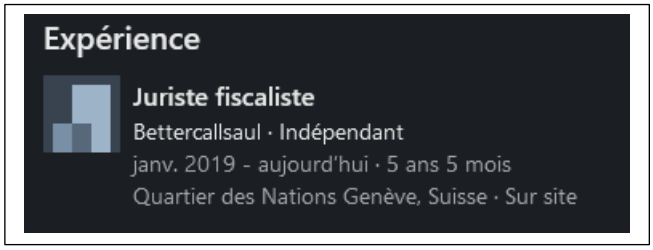
C Comme indiqué dans l'énoncé du challenge, nous devons effectuer une interaction pour le résoudre. Nous envoyons donc un e-mail à cette adresse e-mail professionnelle :



Nous recevons alors une réponse indiquant que Quentin Morel est en voyage d'affaires et qu'il sera de retour le 26 juin. De plus, il est actuellement à Sainte-Marie (124).

Pour trouver le meilleur endroit pour arrêter Quentin Morel, nous devons trouver son profil LinkedIn : https://www.linkedin.com/in/quentin-morel-4667b42b1/

Nous savons alors qu'il travaille chez Bettercallsaul à l'adresse suivante : Quartier des Nations, Genève, Suisse.

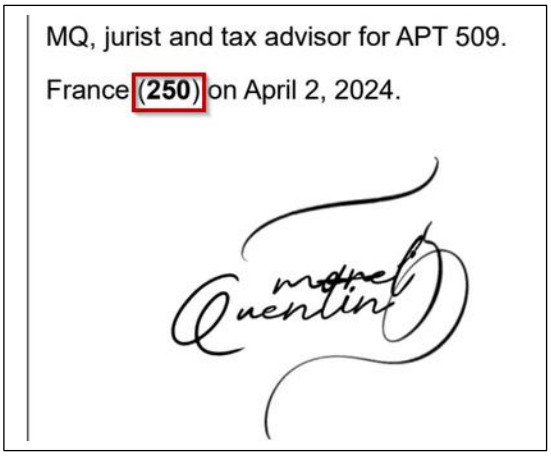


La réponse à cette question était : hacko{26-06_quartier_des_nations_geneve}

Challenge : ?

Pour ce challenge, nous devions déjà terminer le challenge "Welcome Back". Grâce au précédent challenge, nous savons que Quentin Morel est à Sainte-Marie (124).

L'élément clé pour résoudre ce challenge est le "(124)" qui se trouve après Sainte-Marie. Nous nous rappelons alors d'avoir également vu la même chose dans la signature de Quentin Morel sur le fichier Dropbox.



Cette fois-ci c'était France (250).

Après une recherche sur Google avec les termes "France 250", nous tombons sur un site évoquant la norme ISO 3166 : https://www.iso.org/obp/ui/#iso:code:3166:FR.

Puis sur la page Wikipédia de cette norme (https://fr.wikipedia.org/wiki/ISO_3166), nous retrouvons à quel pays est associé le code numérique 124 :

Canada	Canada (le)	CA	CAN	124

Quentin Morel est alors en voyage à Sainte-Marie, au Canada.

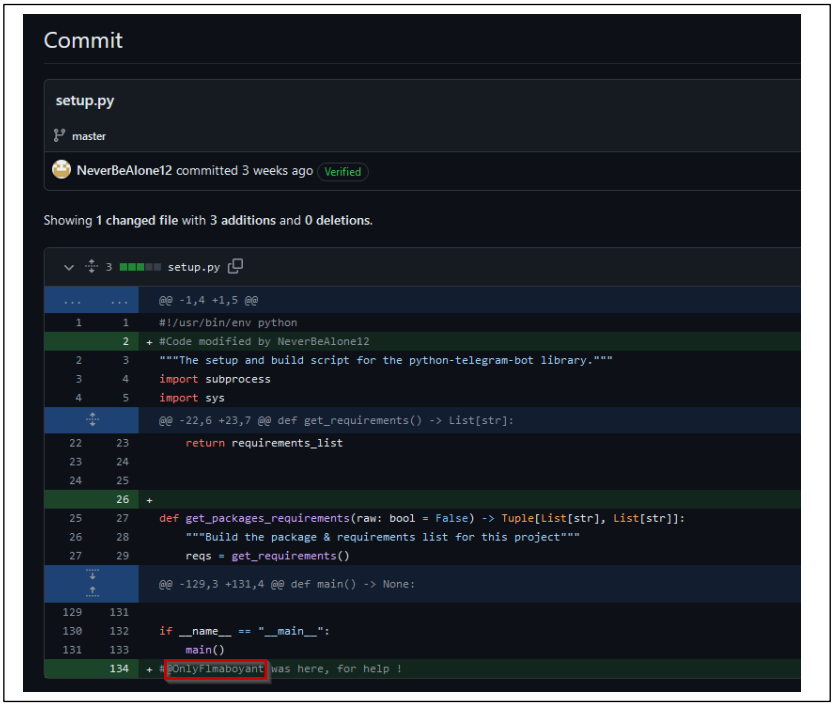
hacko{sainte-marie_canada}

Acte 4 : Le nouveau

Challenge : Le pion

Pour ce challenge, nous nous rappelons alors d'avoir trouvé sur le site WordPress d'APT-509 le pseudonyme "NeverBeAlone12".

En cherchant des comptes avec ce pseudo, nous trouvons le GitHub de cette personne (https://github.com/NeverBeAlone12) . Sur son GitHub, nous retrouvons un dépôt "Python-telegram-bot". En examinant l'historique sur ce dépôt, nous remarquons que des modifications ont été effectuées sur le fichier setup.py.



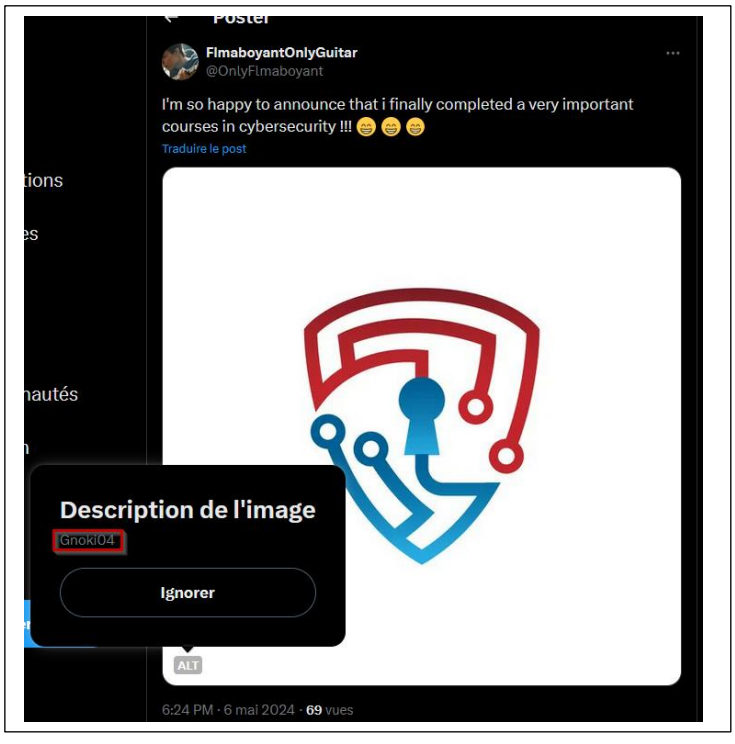
Nous avons alors un nouveau pseudo : @OnlyFlmaboyant. Ensuite, nous trouvons le compte Twitter de ce "NeverBeAlone12" : https://twitter.com/OnlyFlmaboyant.

Dans sa description, nous trouvons alors son identité : Hugo Lecomte (et un nouveau pseudonyme @hugolecomte377).

La réponse au challenge est : hacko{hugo_lecomte}

Challenge : Monter en compétence

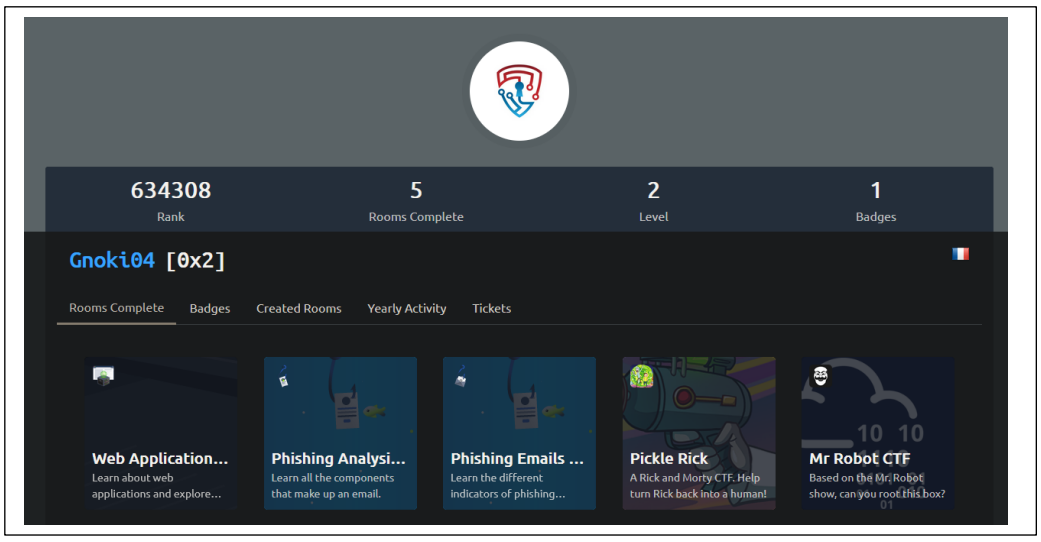
Pour ce challenge, sur le compte Twitter de Hugo, nous trouvons un post évoquant une formation terminée. En regardant la description de l'image du post, nous trouvons un nouveau pseudo : Gnoki04.



Comme ce post évoque un cours sur la cybersécurité, nous allons nous concentrer sur les différentes plateformes d'apprentissage de la cybersécurité en ligne :

- RootMe
- HackTheBox (HTB)
- TryHackMe (THM)

C'est finalement sur TryHackMe que nous trouvons la réponse à notre question : https://tryhackme.com/p/Gnoki04.



Hugo est en train de se former sur le phishing.

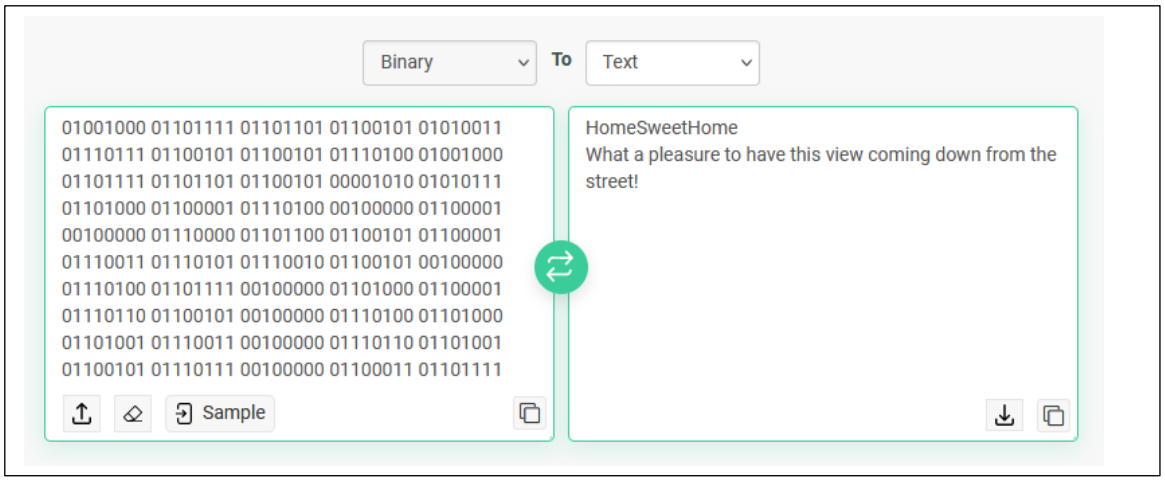
La réponse à cette question était : hacko{phishing}

Challenge : Home Sweet Home

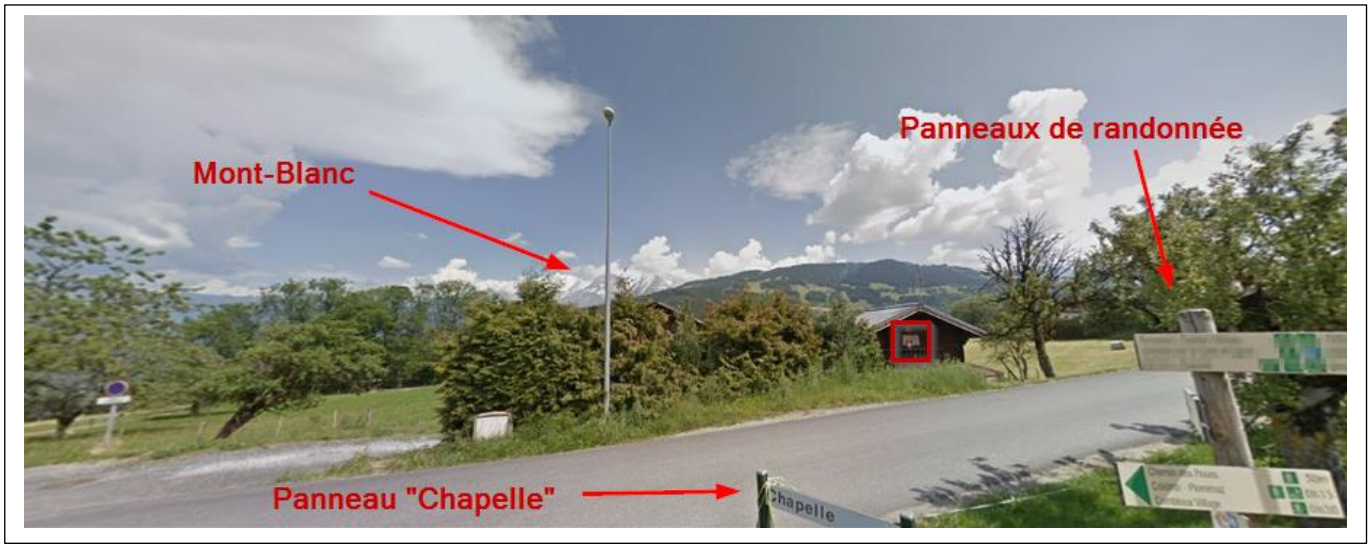
Pour ce challenge ainsi que pour le challenge « Petite amie », nous devons trouver le compte Instagram de Hugo Lecomte. Pour rappel, sur son profil Twitter, nous trouvons : @hugolecomte377.

Grâce à ce pseudonyme, nous découvrons alors son compte Instagram : https://www.instagram.com/hugolecomte377/.

Dans un des posts du 25 avril (https://www.instagram.com/p/C6LO4pntCH5/?img_index=1), il évoque la vue qu'il a depuis sa maison.

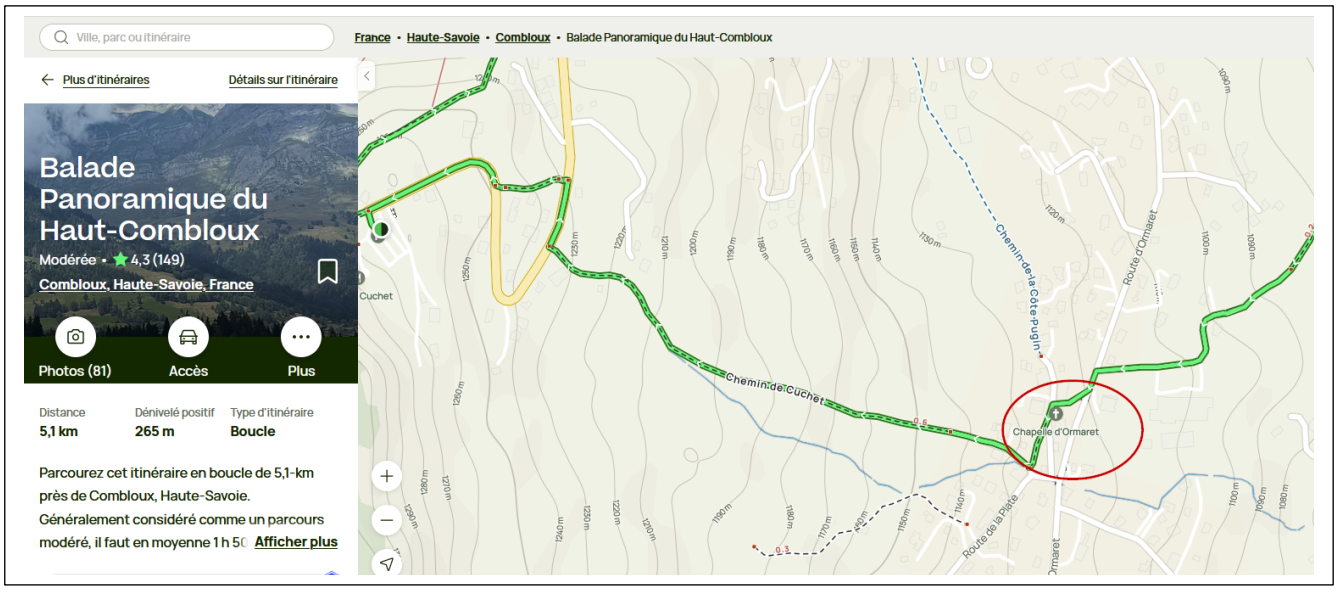


Nous devons alors utiliser du GEOINT pour déterminer où habite Hugo !

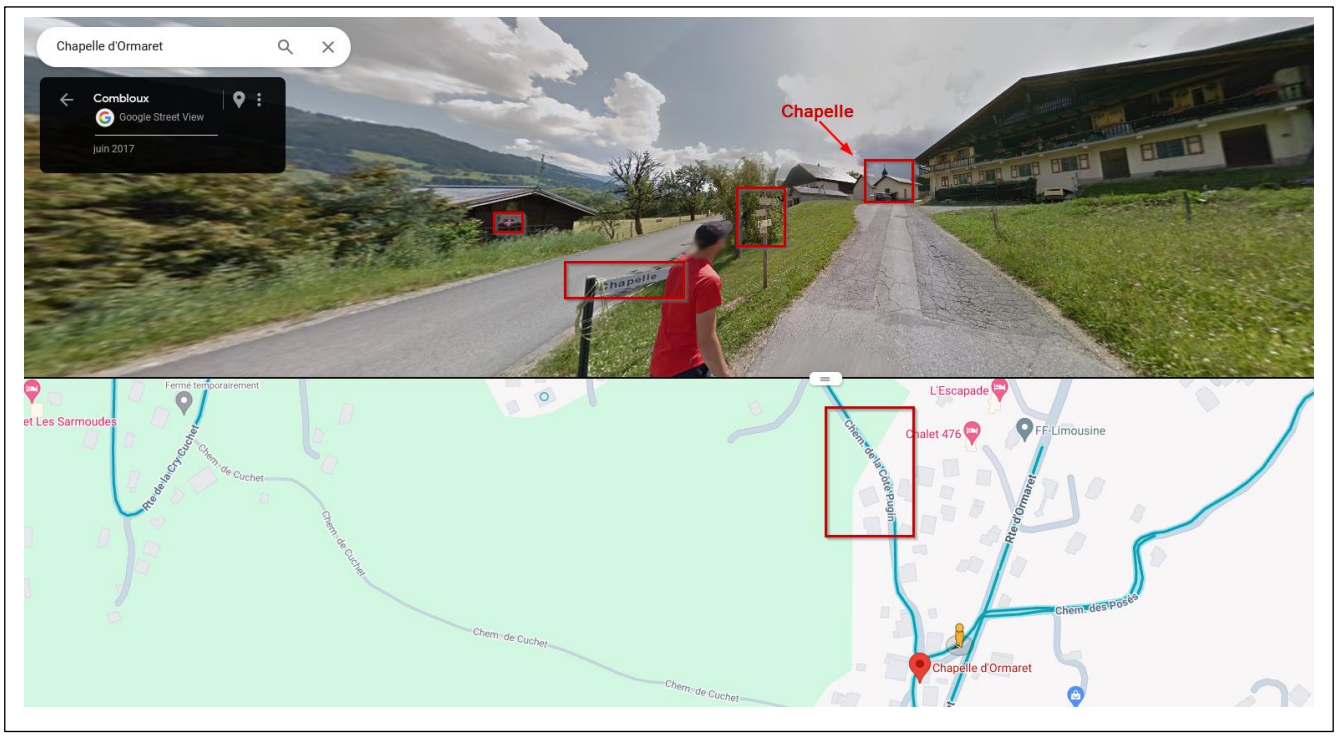


En lisant les panneaux de randonnée, nous savons que nous sommes proches de la ville de « Combloux ». En utilisant le site Alltrails, nous pouvons retrouver les randonnées proches de Combloux : https://www.alltrails.com/fr/france/haute-savoie/combloux.

Puis, en regardant la première randonnée proposée, « Balade Panoramique du Haut Combloux » (https://www.alltrails.com/fr/randonnee/france/haute-savoie/balade-panoramique-du-haut-combloux), nous pouvons retrouver la carte de cette randonnée et une fameuse chapelle.



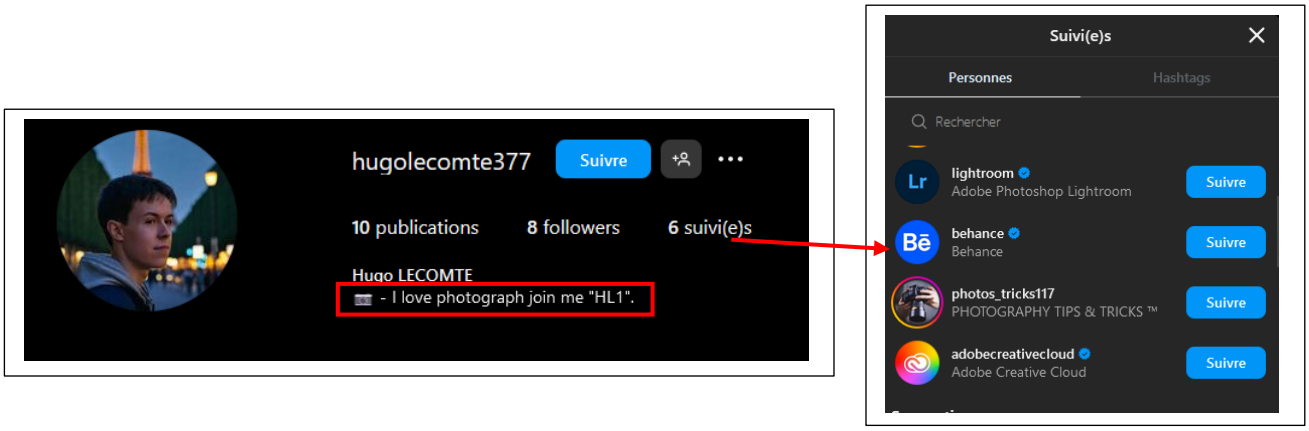
En utilisant Maps, nous allons sur place : [Chapelle d'Ormaret]



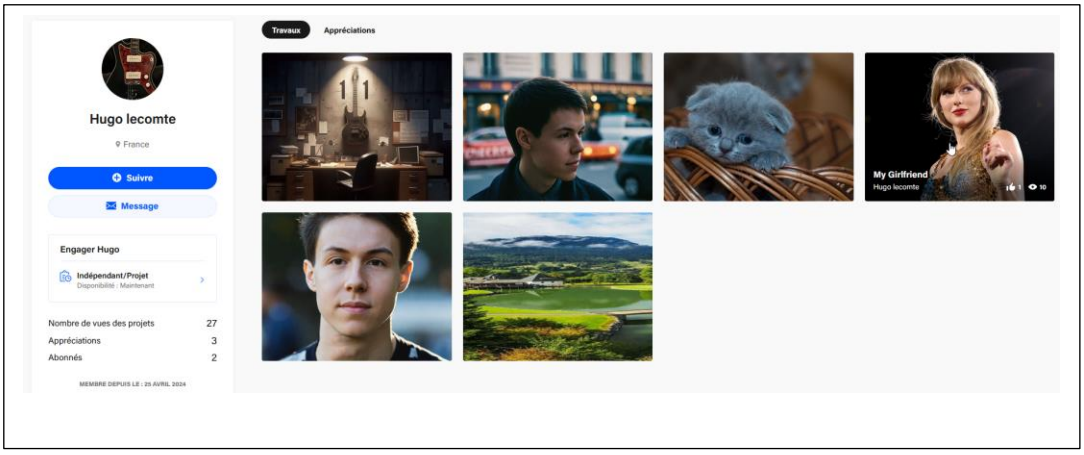
La réponse à ce challenge était donc : hacko{chemin_de_la_cote_pugin-combloux}

Challenge : Petite Amie

Pour ce challenge, nous devons lire la description du compte Instagram de Hugo.



Nous savons alors qu'il aime la photographie et qu'il est potentiellement sur Behance sous le pseudonyme « HL1 » hugolecomte1 Après quelques recherches sur des sites de photographie, nous retrouvons son compte sur Behance : https://www.behance.net/hugolecomte1.



Sa « petite amie » est donc Taylor Swift.

hacko{taylor_swift}

Acte 5 : La chute

Challenge : Un bon ami

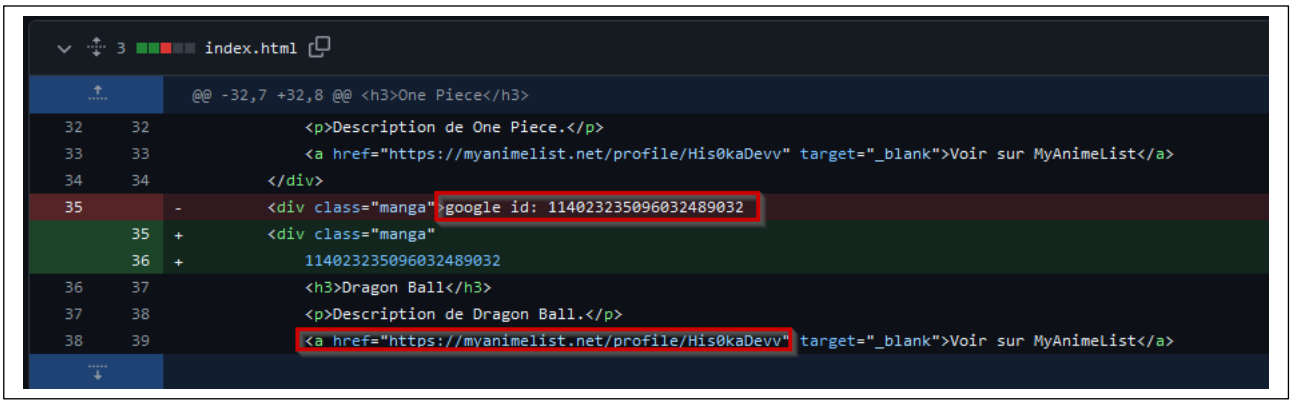
En lisant l'énoncé du challenge, nous savons que « NeverBeAlone12 », alias Hugo Lecomte, travaille avec un autre membre d'APT-509 sur un projet. En observant le GitHub de NeverBeAlone12, nous constatons qu'il a collaboré avec un certain LimaDevv sur un projet intitulé « WebTaskManager » : https://github.com/NeverBeAlone12/WebTaskManager.

La réponse à ce challenge est donc : hacko{limadevv}.

Challenge : [BONUS] Animé

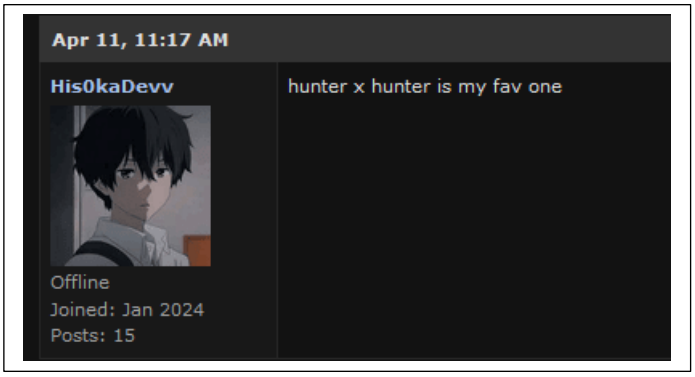
Nous avons maintenant le pseudonyme d'un nouveau membre d'APT-509, « LimaDevv », et un nouveau GitHub à analyser : https://github.com/LimaDevv.

En regardant l'historique de modification du dépôt « FanSite » de LimaDevv, nous retrouvons alors deux informations intéressantes :



Pour ce challenge, l'information la plus intéressante est le lien vers le profil MyAnimeList de LimaDevv, qui est disponible à l'adresse suivante : https://myanimelist.net/profile/His0kaDevv.

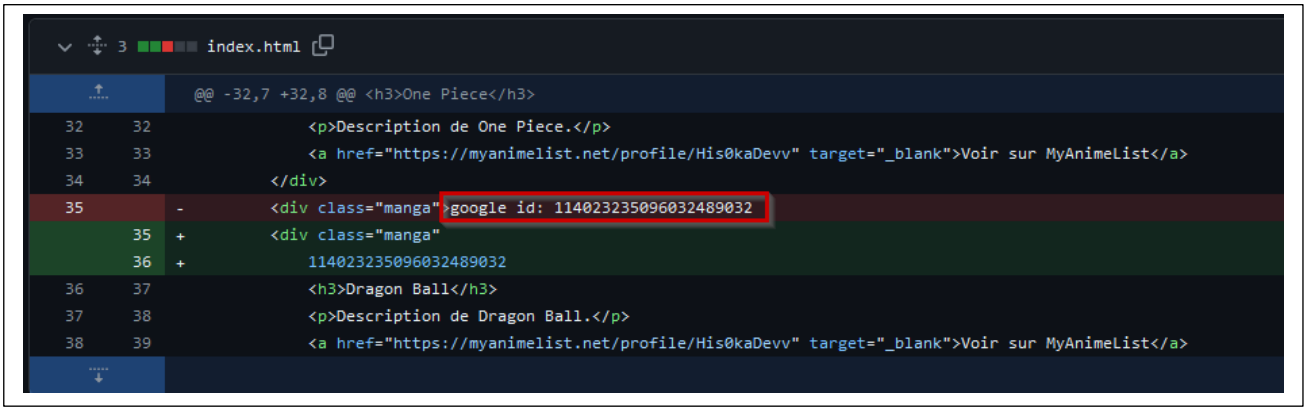
En examinant ses différentes interventions sur le forum, nous trouvons alors une réponse de LimaDevv sur un sujet évoquant son manga préféré : https://myanimelist.net/forum/?topicid=2081224&msgid=70860326.



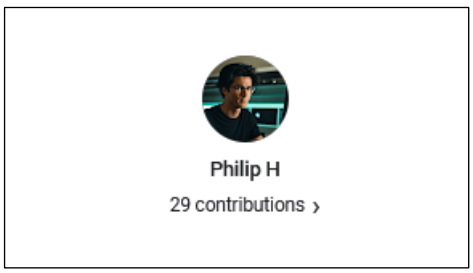
La réponse à ce challenge bonus était donc : hacko{hunter_x_hunter}

Challenge : Démasqué

Pour ce challenge, il est utile de se rappeler que nous avons précédemment trouvé un ID Google (GAIA ID) sur le GitHub de LimaDevv, qui est le suivant : 114023235096032489032.



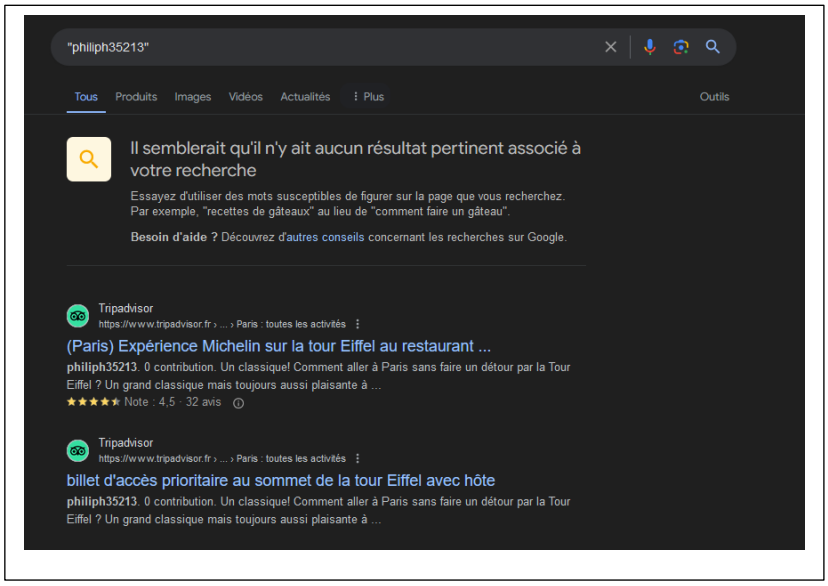
Grâce à cet ID, nous retrouvons son compte de contributeur Google Maps, accessible via le lien suivant : https://www.google.com/maps/contrib/114023235096032489032.



Nous avons alors découvert son prénom, "Philip", mais pas son nom de famille. En observant les différentes contributions (avis) qu'il a laissées, nous trouvons alors un nouveau pseudonyme :

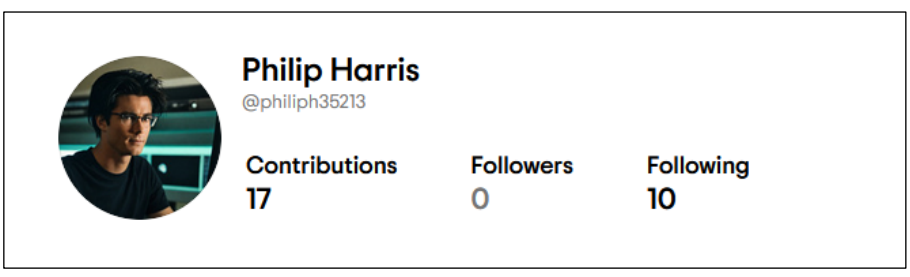
@Philiph35213

Grâce à une recherche utilisant des Google Dorks avec ce pseudonyme, nous découvrons alors que celui-ci possède un compte TripAdvisor :



https://www.tripadvisor.com/Profile/philiph35213

Nous avons finalement son identité complète : Philip Harris



La réponse à ce challenge était : hacko{philip_harris}

Challenge : L'arrestation

Pour ce challenge, il est important de nous concentrer sur nos découvertes. Sur la page TripAdvisor de Philip, nous retrouvons son adresse mail.

philip.h35213@gmail.com

Grâce à Epios (https://epieos.com/?q=philip.h35213%40gmail.com&t=email), nous pouvons accéder au calendrier Google de Philip.

https://calendar.google.com/calendar/u/0/embed?src=philip.h35213@gmail.com

Nous nous apercevons alors que ce calendrier est public et accessible par tous.

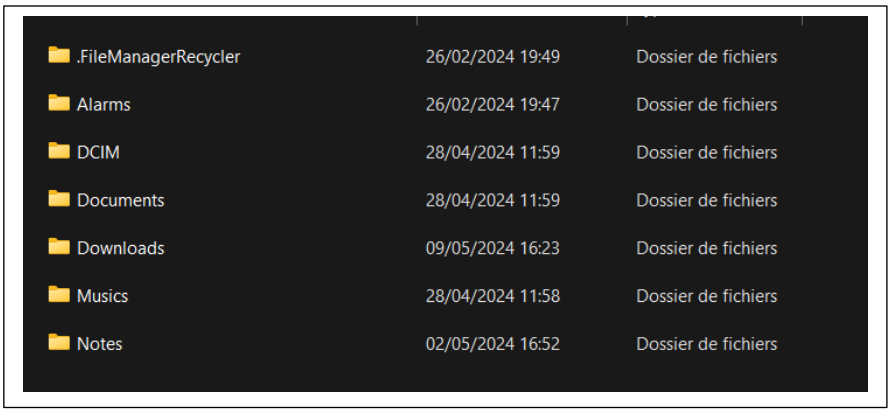
En examinant les différents événements du calendrier, nous constatons que Philip se rend fréquemment à un événement nommé « Diner dans ce super restau ! ». La première occurrence de cet événement dans son calendrier date de décembre 2023.

En consultant les avis laissés par Philip sur TripAdvisor, nous découvrons qu'il a dîné au restaurant « Le Harner » à Lyon en décembre 2023.

Philip peut être alors arrêté dans ce fameux restaurant : hacko{le_harner}

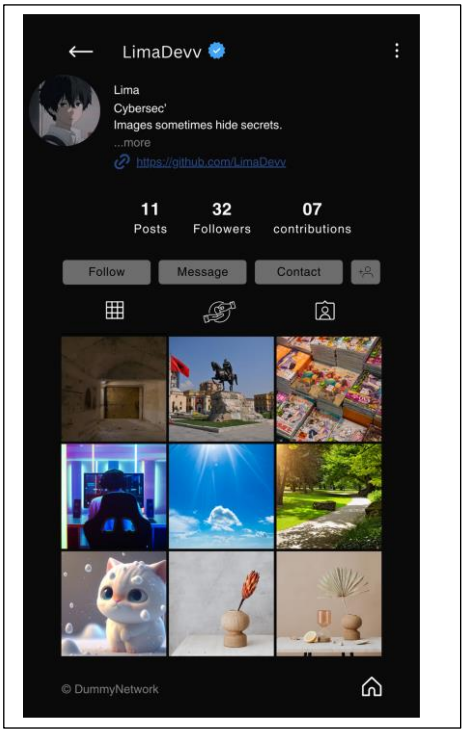
Challenge : Coup fatal 1

Pour ce challenge, nous avons un fichier .zip avec des informations extraites du téléphone de Philip. Comme pour le drive de Charlotte, il est essentiel de trier et d'identifier ce qui est réellement pertinent pour notre enquête. Analysons attentivement le contenu pour en extraire les éléments clés.

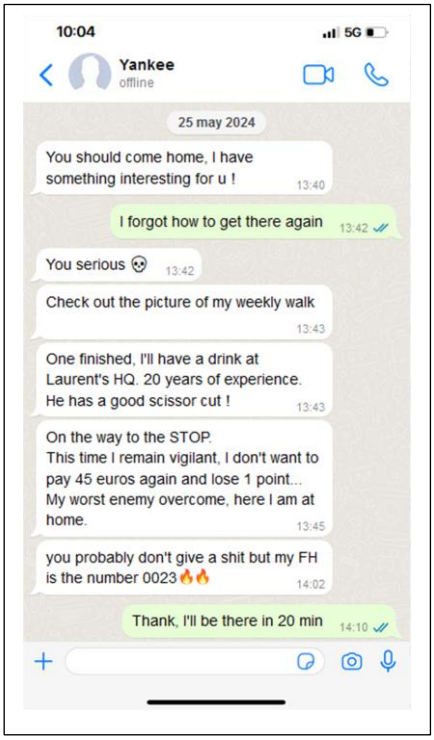


Voici les éléments pertinents trouvés dans son téléphone :

DCIM\Screenshots :



Screenshot de son profil d'un Réseau social



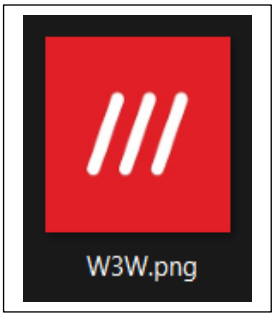
Screenshot d'une conversation avec une certaine « Yankee »

DCIM\Camera :

Photo prise à l'intérieur d'un « bunker »

Dans le repertoire Downloads :

Un fichier .mbox

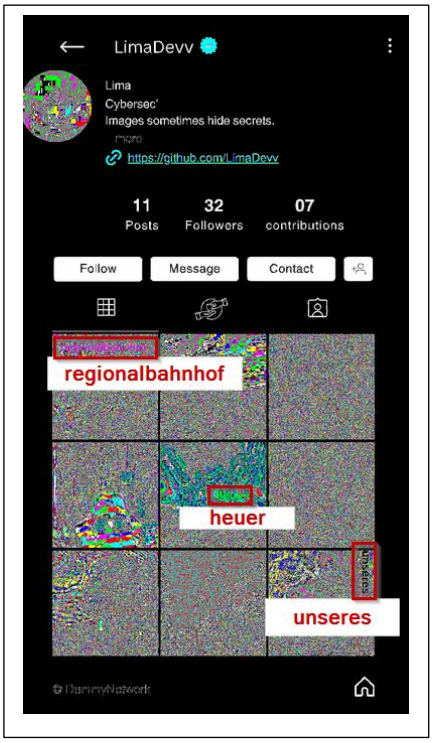


Icon du site W3W

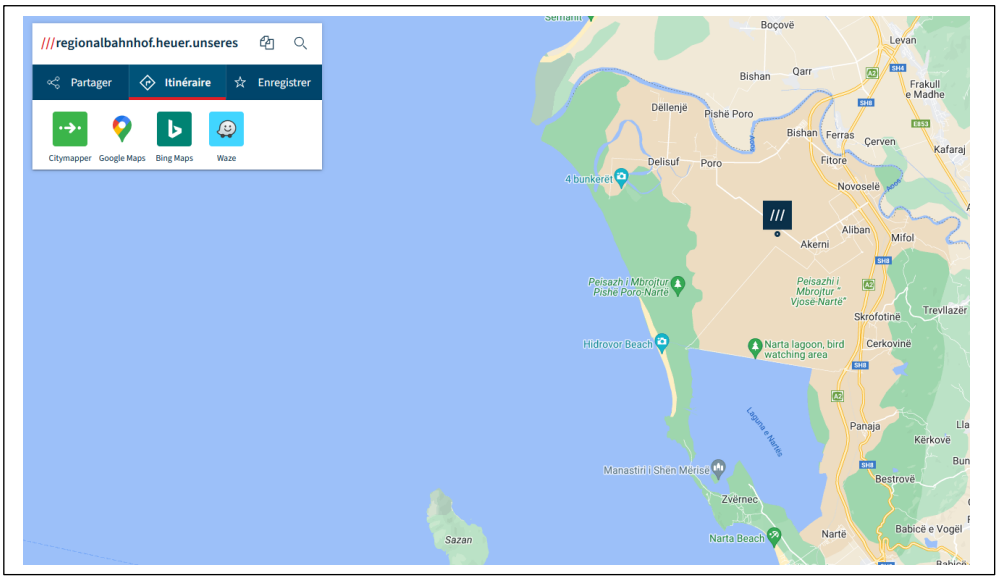
Dans le repertoire Notes :

Un fichier .txt contenant une chaine de caractère suspecte

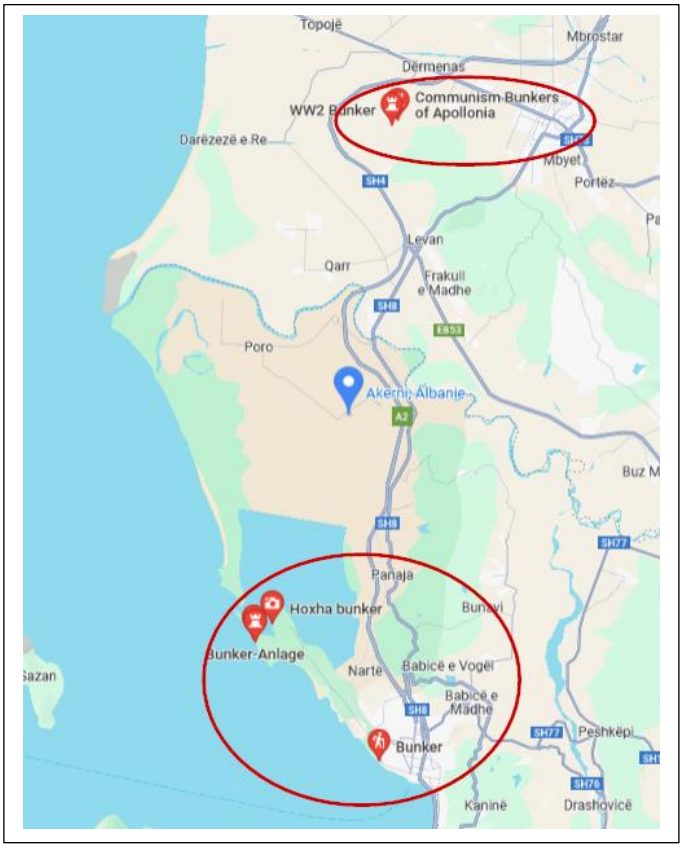
Pour ce premier challenge, nous tentons d'identifier le nom du bunker où se cache APT-509. En examinant de plus près la capture d'écran de son profil Instagram, nous observons que certains mots y sont dissimulés (stéganographie). En analysant cette photo sur Aperisolve (https://www.aperisolve.com/), nous réussissons à déceler trois mots cachés :



En utilisant le site What3Words (https://what3words.com/regionalbahnhof.heuer.unseres), nous obtenons une position GPS précise. Nous nous trouvons en Albanie, à l'aéroport d'Akerni.



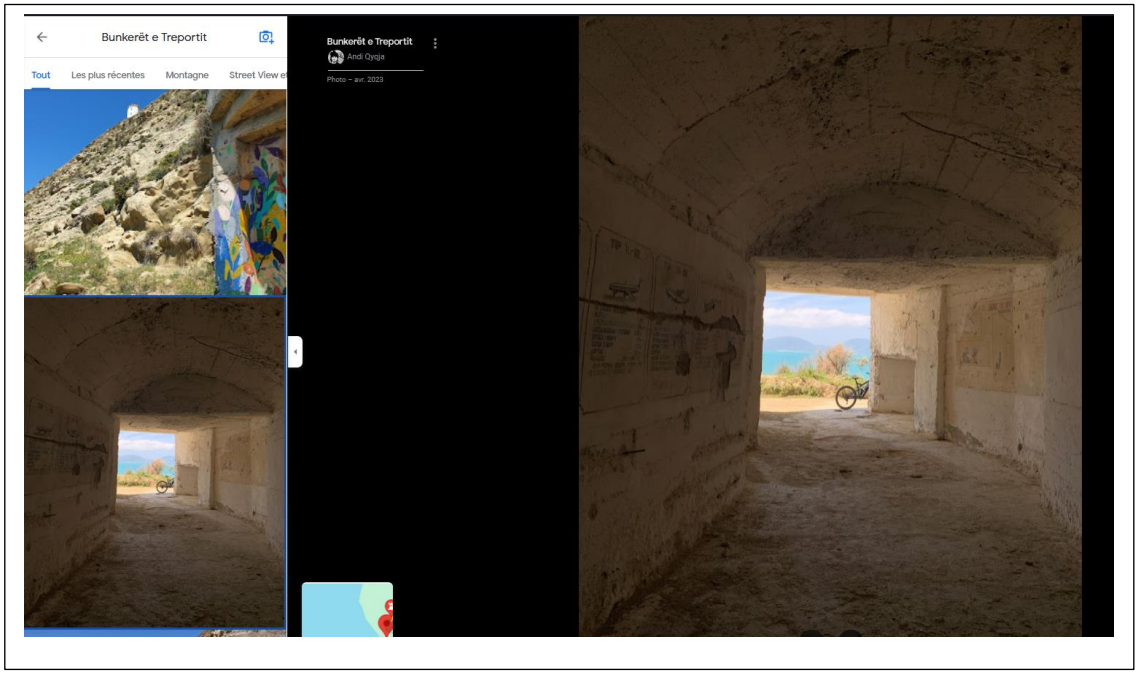
Cependant, nous ne sommes pas directement sur un bunker. Pour localiser les bunkers à proximité de ce lieu, nous utilisons Google Maps. Nous trouvons plusieurs bunkers non loin de cet endroit :



Nous nous rappelons alors la photo de l'intérieur d'un bunker que nous avons trouvée dans le téléphone de Philip. Cela pourrait nous aider à identifier le bunker spécifique parmi ceux repérés à proximité de l'aéroport d'Akerni.

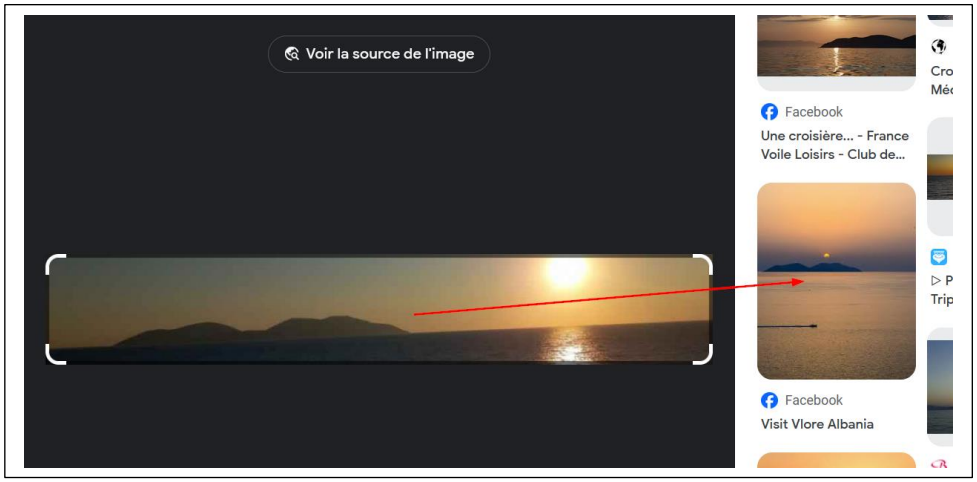
Photo prise à l'intérieur d'un « bunker »

En comparant les différents bunkers que nous avons trouvés ainsi que les photos associées à leurs avis sur Google Maps, nous identifions une photo qui ressemble fortement à celle trouvée dans le téléphone de Philip.



APT-509 se cache alors dans le bunker : Bunkerët e Treportit situé à Zvernec en Albanie

Pour les plus observateurs, il était possible de trouver ce lieu facilement grâce à la photo de couverture de la chaîne YouTube d'APT-509.

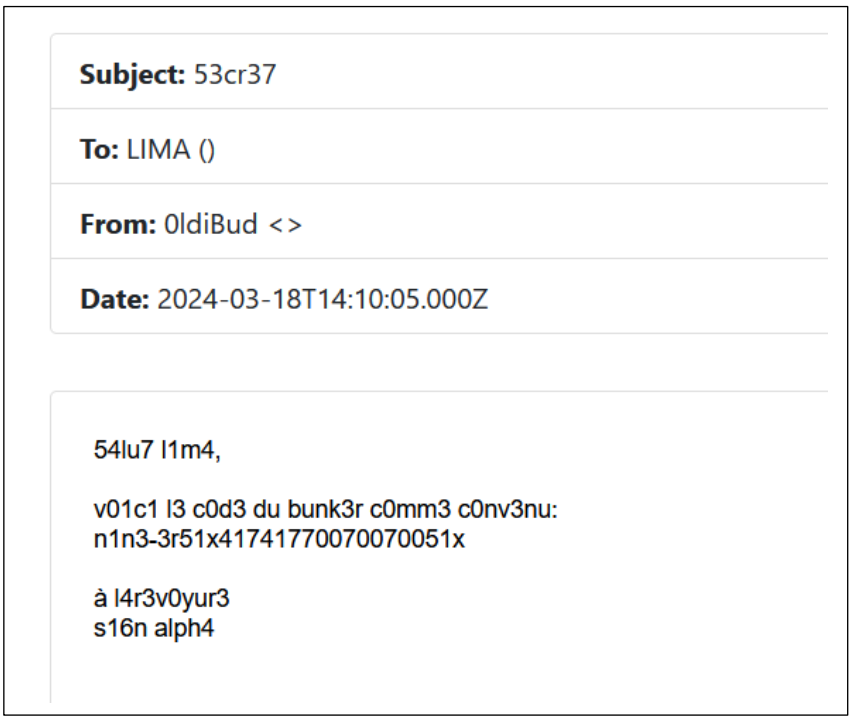


La réponse à ce challenge est donc : hacko{bunkeret_e_treportit}

autre réponse acceptée : hacko{bunkeret_e_zvernecit}

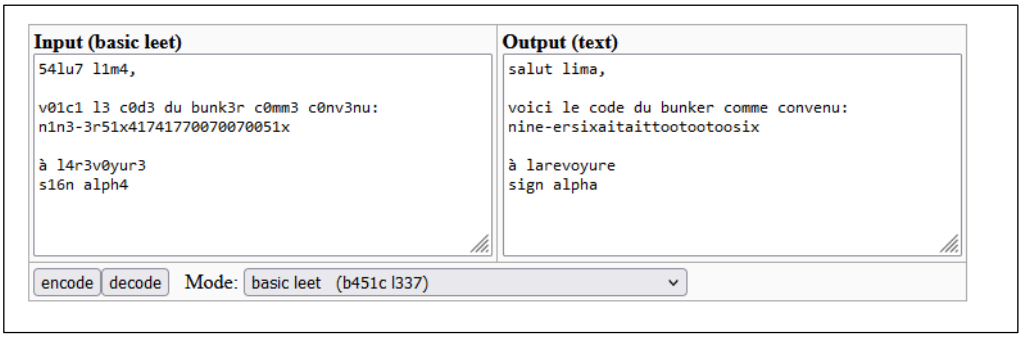
Challenge : Coup fatal 2

Pour ce challenge, il est crucial de continuer à examiner les informations pertinentes trouvées dans le téléphone de Philip. Pour rappel, lors du challenge « Coup fatal 1 », nous avons découvert un fichier nommé inbox.mbox. Nous allons maintenant ouvrir ce fichier à l'aide du site : https://www.mbox-viewer.com/.



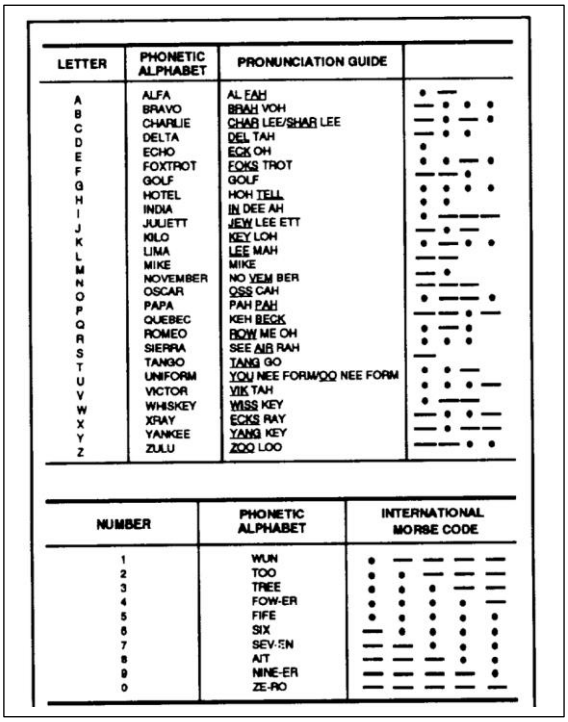
Nous retrouvons un mail intéressant ayant comme sujet « Secret ».

Nous pouvons lire :



(https://www.robertecker.com)

Le code du bunker est alors transmis en utilisant l'alphabet de l'OTAN :



LETTER	PHONETIC ALPHABET	PRONUNCIATION GUIDE
A	ALFA	AL FAH
B	BRAVO	BRAH VOH
C	CHARLIE	CHAR LEE/SHAR LEE
D	DELTA	DEL TAH
E	ECHO	ECK OH
F	FOXTROT	FOKS TROT
G	GOLF	GOLF
H	HOTEL	HOH TELL
I	INDIA	IN DEE AH
J	JULIETT	JEW LEE ETT
K	KILO	KEY LOH
L	LIMA	LEE MAH
M	MIKE	MIKE
N	NOVEMBER	NO VEM BER
O	OSCAR	OSS CAH
P	PAPA	PAH PAH
Q	QUEBEC	KEH BECK
R	ROMEO	ROW ME OH
S	SIERRA	SEE AIR RAH
T	TANGO	TANG GO
U	UNIFORM	YOU NEE FORM/OO NEE FORM
V	VICTOR	VIK TAH
W	WHISKEY	WISS KEY
X	XRAY	ECKS RAY
Y	YANKEE	YANG KEY
Z	ZULU	ZOO LOO

NUMBER	PHONETIC ALPHABET	INTERNATIONAL MORSE CODE
1	WUN	
2	TOO	
3	TREE	
4	FOW-ER	
5	FIFE	
6	SIX	
7	SEV-EN	
8	AIT	
9	NINE-ER	
0	ZE-RO	

Le code du bunker est alors : 96882226

La réponse au challenge était : hacko{96882226}

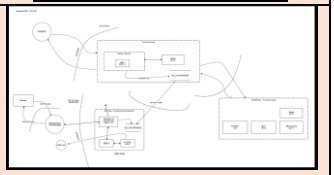
Acte 6 : Opération Spéciale

Challenge : Coup de tonnerre !

Ce challenge nous permet de vous expliquer comment s'est déroulée l'opération policière visant à arrêter les cybercriminels dans leur bunker en Albanie. Malheureusement, les forces de l'ordre sont arrivées trop tard. Les cybercriminels avaient déjà quitté les lieux, laissant derrière eux la note suivante :

"Vous avez été trop lents ! Nous sommes déjà loin, bonne chance pour nous retrouver. N'oubliez pas, nous sommes des fantômes."

À la suite de cela, la police vous fournit un fichier d'enquête intitulé : APT-509-CASE.html.

Page	Screenshot
Première page https://hackolyte.fr/assets/img/TB6LEKoR&k&4cG6A.png	
Deuxième page Caractéristiques sur la mission https://hackolyte.fr/assets/img/8he3i3Fxh7dMDJqP.png	
Troisième page Regroupant la position du bunker et des photos prises à l'intérieur de celui-ci. https://hackolyte.fr/assets/img/gdKP3iT!gmJQgSEr.png	
Quatrième page Photos de la salle serveur retrouvée à l'intérieur du bunker https://hackolyte.fr/assets/img/hQRGQc6coQnxkB8A.png	
Page annexe « élément notable » Schéma SI retrouvé dans la salle serveur du bunker https://hackolyte.fr/assets/img/A86K3eYLTjK5xT93FSh.png	

Cinquième Page Tableau de liège retrouvé dans le bureau d'un prénommé « Alpha ». https://hackolyte.fr/assets/img/eiJRMoB5o54c3t7m.png	

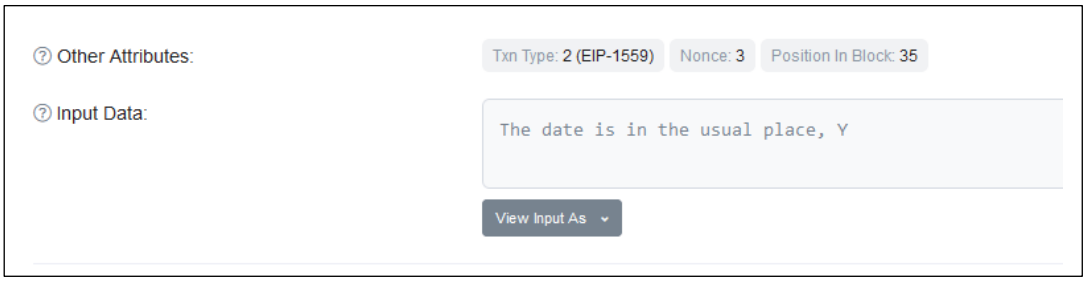
Acte 7 : La commerciale

Challenge : Révèle ton secret !

Conformément à l'énoncé, il est essentiel de prendre du recul et d'examiner toutes les informations à notre disposition. Nous devons à présent identifier la personne responsable des activités de vente liées à APT-509.

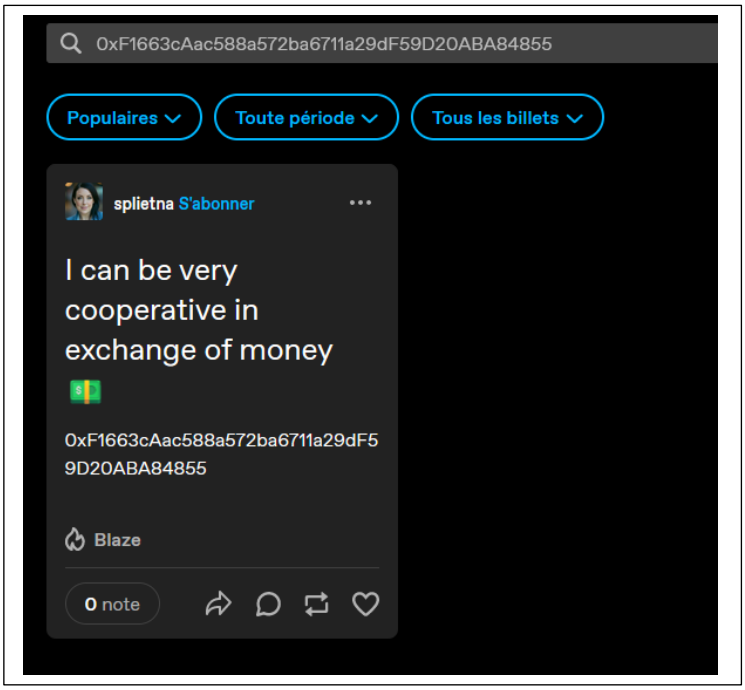
Grâce à nos avancées précédentes, nous avons découvert un nouveau nom de code : « Yankee ». Nous supposons donc que nous devons retrouver la personne qui se cache derrière ce pseudonyme.

Concernant « Yankee », nous disposons uniquement d'une conversation WhatsApp trouvée dans le téléphone de Lima. De plus, si vous avez minutieusement examiné le portefeuille de Quentin Morel, vous avez découvert un message dans un virement, signé par un « Y » (lien : https://basescan.org/tx/0x11e61841bc973067f3d0152195b40a554c21f6e76143785ee8204a4108f3aebe) . Cette information pourrait être cruciale pour relier les points entre ces différents éléments.



Nous avons donc confirmé que Yankee est associé à l'adresse de wallet : 0xF1663cAac588a572ba6711a29dF59D20ABA84855.

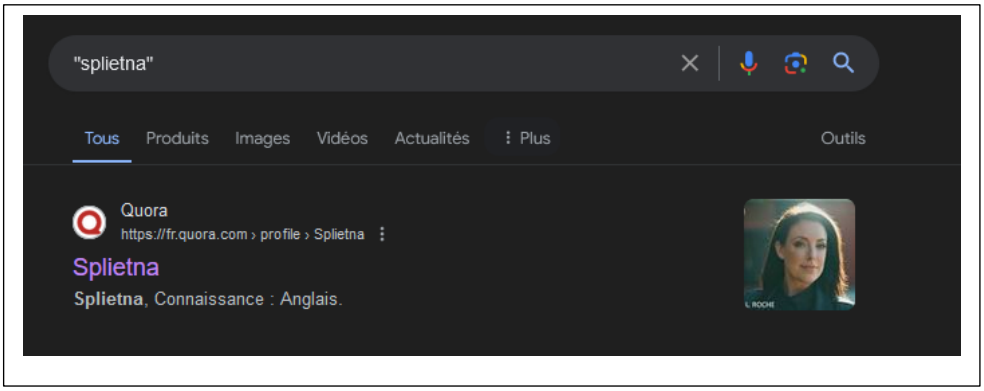
Ces deux informations constituent nos seules pistes sur Yankee pour le moment. Nous allons donc approfondir notre enquête sur cette adresse de wallet. Il arrive parfois que des individus partagent leur adresse de wallet sur les réseaux sociaux. Après une recherche approfondie sur différents réseaux, nous découvrons un post de Yankee sur le réseau social Tumblr.



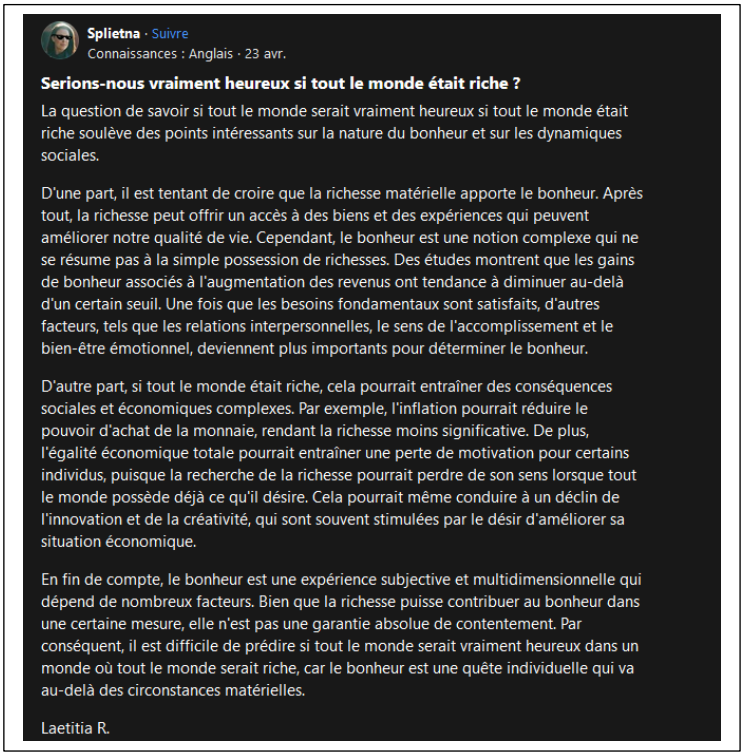
(https://www.tumblr.com/splietna)

Nous avons découvert un pseudonyme associé à Yankee : Splietna.

Pour ce challenge, nous allons nous intéresser à un post de Splietna sur Tumblr où il mentionne qu'il répond à des questions en ligne. En utilisant des recherches Dorks, nous trouvons son profil sur Quora, une plateforme de questions-réponses en ligne.



Une fois sur Quora, nous trouvons les publications de Splietna. Dans une de ses réponses, elle signe « Laetitia R. ». Cette signature nous donne un indice précieux sur l'identité réelle derrière le pseudonyme Splietna.



Splietna · Suivre
Connaissances : Anglais · 23 avr.

Serions-nous vraiment heureux si tout le monde était riche ?

La question de savoir si tout le monde serait vraiment heureux si tout le monde était riche soulève des points intéressants sur la nature du bonheur et sur les dynamiques sociales.

D'une part, il est tentant de croire que la richesse matérielle apporte le bonheur. Après tout, la richesse peut offrir un accès à des biens et des expériences qui peuvent améliorer notre qualité de vie. Cependant, le bonheur est une notion complexe qui ne se résume pas à la simple possession de richesses. Des études montrent que les gains de bonheur associés à l'augmentation des revenus ont tendance à diminuer au-delà d'un certain seuil. Une fois que les besoins fondamentaux sont satisfaits, d'autres facteurs, tels que les relations interpersonnelles, le sens de l'accomplissement et le bien-être émotionnel, deviennent plus importants pour déterminer le bonheur.

D'autre part, si tout le monde était riche, cela pourrait entraîner des conséquences sociales et économiques complexes. Par exemple, l'inflation pourrait réduire le pouvoir d'achat de la monnaie, rendant la richesse moins significative. De plus, l'égalité économique totale pourrait entraîner une perte de motivation pour certains individus, puisque la recherche de la richesse pourrait perdre de son sens lorsque tout le monde possède déjà ce qu'il désire. Cela pourrait même conduire à un déclin de l'innovation et de la créativité, qui sont souvent stimulées par le désir d'améliorer sa situation économique.

En fin de compte, le bonheur est une expérience subjective et multidimensionnelle qui dépend de nombreux facteurs. Bien que la richesse puisse contribuer au bonheur dans une certaine mesure, elle n'est pas une garantie absolue de contentement. Par conséquent, il est difficile de prédire si tout le monde serait vraiment heureux dans un monde où tout le monde serait riche, car le bonheur est une quête individuelle qui va au-delà des circonstances matérielles.

Laetitia R.

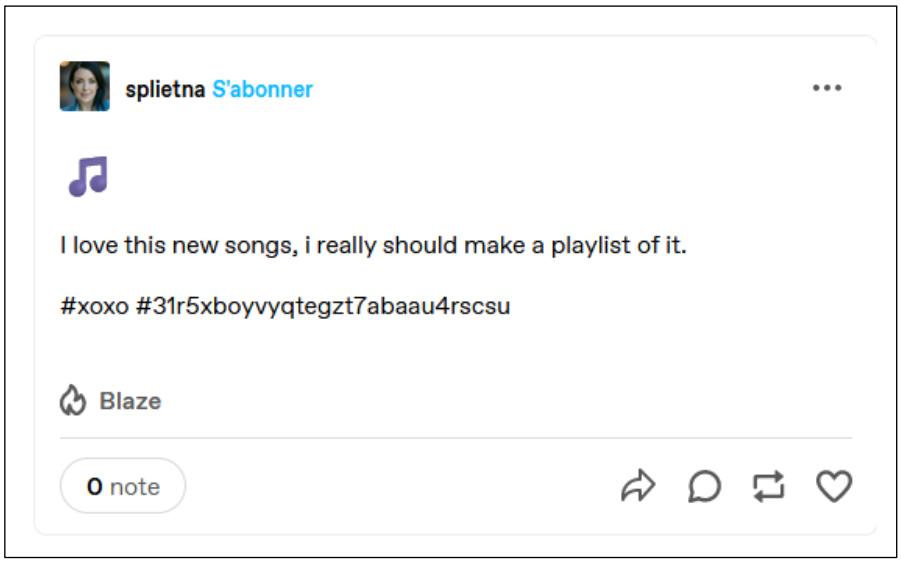
Nous avons donc son prénom, Laetitia. Pour retrouver son nom de famille, rappelons-nous que nous l'avons vu lors de notre recherche Dorks. Il apparaît sur sa photo de profil sur Quora : https://qph.cf2.quoracdn.net/main-thumb-2552810573-200-rmdzkzvcwhxsaberbibxaeczsrtdvzeg.jpeg.

La personne se cachant derrière Yankee est alors Laetitia Roche.

La réponse attendue était : hacko{laetitia_roche}

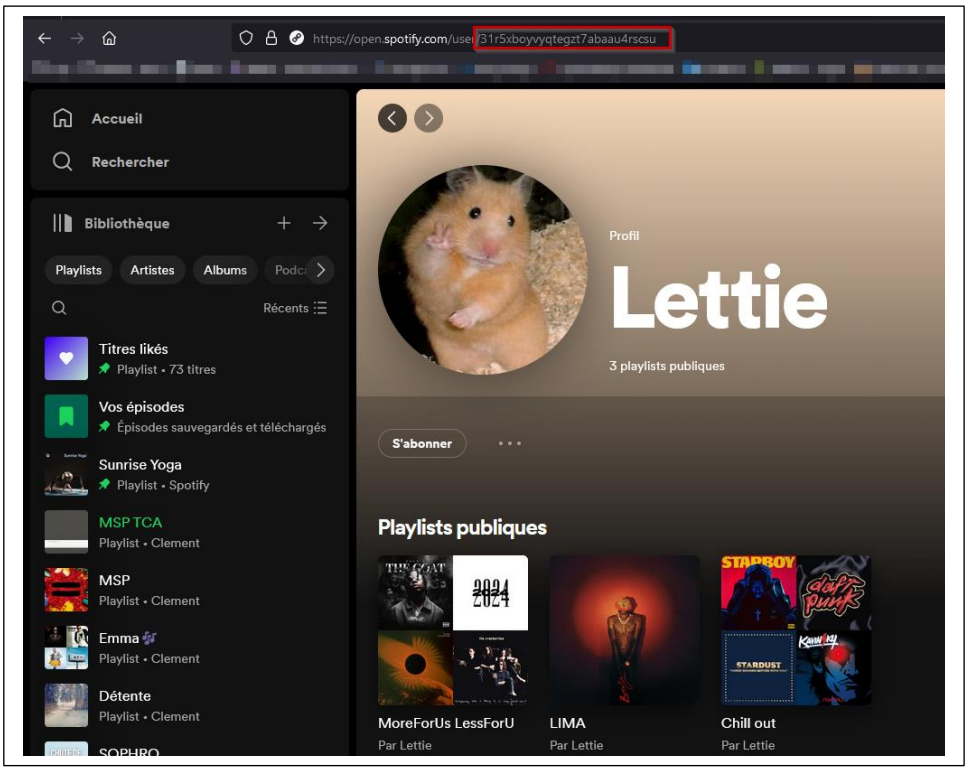
Challenge : La transaction 2

Pour ce challenge, nous devons déterminer la date à laquelle l'argent de Charlotte quittera la France. En explorant le Tumblr de Laetitia, nous tombons sur un post où elle parle d'une musique qu'elle envisage d'ajouter à sa playlist. Ce détail pourrait nous fournir des indices supplémentaires sur le timing de ses actions :

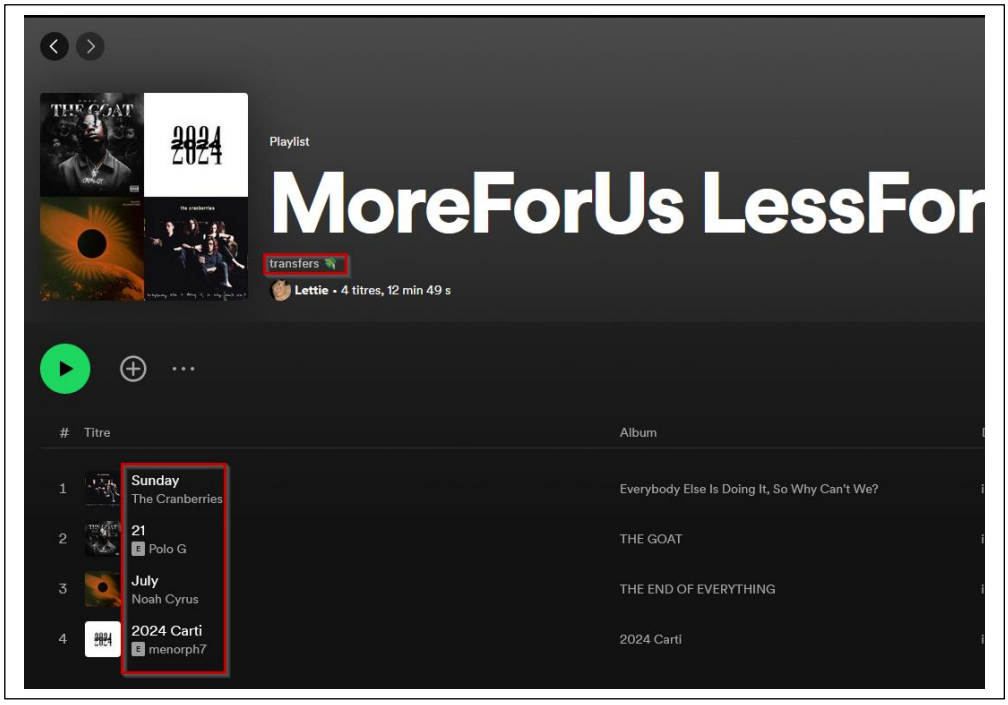


Nous remarquons un hashtag inhabituel : #31r5xboyvyqtegzt7abaau4rscsu. En recherchant ce hashtag, nous découvrons le profil de Laetitia sur Spotify : https://open.spotify.com/user/31r5xboyvyqtegzt7abaau4rscsu.

Ce lien pourrait nous offrir plus d'indices sur ses activités ou ses plans.



C'est dans la première playlist créée par Laetitia que nous découvrons la date du transfert d'argent : https://open.spotify.com/playlist/3xfbvTGAhDpXXIr5bWMi0E.

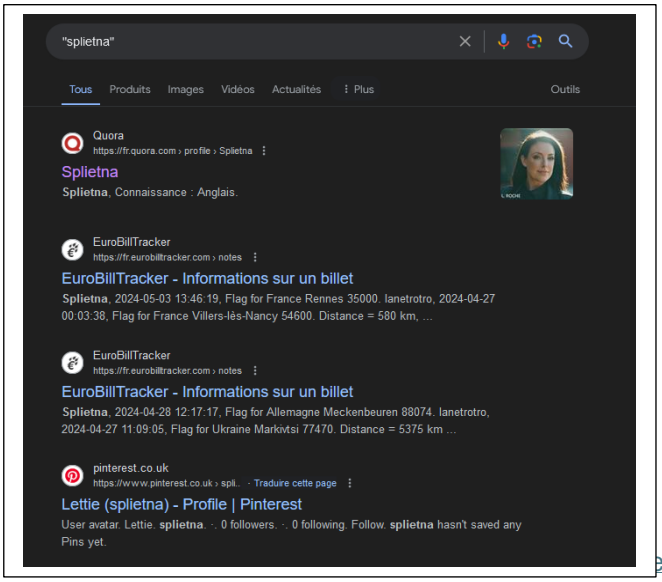


Grâce aux titres des chansons dans la playlist, nous avons pu déduire que le virement est prévu pour le dimanche 21 juillet 2024.

Réponse attendue : hacko{dimanche_21_juillet_2024}

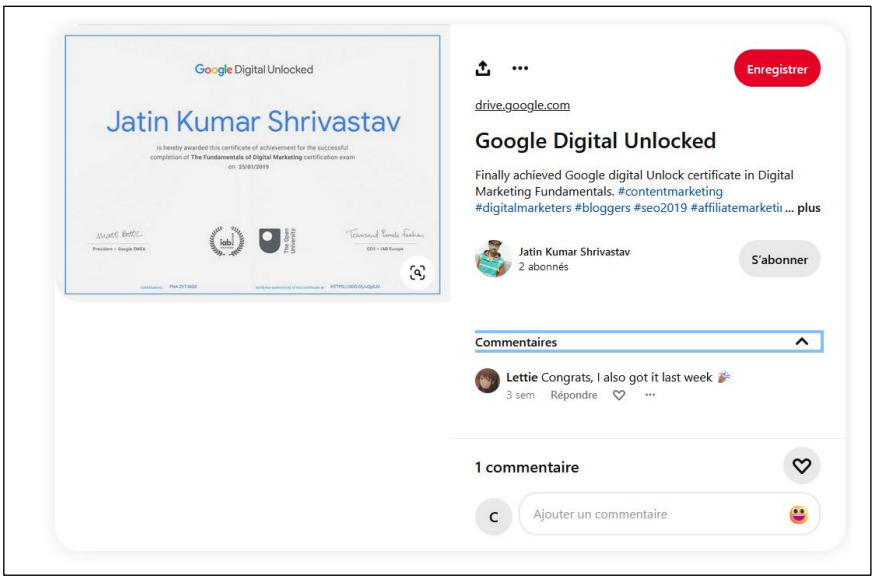
Challenge : La formation

Pour ce challenge, nous devons déterminer la dernière formation suivie par Laetitia. À l'instar du challenge « Révèle ton secret ! », une recherche Dorks utilisant son pseudonyme révèle qu'elle possède un compte Pinterest. En explorant ce compte, nous pourrions trouver des informations sur ses intérêts récents ou des formations qu'elle aurait épinglées.



est.co.uk/splietna/)

En explorant Pinterest, nous trouvons les éléments sauvegardés par Laetitia, y compris un commentaire qu'elle a laissé sur un post concernant une certification :



Elle a donc passé la formation : « The Fundamentals of Digital Marketing ».

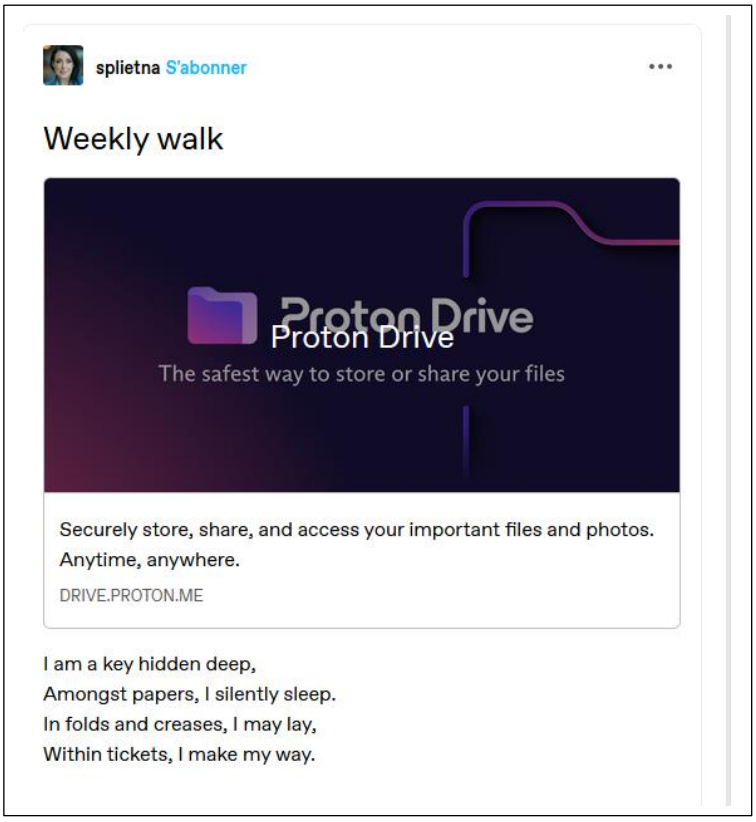
Flag attendu : hacko{the_fundamentals_of_digital_marketing}

Challenge : Toc Toc Toc !

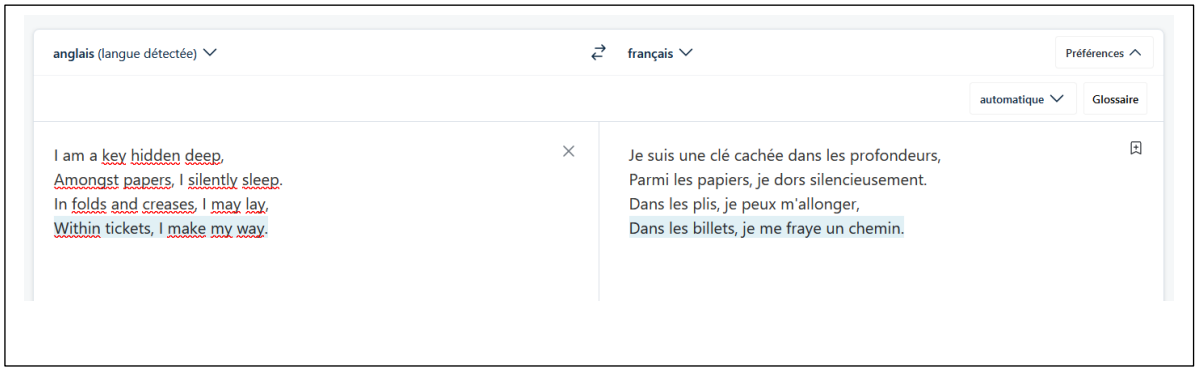
Pour ce challenge, nous devons déterminer l'adresse précise de Laetitia, également connue sous le nom de Yankee. En examinant son Tumblr, nous découvrons un post qui contient un lien vers un drive Proton appelé « Weekly Walk » (https://www.tumblr.com/splietna/749851813005721600/weekly-walk?source=share).

Voici le lien vers le drive Proton : https://drive.proton.me/urls/A7TBS4WDE4#DBFAl9UEVOBK.

Toutefois, l'accès est sécurisé par un mot de passe. Dans le post associé, nous trouvons un petit poème qui pourrait contenir des indices pour le mot de passe.

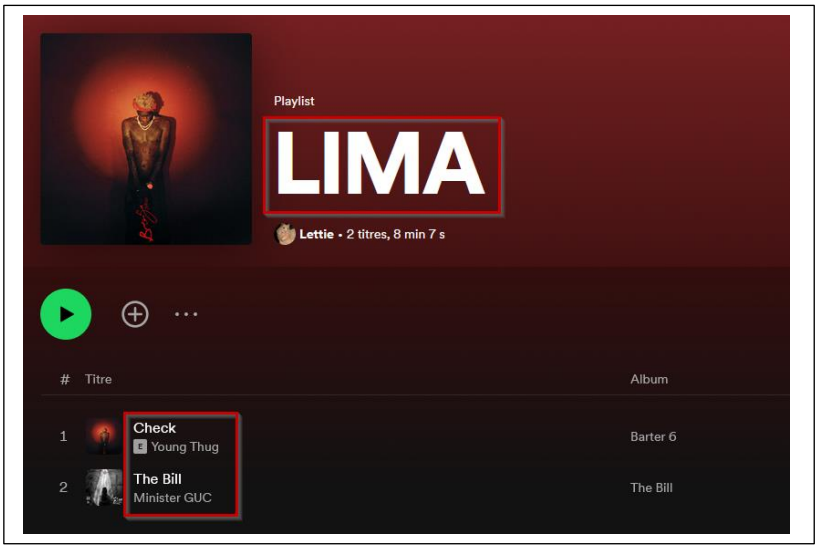


Voici la traduction :



En outre, sur son compte Tumblr, nous découvrons un post où elle montre un billet, accompagné de la légende : « A new one in my collection 💵 ».

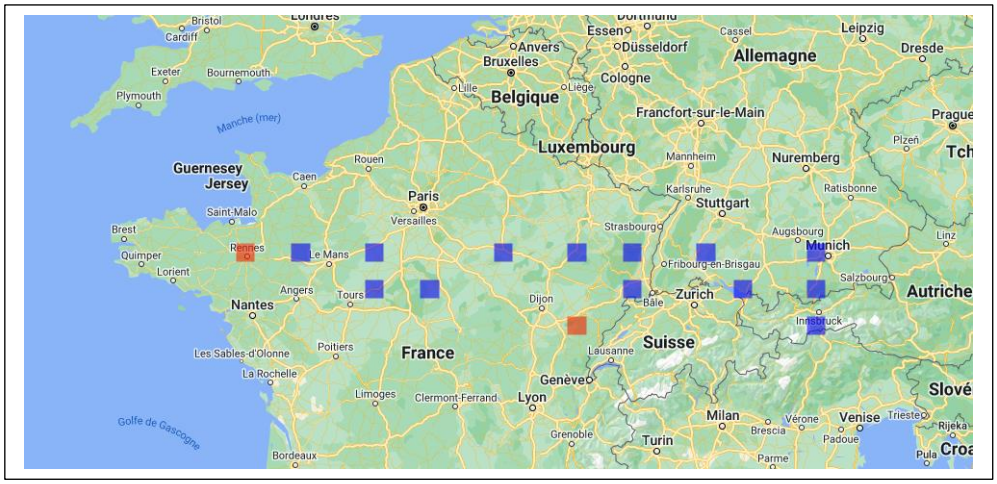
Finalement, sur son compte Spotify, nous trouvons une playlist intitulée "Lima" où Yankee (Laetitia) mentionne de « Regarder les billets ».



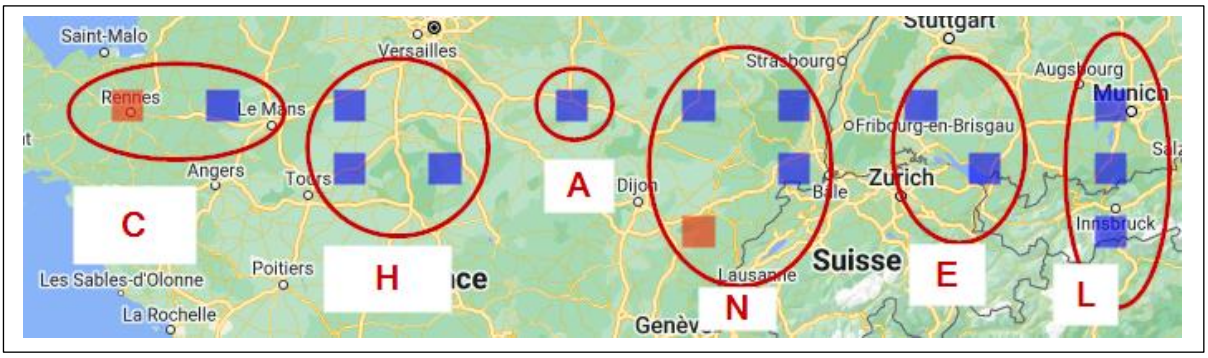
Nous pouvons alors en déduire que toutes ces trouvailles pourraient nous aider à déterminer le mot de passe. Nous allons vérifier sur Eurobillet (un site en ligne pour enregistrer des billets) si Laetitia possède un compte.

Nous avons découvert sur ce site un compte sous le nom de « Splietna ». L'analyse du profil révèle qu'elle a enregistré un total de 17 billets. En consultant l'onglet « carte » de son profil, nous visualisons les emplacements des billets enregistrés par Laetitia sur une carte.

(https://fr.eurobilltracker.com/map/usernotes.php?user=238173;key=363ab212aefa3a52364b;engine=gmb).



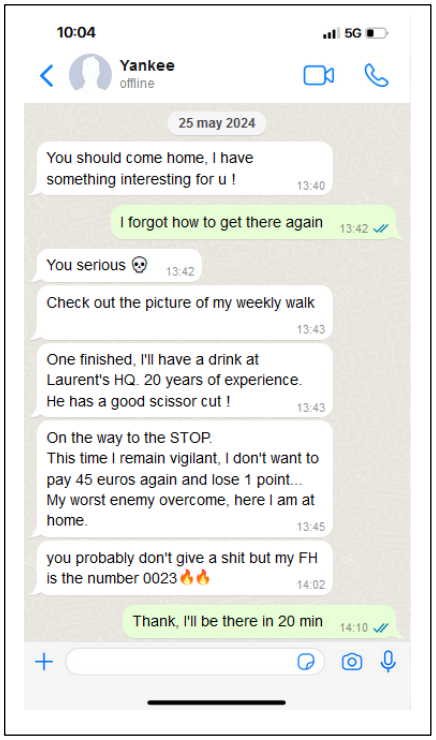
Cependant, la disposition des billets sur la carte est inhabituelle. Il semble que cela puisse représenter un mot écrit en braille.



Une fois décodé nous trouvons le mot : chanel

Excellent ! Avec le drive ouvert, nous trouvons une photographie de la balade hebdomadaire de Laetitia, qui pourrait nous révéler des indices supplémentaires sur son emplacement actuel ou ses activités habituelles.

Nous avons maintenant un point de départ ! De plus, rappelons-nous que nous avions découvert une conversation entre Lima et Yankee sur le téléphone de Lima.



Nous pouvons utiliser cette conversation pour retrouver le domicile de Yankee.

Premièrement, nous devons identifier l'endroit où a été prise la photo stockée sur le drive Proton de Laetitia. L'image révèle le nom "Imprimerie de la tour". Nous explorons ensuite toutes les entreprises portant ce nom via le site Pappers (https://www.pappers.fr/recherche?q=Imprimerie+de+la+tour). L'aspect de l'imprimerie sur la photo laisse penser qu'elle est fermée. Nos recherches sur Pappers nous mènent à une entreprise située à APT, fermée mais correspondant à la description (https://www.pappers.fr/entreprise/imprimerie-de-la-tour-349831024).

En vérifiant l'adresse sur Maps, nous confirmons que l'imprimerie visible dans le drive de Laetitia se trouve au 33 rue René Cassin, 84400 APT.

Maintenant, nous analysons la capture d'écran trouvée dans le téléphone de Lima, qui indique que Lima a rendu visite à Yankee. Nous allons enquêter sur cette piste pour localiser précisément son domicile.

Voici ce que Yankee dit dans sa conversation avec Lima :

Nous avons déjà établi que Laetitia se promène régulièrement dans la ville d'APT grâce à la photo de sa marche hebdomadaire. À partir de là, nous explorons un indice supplémentaire qu'elle fournit : elle mentionne avoir pris un verre au siège social de Laurent, un professionnel avec plus de 20 ans d'expérience. Pour en savoir plus, nous utilisons Pappers pour identifier les entreprises à APT dont le propriétaire s'appelle Laurent et qui existent depuis environ 20 ans.

Voici notre recherche : https://www.pappers.fr/recherche?q=Laurent&date_creation_min=01-05-1998&date_creation_max=04-06-2000&ville=84400.

Parmi les 11 résultats obtenus, une entreprise de coiffure semble particulièrement pertinente : https://www.pappers.fr/entreprise/guichard-420616351. L'adresse du siège social est trouvée à HAMEAU DU CHENE, 1015 RTE D'APT, 84400 APT.

Poursuivons notre analyse de la conversation entre Yankee et Lima. Elle mentionne ensuite : « En direction du STOP... ». Heureusement, juste à côté du siège social de Laurent, il y a un restaurant appelé « Le Stop ». Cela indique qu'elle a pris la route en direction de ce restaurant, situé sur l'axe routier D900. Ces détails nous aident à mieux comprendre son trajet et à affiner notre recherche de son domicile.

Dans son message, elle mentionne la perte d'un point et une amende de 45 euros, ce qui suggère qu'elle a été flashée par un radar. Pour identifier le radar en question, nous allons consulter le site officiel du gouvernement français qui répertorie tous les radars : https://radars.securite-routiere.gouv.fr/#/

Effectivement, il y a un radar sur l'axe D900, précisément avant d'arriver à la localité appelée « Beaumettes ». Cela nous permet de confirmer la route qu'elle a empruntée et de se rapprocher encore plus de son domicile potentiel.

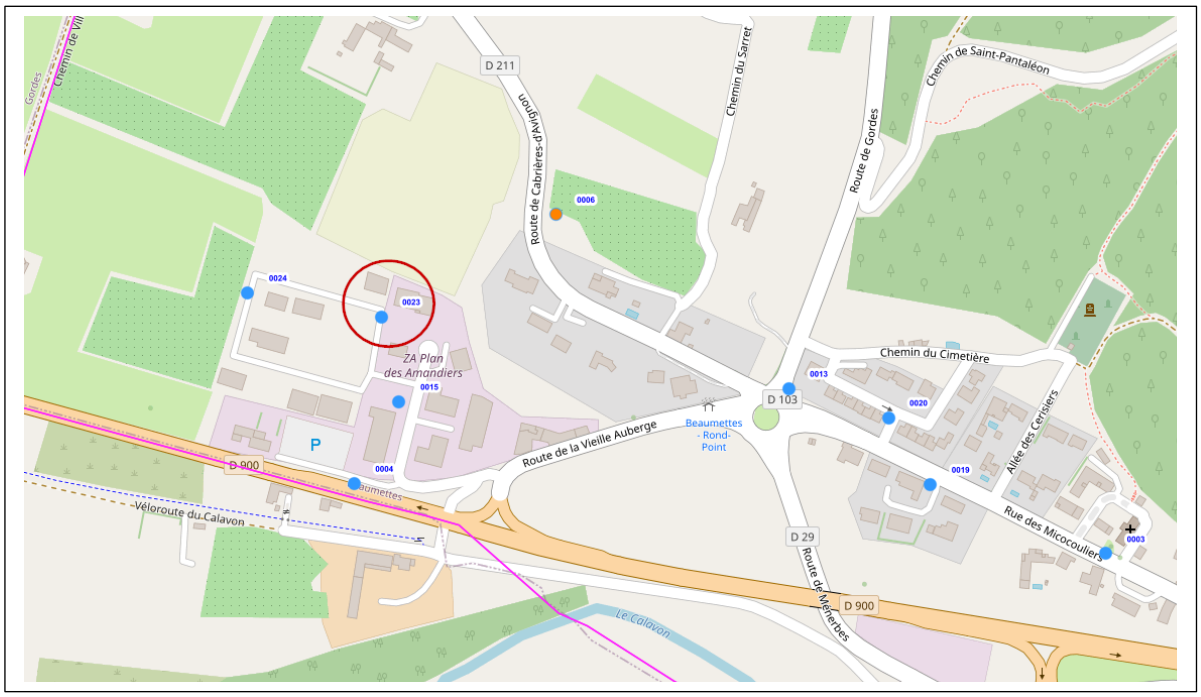
Il ne reste plus qu'à retrouver sa maison. Dans son message, Laetitia mentionne que sa mission est située près du « FH 0023 ». Nous devons comprendre ce que signifie « FH ». Pour cela, nouspouvons utiliser Google pour nous aider.
https://www.collinsdictionary.com/dictionary/english/fh

Nous découvrons alors que FH correspond à « Fire hydrant », ce qui se traduit par bouche d'incendie en français.

Nous devons ensuite localiser un site qui recense et fournit des informations sur toutes les bouches d'incendie présentes à Beaumettes.

Après une recherche sur Google, nous trouvons le site du SDIS 84 qui inclut une carte des bouches d'incendie de la région : https://deci.sdis84.fr/carte-des-pei

Nous cherchons maintenant la bouche d'incendie numéro 0023 dans la ville :



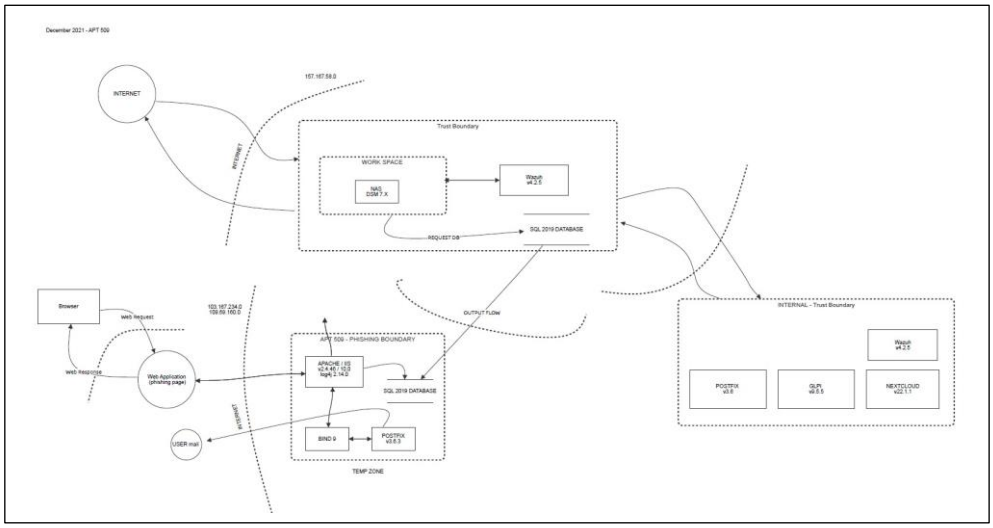
Laetitia alias Yankee habite alors au coordonnées : 43.86085964979977, 5.192963919596549

La réponse au challenge était donc : hacko{43.8608,5.1929}

Acte 8 : Plan blanc

Challenge : Vulnérabilité

Pour ce challenge, nous allons uniquement nous intéresser aux technologies accessibles depuis Internet (potentiel point d'entrée pour la police). Le schéma a été réalisé avec l'outil OWASP Threat Dragon, disponible sur (https://owasp.org/www-project-threat-dragon/).



https://hackolyte.fr/assets/img/A86K3eYLTjK5xT93FSh.png

Voici un tableau récapitulatif des différentes technologies directement exposées sur Internet. Pour la classification, nous avons utilisé le site : https://www.cvedetails.com.

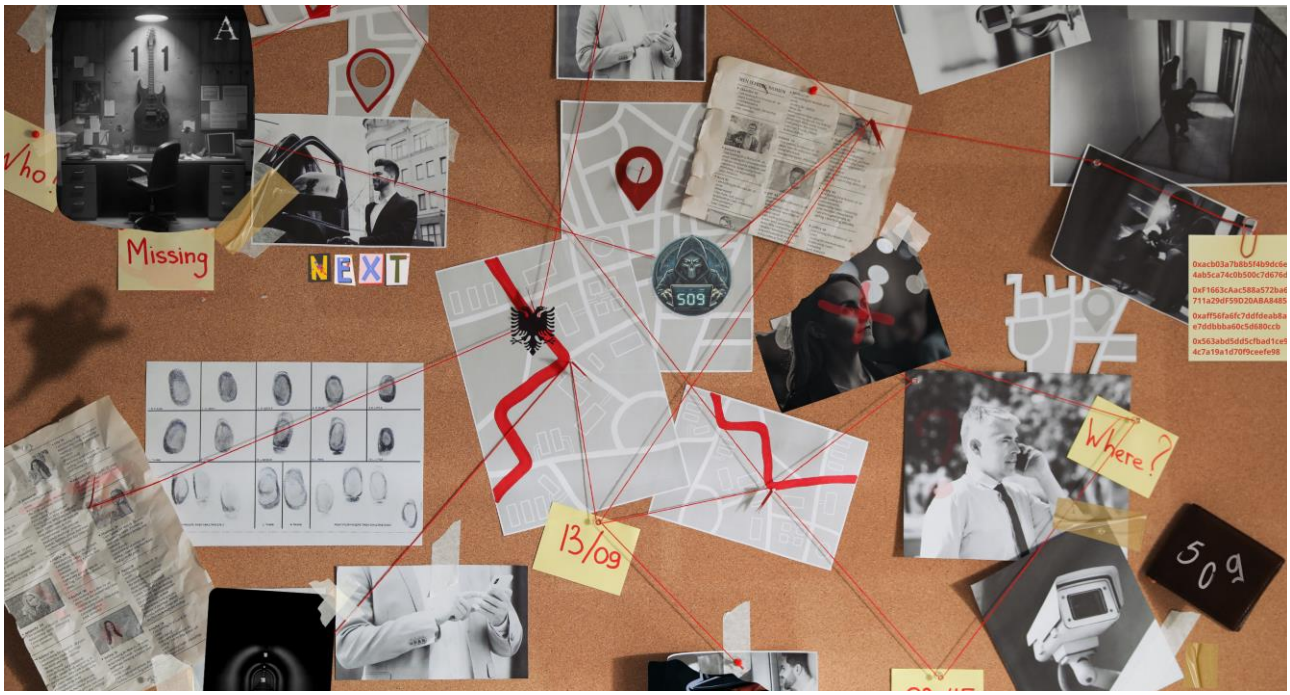
Technologie	Version	Score CVSS	EPSS	CVE DETAIL
Apache	2.4.46	9.8	70.6%	Lien
IIS	10.0	NONE	NONE	Lien
Log4j	2.14.0	10	97.5%	Lien
SQL 2019	X	8.8	0.16%	Lien

APT-509 est vulnérable à la faille majeure de décembre 2021, log4j (CVE-2021-44228). Plus de détails sur cette vulnérabilité sont disponibles ici : https://www.cvedetails.com/cve/CVE-2021-44228/.

Réponse attendue : hacko{CVE-2021-44228}

Challenge : άλφα

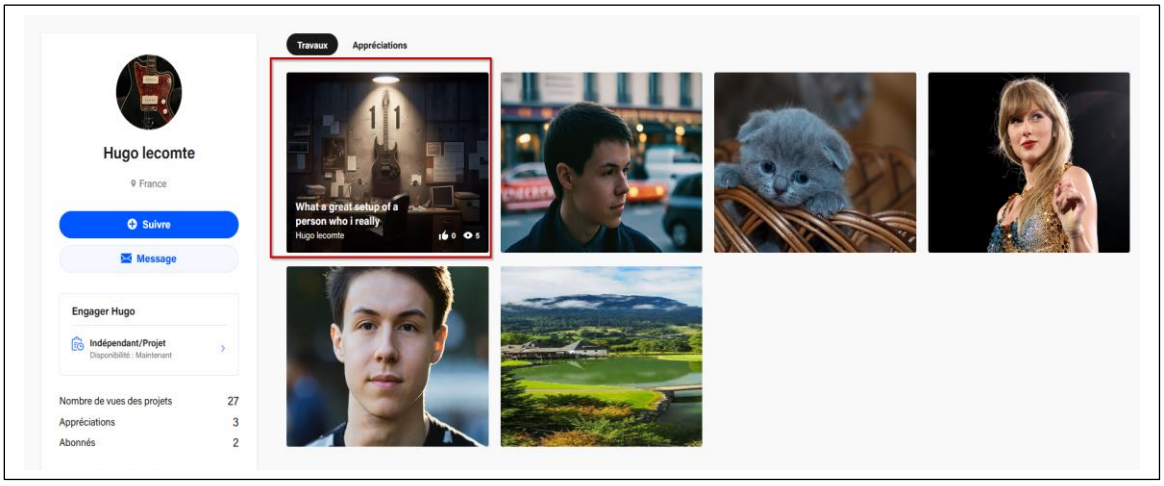
Pour ce défi, comme l'énoncé le suggère, nous devons prendre du recul sur toutes les informations que nous possédons. En nous appuyant sur les dossiers d'enquête fournis par la police (Acte 6 : Opération spéciale), nous disposons d'un tableau de liège trouvé dans le bureau d'Alpha.



Voici a quoi correspond chacun des éléments (bulle rouge avec chiffre sur la photo) :

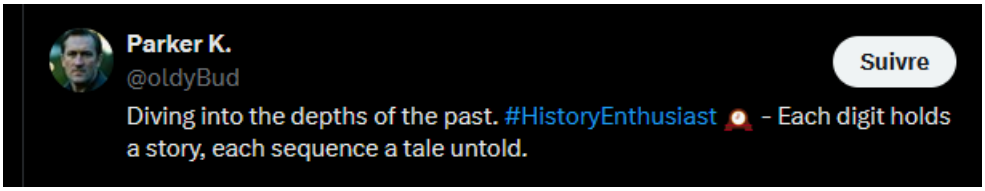
1. **Image du Bureau d'Alpha** : En haut à droite, la lettre "Alpha" est clairement visible, suggérant son importance, lien avec Alpha.
2. **Aigle Bicéphale** : Symbolise la localisation du premier cyber-bunker d'APT-509.
3. **Logo d'APT-509** : Représente l'entité ou le groupe concerné.
4. **Logo des Enquêteurs** : Le logo du CTF est accompagné du texte « warning », indiquant que les membres d'APT-509 sont conscients de l'enquête en cours à leur encontre.
5. **Adresses Wallet** : La seconde adresse mentionnée correspond à celle de Yankee.
6. **Texte Référence à APT-509** : Mention spécifique liant les éléments du tableau à APT-509.
7. **Image de Charlotte** : Photo de Charlotte, victime d'APT-509, avec un trait barré à travers, indiquant une cible atteinte.

Point d'intérêt : Image du bureau d'Alpha - Nous sommes frappés par une familiarité avec l'image du bureau d'Alpha. Effectivement, une image similaire se trouve sur le compte Behance de Hugo Lecomte, suggérant potentiellement un lien ou une coïncidence notable qui mérite une enquête plus détaillée.



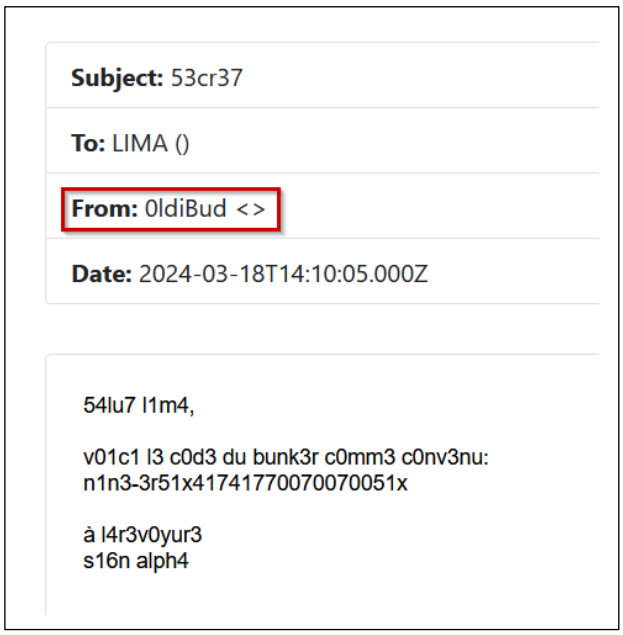
Dans le titre de cette photo, nous pouvons lire : « What a great setup of a person who I really appreciate! ». Cela suggère que Hugo Lecomte entretient un lien direct avec Alpha.

Examinons donc les abonnés de Hugo ; il est probable qu'Alpha et lui se suivent mutuellement sur au moins un des réseaux sociaux de Hugo. En parcourant les abonnés de son compte Twitter, nous découvrons un compte particulièrement intéressant :



(https://twitter.com/oldyBud)

Nous avons donc identifié Alpha ! Pour rappel, dans le fichier .mbox découvert dans le téléphone de Lima (Philip Harris), nous trouvons un pseudonyme « oldbud » utilisé pour signer les messages en tant que « Alpha ».



0ldiBud (pseudonyme utilisé dans le mail) / OldyBud (pseudonyme twitter)

Pour retrouver le nom de famille d'Alpha, nous avons son prénom "Parker" qui apparaît dans l'un de ses posts.

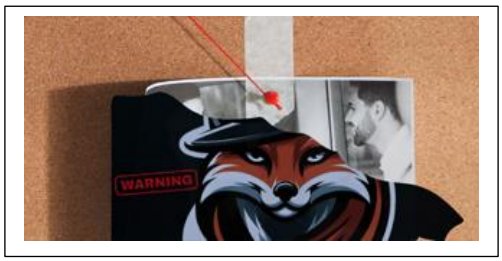
Alpha s'appelle donc Parker Kenneth.

Grâce à toutes nos informations, nous pouvons déduire que Parker Kenneth est le professeur de guitare de Hugo Lecomte.

Réponse attendue : hacko{kenneth_parker}

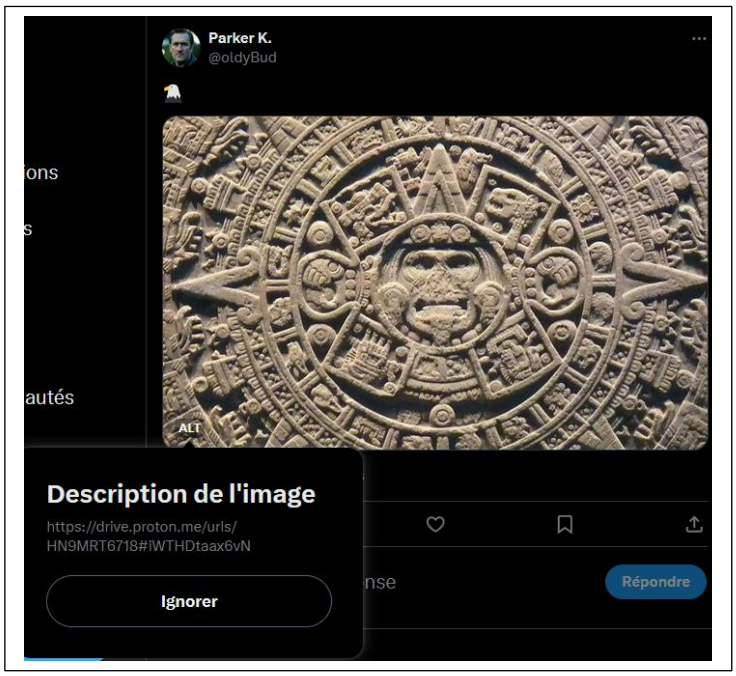
Challenge : Programme malveillant

Comme découvert sur le tableau de liège dans le bureau d'Alpha, nous savons maintenant qu'APT-509 est au courant que nous enquêtons sur eux.



Pour trouver et désactiver le programme, nous devons d'abord enquêter sur Parker (Alpha).

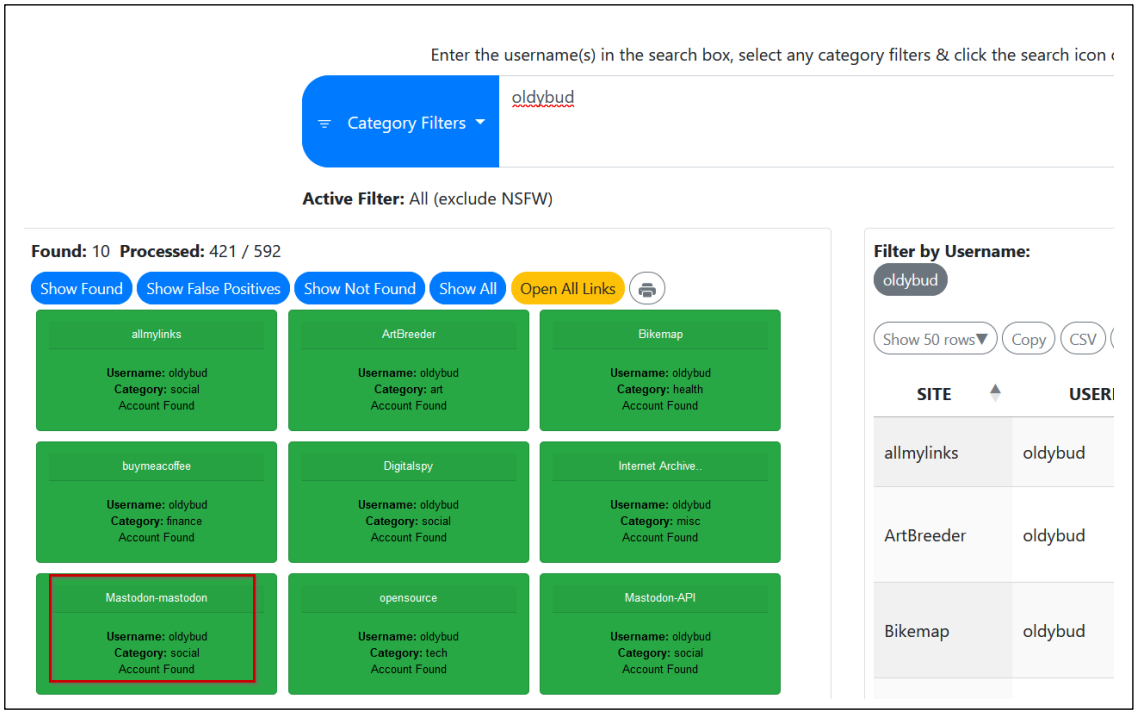
Dans l'un de ses posts Twitter, nous trouvons un lien vers un drive dans la description d'une image.



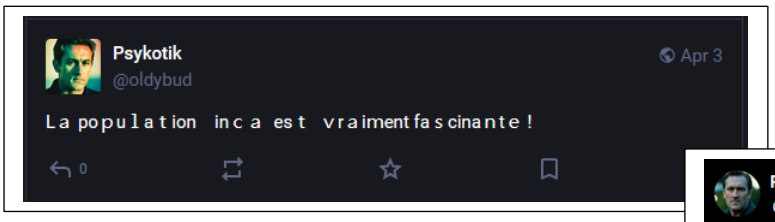
(https://drive.proton.me/urls/HN9MRT6718#iWTHDtaax6vN)

Comme toujours, nous avons besoin d'un mot de passe pour accéder au drive.

Grâce à l'outil en ligne What's My Name, nous avons découvert qu'Alpha possède également un compte Mastodon (https://mastodon.social/@oldybud) :



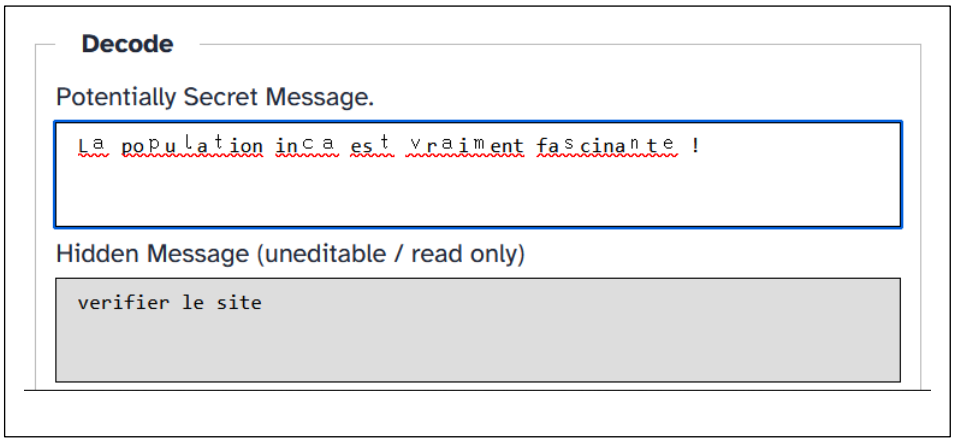
Sur les deux réseaux sociaux d'Alpha, nous retrouvons des posts avec une drôle d'écriture.



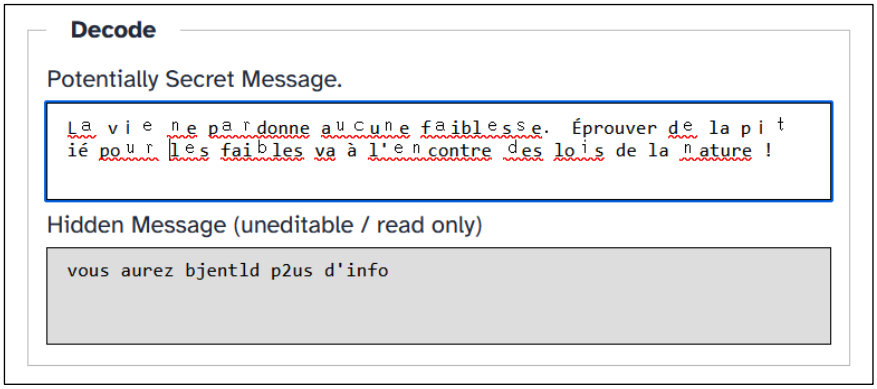
Ces messages cachent en réalité d'autres phrases. Pour décoder et révéler le secret de chacun des posts, nous allons utiliser cet outil : https://holloway.nz/steg/.

Voici les messages décodés, présentés dans leur ordre chronologique :

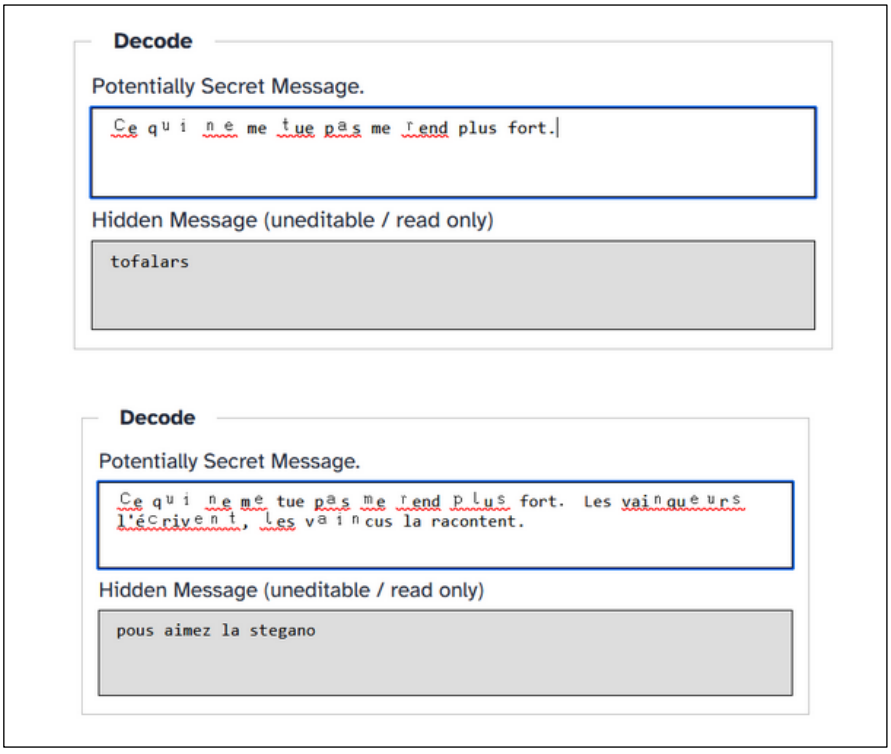
08/04/2024 :



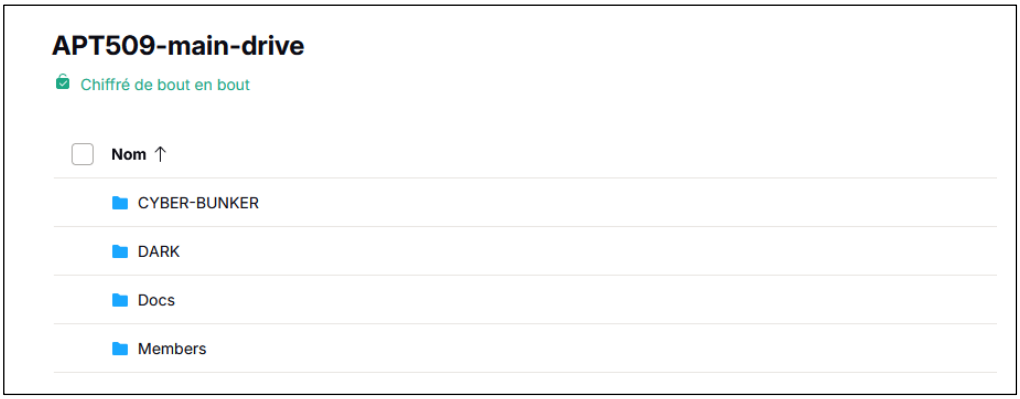
23/04/2024 :



01/05/2024 :



Nous avons ainsi découvert le mot de passe pour accéder au drive mentionné précédemment : tofalars.

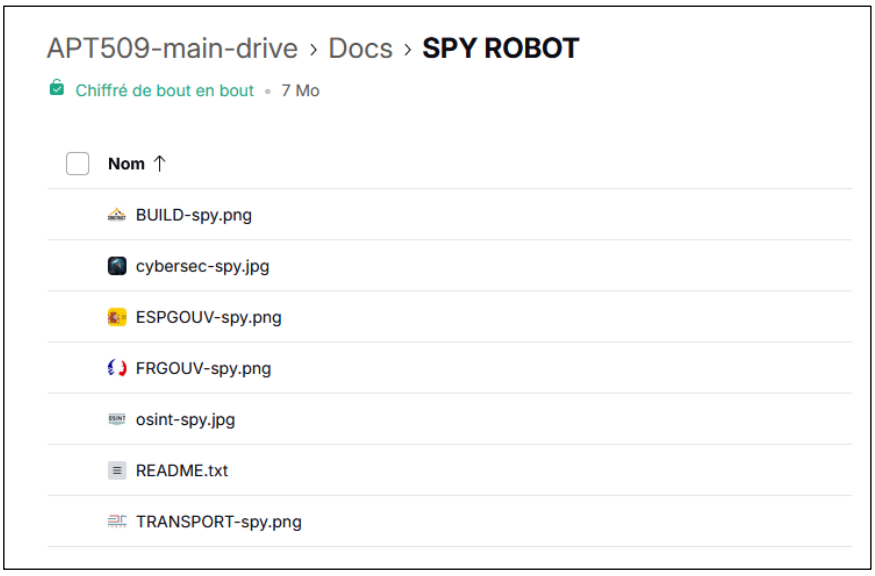


Nous avons réussi à infiltrer APT-509 et avons désormais accès à leur drive !

En explorant les différents dossiers, nous avons pu en apprendre davantage sur la structure et les noms de code utilisés par APT-509 :

- F (Foxtrot) : Hugo Lecomte
- L (Lima) : Philip Harris
- Y (Yankee) : Laetitia Roche
- Z (Zulu) : Quentin Morel
- A (Alpha) : Parker Kenneth

Dans ce challenge, nous devons désactiver le robot d'espionnage d'APT-509. Sur le drive, nous avons trouvé un dossier intitulé « SPY ROBOT ».



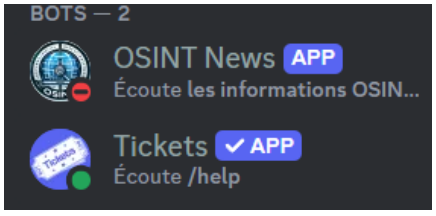
En consultant le fichier README de ce dossier, nous en apprenons davantage sur ce robot d'espionnage et découvrons surtout la commande pour interagir avec lui : `>>>ptEPQ9o4iDXfp7F_menu`.

SPY ROBOT, to be deployed only if the whole team agrees.
If "white plan" activated, right to deploy it wherever you want.

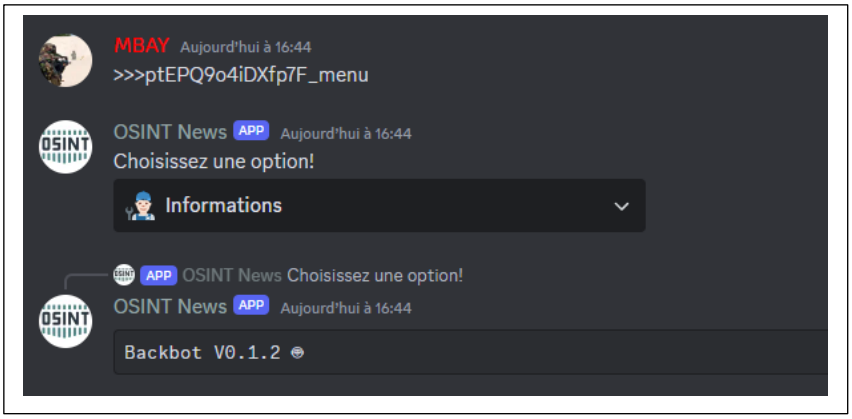
To interact with the bot, use this ">>>ptEPQ9o4iDXfp7F_menu" where it is located.

Nous devons maintenant découvrir où APT-509 a installé ce robot pour nous espionner. En examinant les images contenues dans le dossier « SPY ROBOT », une image attire particulièrement notre attention : « osint-spy.jpg ».

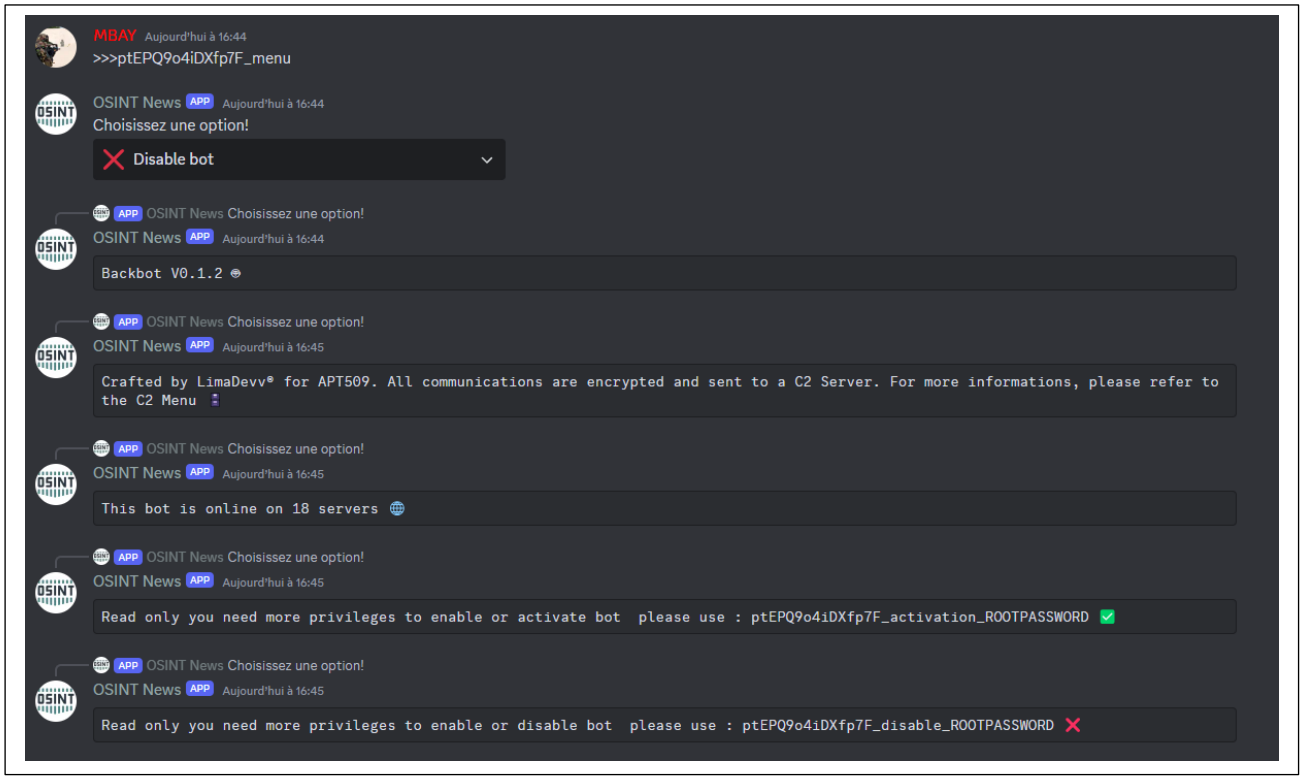
Nous avons retrouvé cette même image utilisée par un bot sur le serveur Discord dédié à cette enquête.



Il semble que APT-509 utilise le Discord pour nous espionner ! Nous allons donc, depuis notre canal d'équipe, tenter d'interagir avec le bot en utilisant la commande spécifiée dans le fichier « README.txt ».



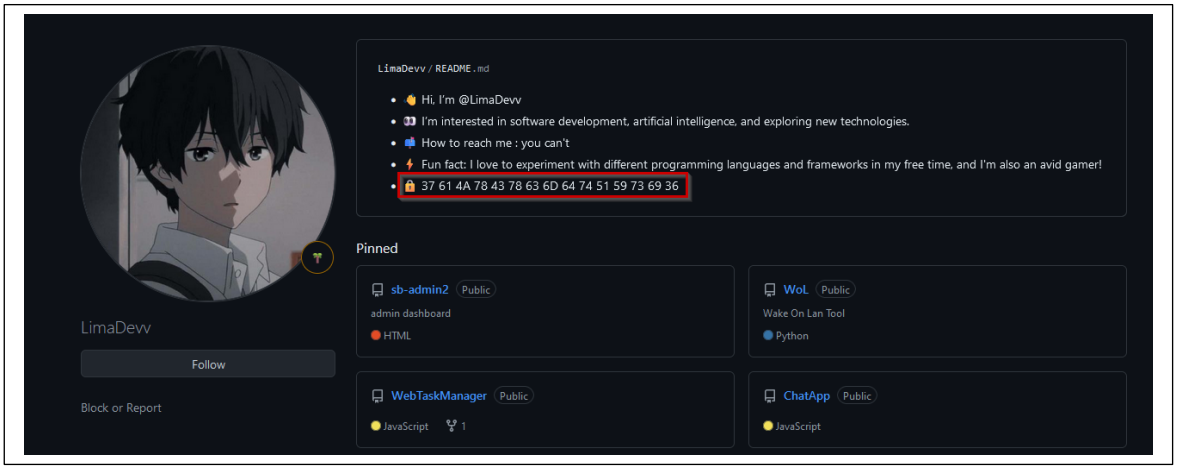
Le bot a répondu, confirmant ainsi que APT-509 utilise le Discord de l'enquête pour nous espionner. Il nous a également présenté un menu interactif. Voici ce que le bot affiche lorsque nous naviguons dans ce menu :



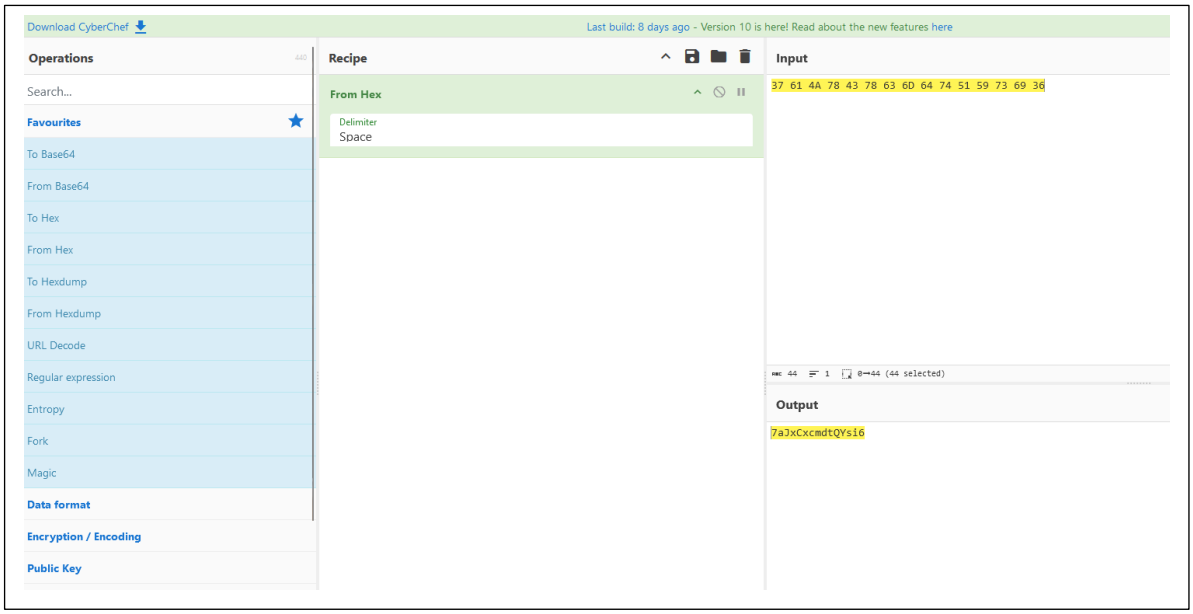
Grâce à l'option « crédit » du menu, nous apprenons que ce robot d'espionnage a été développé par LimaDevv, alias Philip Harris, un membre d'APT-509. Pour désactiver le robot d'espionnage, nous devons utiliser la commande suivante :

```
>>> ptEPQ9o4iDXfp7F_disable_ROOTPASSWORD.
```

Cependant, nous n'avons pas le mot de passe root... Étant donné que le robot a été créé par Lima et en se basant sur nos notes tout au long de l'enquête, nous avons trouvé un code dans la bio du profil GitHub de Lima. Ce code pourrait être le mot de passe root nécessaire pour désactiver le robot.

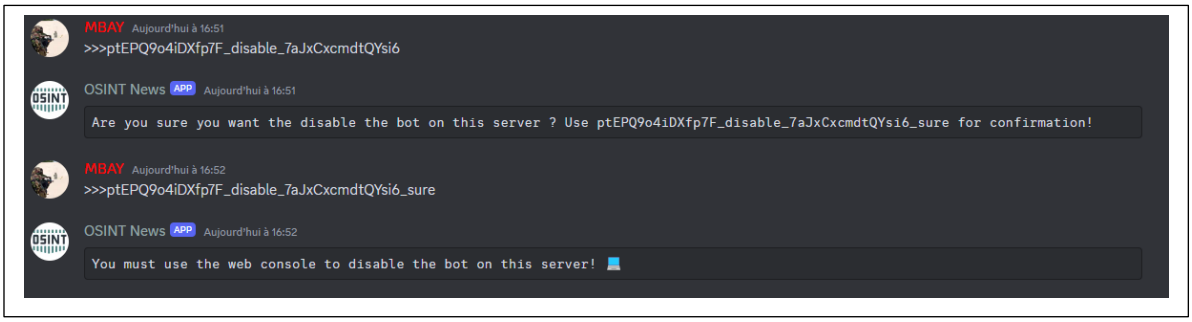


En utilisant CyberChef (https://gchq.github.io/CyberChef/) et son outil "baguette magique", nous avons identifié que le code était en HEXA. Après avoir décodé la chaîne, nous avons obtenu ce qui semble être un mot de passe : **7aJxCxcmdtQYsi6**.



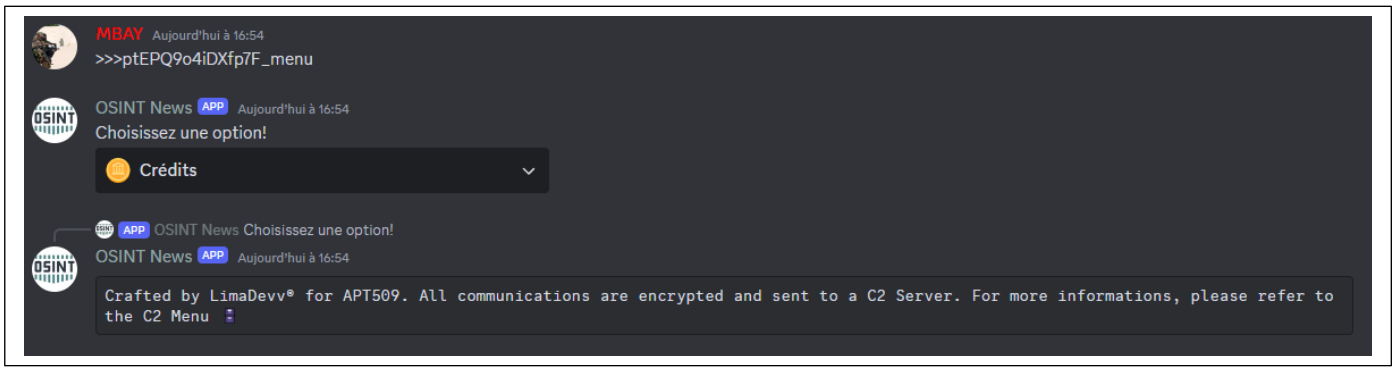
"7aJxCxcmdtQYsi6" pourrait être le mot de passe root nécessaire pour désactiver le robot d'espionnage d'APT-509. Utilisons maintenant la commande déjà identifiée, en y ajoutant le mot de passe que nous venons de découvrir :

```
>>>ptEPQ9o4iDXfp7F_disable_7aJxCxcmdtQYsi6
```



Cette fois, le système ne nous a pas demandé de saisir le mot de passe root, confirmant ainsi que « 7aJxCxcmdtQYsi6 » est bien le mot de passe root pour le robot d'espionnage d'APT-509. Toutefois, il est maintenant nécessaire d'utiliser la console web pour désactiver le robot.

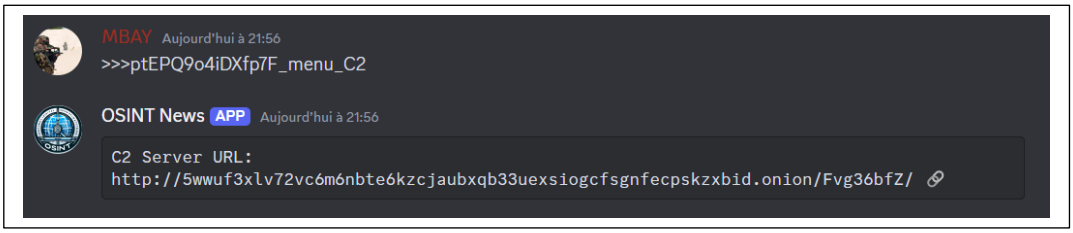
Précédemment, nous avons constaté que toutes les communications sont envoyées vers un serveur de commande et de contrôle (C2).



Nous devons donc accéder au menu C2 du robot. Pour cela, nous reprenons la commande d'interaction de base et ajoutons « C2 » à la fin :

```
>>>ptEPQ9o4iDXfp7F_menu_C2
```

En utilisant cette commande, nous obtenons les informations détaillées concernant le serveur C2 utilisé par APT-509.



Tous les messages sont donc envoyés vers le serveur C2 à l'URL suivante : http://5wwuf3xlv72vc6m6nbte6kzcjaubxqb33uexsiogcfsgnfecpskzxbid.onion/Fvg36bfZ/

En utilisant TOR pour accéder à cette adresse, nous arrivons sur le terminal de commande du C2. Après avoir tapé la commande « help », nous obtenons une liste des commandes disponibles que nous pouvons utiliser pour interagir avec le système.

```
user@apt509c2:~$ help
Below there's a list of commands that you can use.
You can use autofill by pressing the TAB key, autocompleting if there's only 1 possibility, or sho
possibilities.

ls - List information about the files and folders (the current directory by default).
cat - Read FILE(s) content and print it to the standard output (screen).
whoami - Print the user name associated with the current effective user ID and more info.
date - Print the system date and time.
help - Print this menu.
clear - Clear the terminal screen.
reboot - Reboot the system.
robot - Display informations about the spy robot.
robot_disable - Disable the spy robot on a specific server.
robot_enable - Enable the spy robot on a specific server.
```

Pour désactiver le robot d'espionnage, nous devons utiliser la commande `robot_disable`.

En entrant cette commande, `robot_disable`, nous obtiendrons les instructions nécessaires pour l'utiliser correctement.

```
user@apt509c2:~$ robot_disable
Use : robot_disable_IDSRV_C2ROOTPWD
```

Pour désactiver le robot d'espionnage, nous avons besoin des informations suivantes :

- L'ID du serveur sur lequel le robot est installé, qui dans ce cas est l'ID du serveur de l'enquête : 1196422674105253978.
- Le mot de passe C2 que nous avons trouvé précédemment : 7aJxCxcmdtQYsi6.

```
user@apt509c2:~$ robot_disable_1196422674105253978_7aJxCxcmdtQYsi6
The spy robot activated on server 1196422674105253978 has been deactivated. exit code 0x8725EZ
```

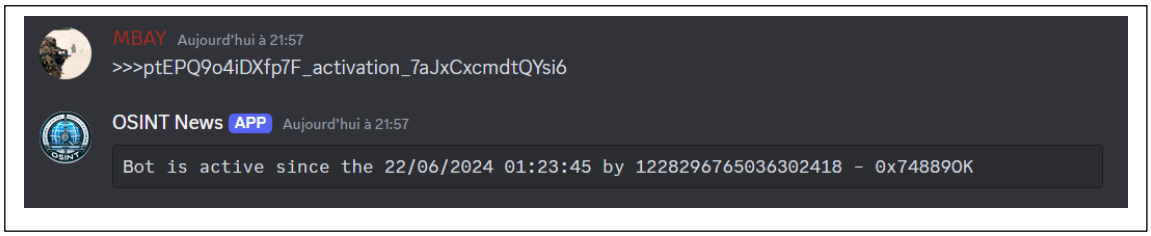
Après avoir saisi la commande, nous avons réussi à désactiver le robot. Le code de retour qui confirme la désactivation du robot est : 0x8725EZ.

La solution à ce challenge est donc : hacko{0x8725EZ}

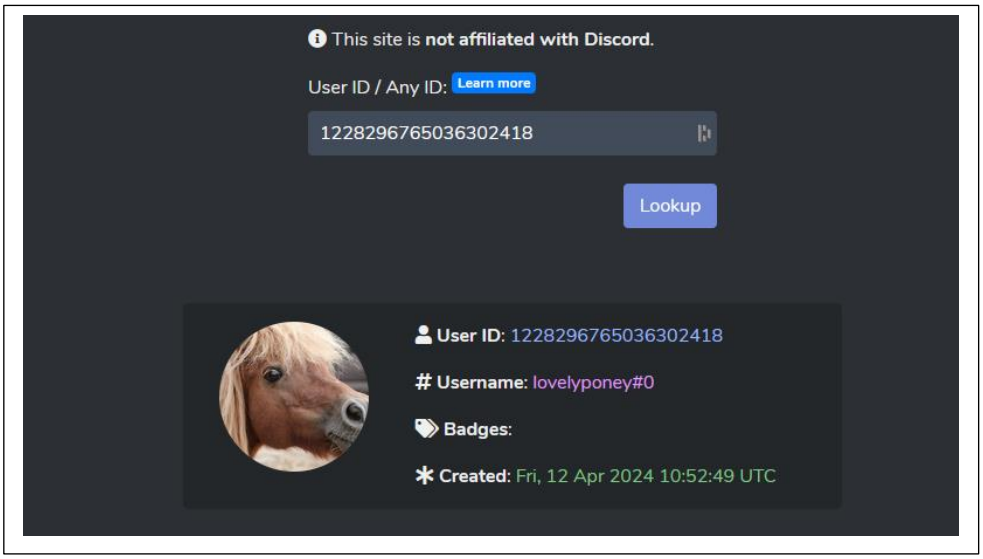
Challenge : Identité

Pour déterminer qui a activé le robot d'espionnage sur Discord, nous devons effectuer une nouvelle interaction, comme indiqué par le symbole de l'œil dans l'énoncé du challenge.

En accédant au menu « Activate boot », nous obtenons des informations concernant la personne qui a activé le robot d'espionnage sur le Discord, ainsi que la date de cette activation.



Nous disposons maintenant d'une chaîne de caractères qui semble correspondre à un ID Discord : 1228296765036302418. Pour identifier la personne derrière cet ID, nous utiliserons le site suivant : https://discord.id/. Ce site nous permettra de retrouver les informations du profil associé à cet ID sur Discord.



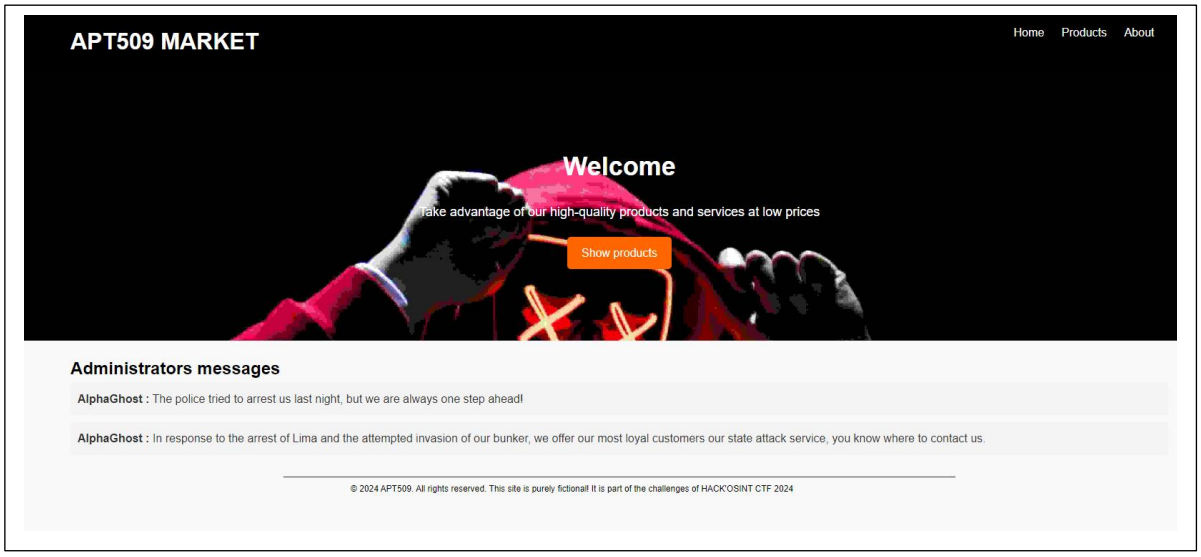
La personne qui a activé le robot d'espionnage est identifiée par le pseudonyme : lovelyponey.

La réponse à ce challenge est donc : hacko{lovelyponey}

Challenge : Le côté obscur

Dans ce challenge, on nous demande d'identifier depuis quel autre site APT-509 propose ses services. Comme nous l'avons découvert précédemment, APT-509 utilise également un site .onion.

Par conséquent, APT-509 propose ses services via le site suivant : https://5wwuf3xlv72vc6m6nbte6kzcjaubxqb33uexsiogcfsgnfecpskzxbid.onion/.



Réponse attendue : hacko{http://5wwuf3xlv72vc6m6nbte6kzcjaubxqb33uexsiogcfsgnfecpskzxbid.onion}

Challenge : Nouvelle cible

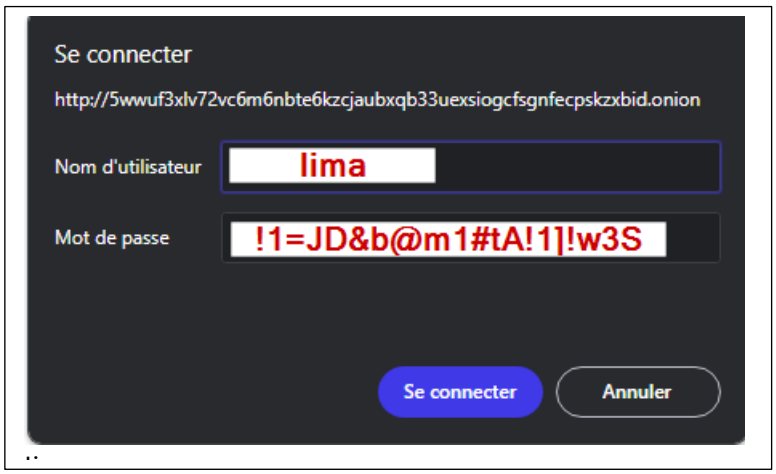
Pour découvrir la prochaine cible d'APT-509, nous examinons le site .onion précédemment identifié. En inspectant le code source de la page principale, nous tombons sur un lien menant à une section privée : /private/index.html.

L'adresse complète est : http://5wwuf3xlv72vc6m6nbte6kzcjaubxqb33uexsiogcfsgnfecpskzxbid.onion/private/index.html

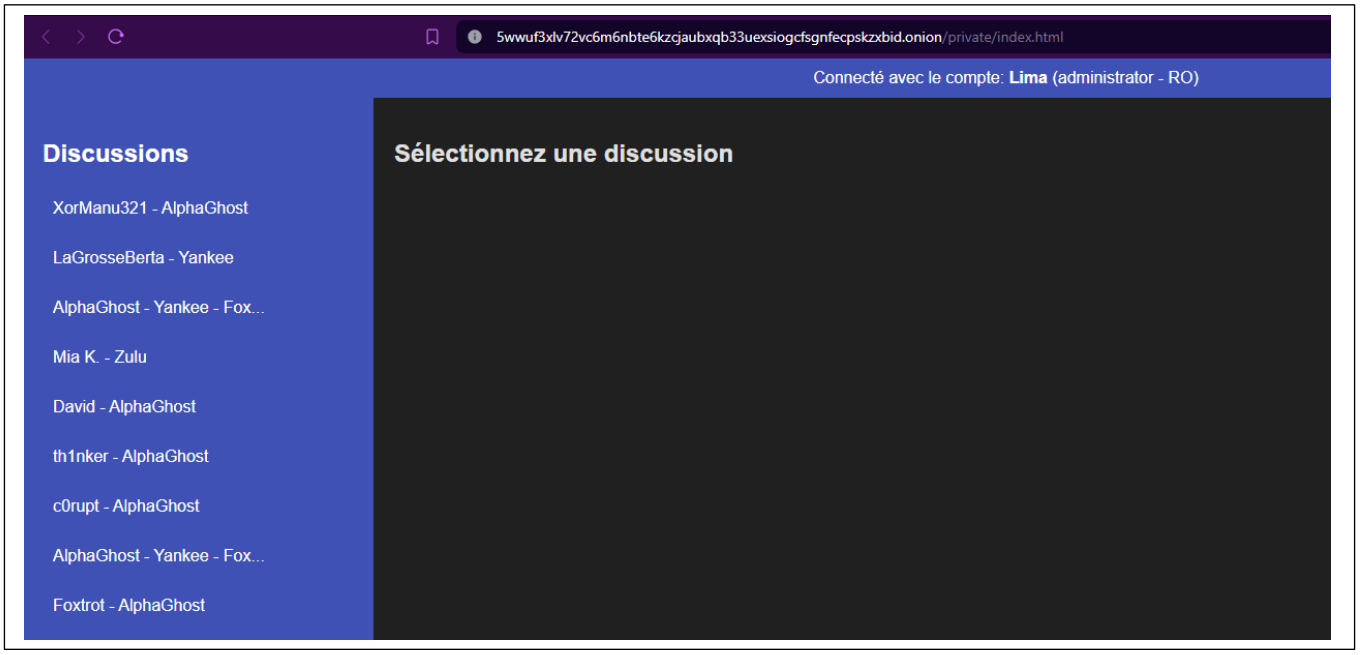
Cependant, l'accès à cette page nécessite des identifiants de connexion. Nous nous rappelons alors une note trouvée dans le téléphone de Lima, contenue dans le fichier wrd.txt. Les informations d'identification trouvées dans ce fichier sont les suivantes :

- Utilisateur : lima
- Mot de passe : !1=JD&b@m1#tA!1]!w3S

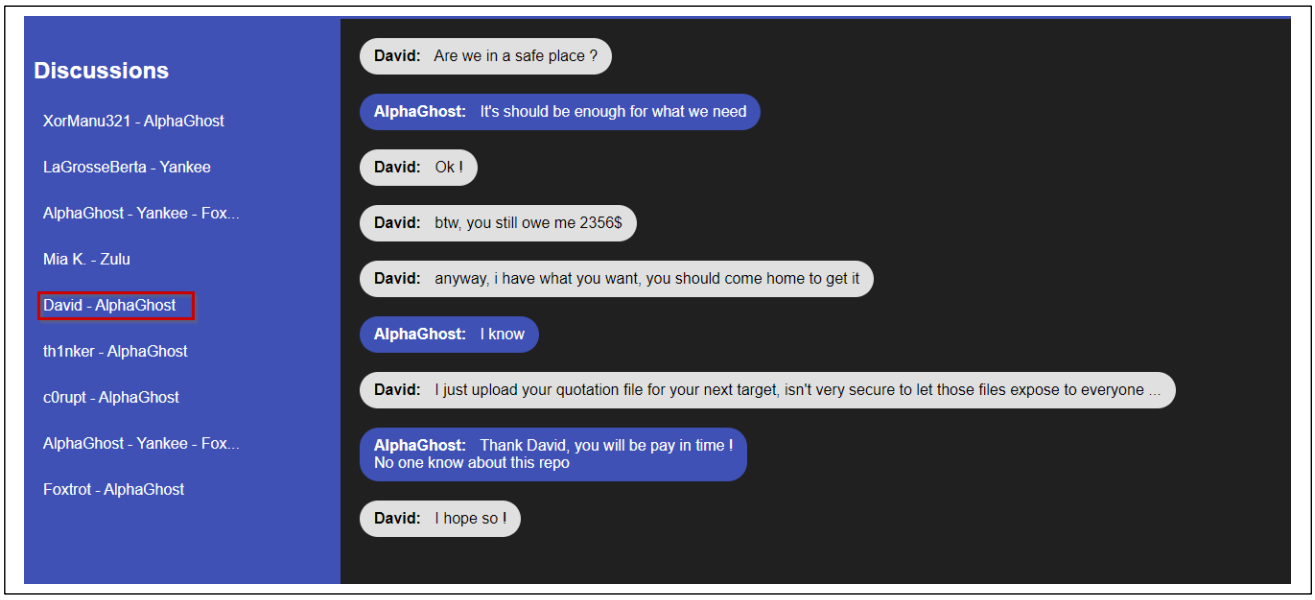
En essayant de s'authentifier avec ces informations :



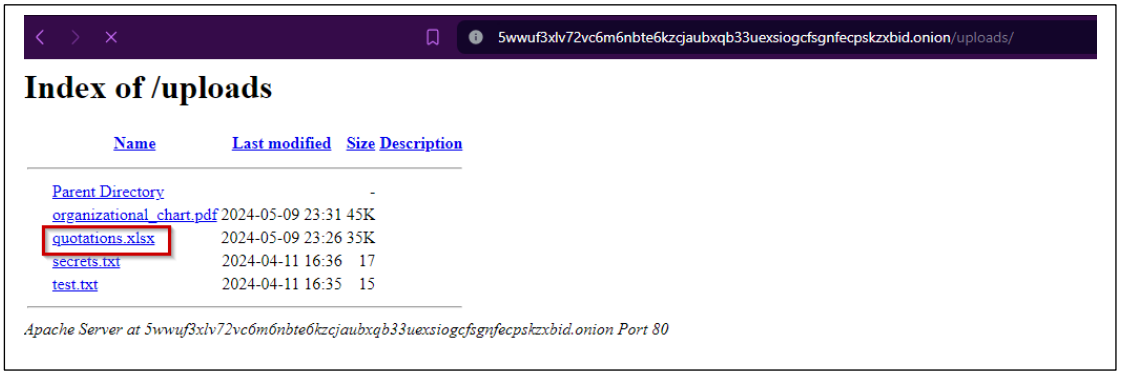
Nous avons maintenant accès au dark chat d'APT-509, grâce une fois de plus à Lima !



En analysant toutes les discussions, nous découvrons une conversation particulièrement intéressante entre Alpha et son fournisseur, David.

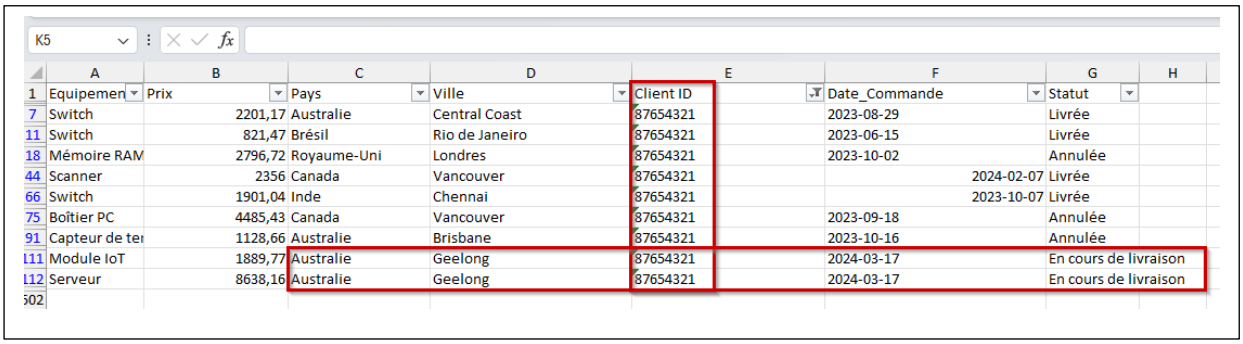


David mentionne qu'il a upload le fichier de commande, appelé « quotation file », d'Alpha dans un environnement peu sécurisé. En explorant /uploads/ sur le site .onion, nous découvrons alors un répertoire d'uploads d'APT-509.



En consultant le fichier, nous tombons sur plus de 500 lignes de commande. Afin de repérer les commandes spécifiques à Alpha, nous retrouvons dans le drive d'APT-509, plus précisément dans le dossier « Members/A(α) », une carte de visite (seller.png) appartenant à David, le fournisseur d'APT-509.

En utilisant l'ID trouvé sur la carte de visite de David dans le fichier « quotation file », nous effectuons un filtre pour isoler les transactions associées à Alpha. Cela révèle que la prochaine cible d'APT-509 est la ville de Geelong en Australie.



	A	B	C	D	E	F	G	H
1	Equipemen	Prix	Pays	Ville	Client ID	Date_Commande	Statut	
7	Switch	2201,17	Australie	Central Coast	87654321	2023-08-29	Livrée	
11	Switch	821,47	Brésil	Rio de Janeiro	87654321	2023-06-15	Livrée	
18	Mémoire RAM	2796,72	Royaume-Uni	Londres	87654321	2023-10-02	Annulée	
44	Scanner	2356	Canada	Vancouver	87654321	2024-02-07	Livrée	
66	Switch	1901,04	Inde	Chennai	87654321	2023-10-07	Livrée	
75	Boîtier PC	4485,43	Canada	Vancouver	87654321	2023-09-18	Annulée	
91	Capteur de ter	1128,66	Australie	Brisbane	87654321	2023-10-16	Annulée	
111	Module IoT	1889,77	Australie	Geelong	87654321	2024-03-17	En cours de livraison	
112	Serveur	8638,16	Australie	Geelong	87654321	2024-03-17	En cours de livraison	

Réponse attendue : hacko{geelong_australie}

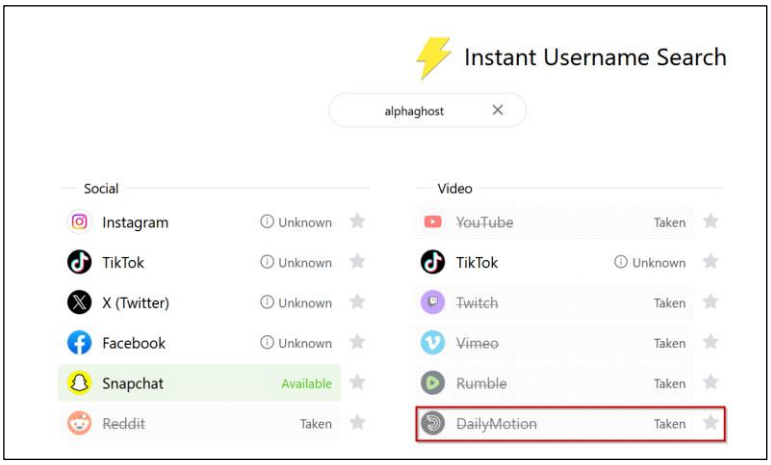
Challenge : CYBER-BUNKER

Pour localiser le nouveau bunker d'APT-509, l'analyse des conversations sur le dark chat est cruciale. En explorant plus en détail, nous tombons sur un échange entre les membres d'APT-509 où ils mentionnent des détails sur le déplacement et l'installation dans un nouveau lieu.

Voici les informations collectées :

- Alpha utilise également le pseudonyme « alphaghost ».
- Alpha a publié une vidéo contenant les coordonnées du nouveau CYBER-BUNKER, mais elle n'est pas disponible sur YouTube.

Nous avons découvert la chaîne Dailymotion d'alphaghost en utilisant instant Username Search : https://www.dailymotion.com/alphaghost



Dans la vidéo intitulée "White plan !" (https://www.dailymotion.com/video/x8y7x96) sur Dailymotion, nous observons un flash de lumière sur l'entrée d'un bunker, qui semble transmettre un message en code Morse.

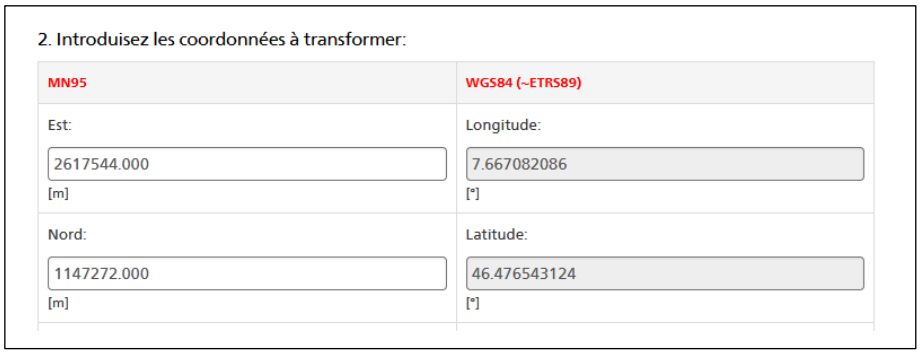
Une fois le code Morse décodé, nous obtenons la chaîne suivante : 2617544M1147272M.

Cela semble être des coordonnées GPS, mais de quel type ? Une exploration approfondie du dark chat nous révèle des informations intrigantes :

Pourquoi APT-509 évite-t-il de cibler la Suisse ?

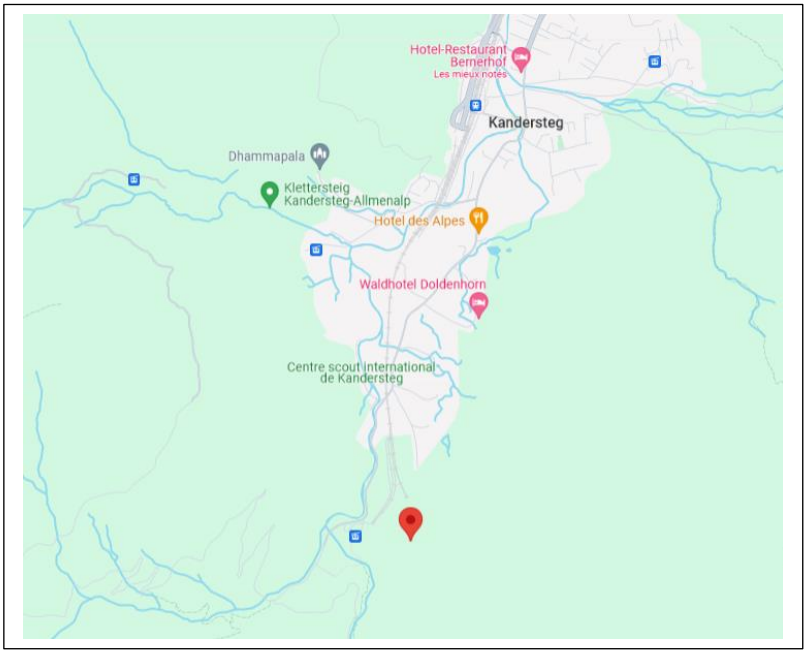
Nous explorons alors le système de coordonnées suisse sur : https://www.swisstopo.admin.ch/fr/le-systeme-de-coordonnees-suisse.

Nous réalisons que la chaîne trouvée précédemment correspond au format MN95, un système de coordonnées suisse. Nous procéderons ensuite à convertir ces coordonnées MN95 en WGS84 en utilisant le site : https://www.swisstopo.admin.ch/fr/conversion-coordonnees-navref vous pouviez également utiliser ce site (https://coordinates-converter.com).



Nous disposons désormais des coordonnées suivantes : 7.667082086, 46.476543124. En les saisissant sur Google Maps, (maps) nous localisons un point près de la ville de Kandersteg en Suisse.

Nous avons alors maintenant les coordonnées suivantes : 7.667082086, 46.476543124



En cherchant des bunkers à proximité de ces coordonnées, nous identifions la « Centrale de commandement K20 » dont vous trouverez des détails sur la page Wikipédia : https://fr.wikipedia.org/wiki/Centrale_de_commandement_K20.

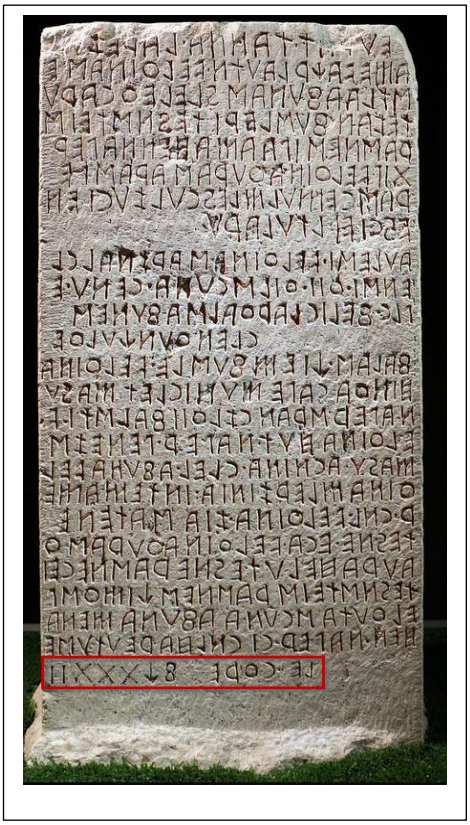
Les coordonnées GPS du bunker indiquées sur Wikipédia sont 46.475590537273625, 7.664452895249082.

Depuis Street View, nous pouvons confirmer l'existence de ce bunker :

La réponse attendue était donc : hacko{46.4755,7.664}

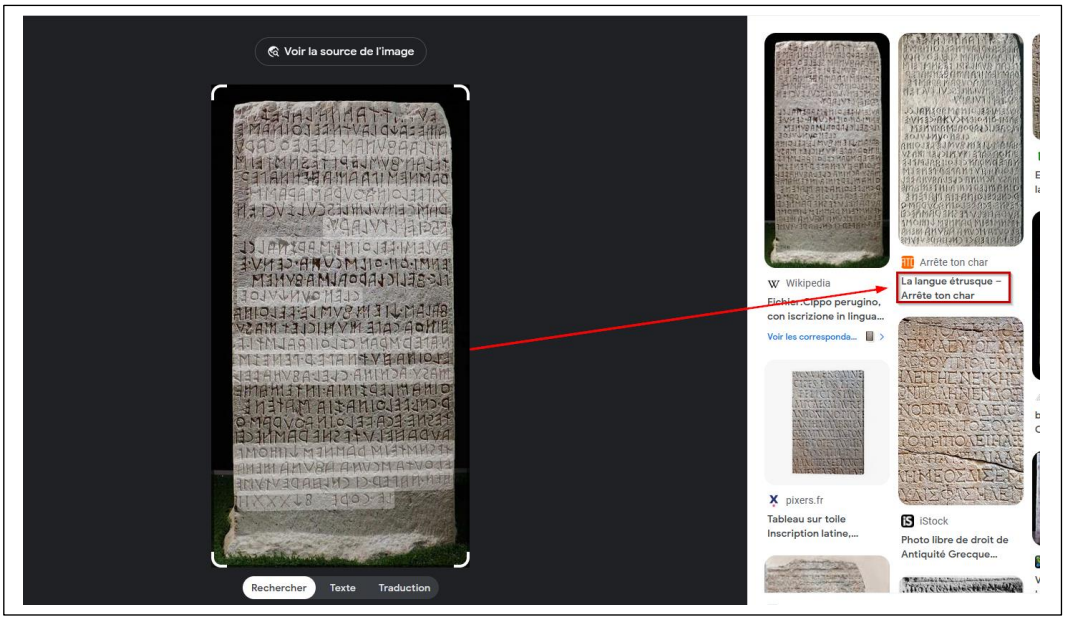
Challenge : Discrétion assurée !

Pour ce dernier défi de l'enquête, il nous fallait découvrir le code d'accès du nouveau CYBER-BUNKER d'APT-509. Encore une fois, c'est Alpha, le chef d'APT-509, qui divulgue ce code. Sur son compte Twitter, nous tombons sur un tweet contenant une image très révélatrice : https://twitter.com/oldyBud/status/1786386103441735694.

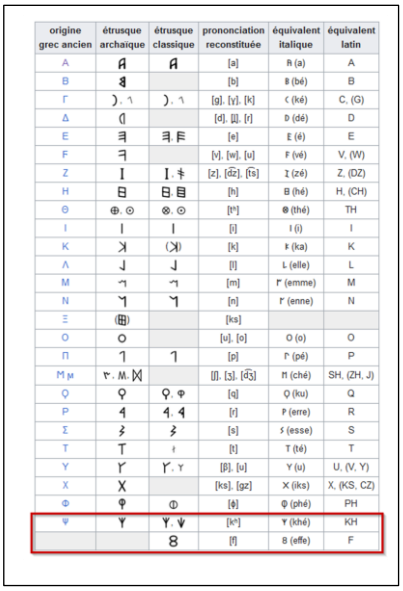


Nous découvrons sur la dernière ligne de cette stèle une phrase faisant allusion à un code :

En utilisant la recherche inversée d'image (https://lens.google.com), nous apprenons que cette stèle est en réalité écrite en étrusque.



Nous consultons la page sur l'alphabet étrusque pour décoder le texte : https://fr.wikipedia.org/wiki/Alphabet_%C3%A9trusque



origine grec ancien	étrusque archaique	étrusque classique	prononciation reconstituée	équivalent italique	équivalent latin
A	A	A	[a]	A (a)	A
B	B		[b]	B (bé)	B
Γ	), ٦	), ٦	[g], [γ], [k]	C (ké)	C, (G)
Δ	D		[d], [ð], [r]	D (dé)	D
E	E	E, E	[e]	E (é)	E
F	F		[v], [w], [u]	F (vé)	V, (W)
Z	I	I, ǂ	[z], [dz], [ts]	Z (zé)	Z, (DZ)
H	B	B, B	[h]	B (hé)	H, (CH)
Θ	⊕, ⊙	⊗, ⊙	[tʰ]	Θ (thé)	TH
I	I	I	[i]	I (i)	I
K	K	(K)	[k]	K (ka)	K
Λ	L	L	[l]	L (elle)	L
M	٦	٦	[m]	M (emme)	M
N	٦	٦	[n]	N (enne)	N
Ξ	⊞		[ks]		
O	O		[u], [o]	O (o)	O
Π	٦	٦	[p]	P (pé)	P
M M	٣, M, ⋈		[ʃ], [s], [d͡s]	M (ché)	SH, (ZH, J)
Q	Q	Q, Φ	[q]	Q (ku)	Q
P	4	4, 4	[r]	P (erre)	R
Σ	ξ	ξ	[s]	S (esse)	S
T	T	ŧ	[t]	T (té)	T
Y	Y	Y, ٢	[β], [u]	Y (u)	U, (V, Y)
X	X		[ks], [gz]	X (iks)	X, (KS, CZ)
Φ	Φ	Φ	[ɸ]	Φ (phé)	PH
Ψ	Y	Y, Ψ	[kʰ]	Y (khé)	KH
		8	[f]	8 (effe)	F

Le « 8 » correspond alors à un « F » et la flèche du bas « ↓ » correspond à « KH ».

Nous avons alors décodé le début du code et devons maintenant déterminer la signification de « XXXII ».

En consultant http://monsu.desiderio.free.fr/curiosites/etrusque.html, nous apprenons qu'ils correspondent aux chiffres romains, donc XXXII signifie 32.

Chiffres romains	Chiffres étrusques	Autres signes étrusques	Chiffres arabes
I V X L C C ou M ? M ou ?	Ⅰ Λ X ↑ ☾ ✳ ⊖ ◇	+ (cent)	1 5 10 50 100 100 ou 1 000 ? 1 000 ou ?

Par conséquent le code décodé est : fkh32.

La réponse attendue était : hacko{fkh32}

END OF WATCH

Challenge de clôture de la compétition :

Quel endroit étrange... Comment se fait-il qu'APT509 puisse se réfugier dans un bunker gouvernemental suisse ?!! Qui leur a donné les accès... ?

Malheureusement, notre compétence s'arrête ici. Nous avons transmis l'intégralité du dossier d'enquête à l'OFCS (Office Fédéral de la Cybersécurité Suisse). Espérons que ce groupe soit démantelé et ne fasse plus de victimes. Quant à l'affaire de Charlotte, malheureusement, il est peu probable qu'elle retrouve son argent. Ayant agi de son propre chef (en cliquant et saisissant son mot de passe), sa banque refuse de la rembourser.

Cependant, chères enquêtrices, chers enquêteurs,

Voici les dernières informations présentes dans notre dossier d'enquête :

- HARRIS Philip, alias Lima, développeur au sein d'APT509, n'a toujours pas coopéré. Il est actuellement en détention provisoire en attendant son jugement.
- LECOMTE Hugo, alias Foxtrot, un nouveau membre d'APT509, a été arrêté grâce à vos précieuses informations chez lui alors qu'il rendait visite à sa famille.
- ROCHE Laetitia, alias Yankee, a été arrêtée chez elle, non loin de la ville d'Apt. En raison de ses responsabilités familiales, elle était rarement présente au CYBER-BUNKER. Grâce à une certaine somme d'argent, elle nous a communiqué énormément d'informations sur APT509.
- MOREL Quentin, alias Zulu, une opération est en cours avec l'OFCS. Nous attendons son retour à son bureau pour l'appréhender. Il sera jugé en France.
- En ce qui concerne PARKER Kenneth, alias Alpha, nous pensons fortement qu'il se cache au sein du K20.

Dans tous les cas, le groupe de cybercriminels "APT509" a été sérieusement affaibli grâce à vous ! Espérons ne pas les revoir de sitôt.

Nous vous remercions à nouveau pour votre précieuse aide. Sans vous, nous n'aurions jamais réussi à retrouver et à arrêter tous ces cybercriminels !

Nous déclarons officiellement votre mission terminée. Et qui sait... peut-être à bientôt.

FLAG à entrer : hacko{end_of_watch}

Remerciements

Nous tenons à conclure cette write-up en exprimant notre gratitude envers tous les acteurs qui ont contribué au succès de cette enquête.

Nous souhaitons également remercier chaleureusement tous les bêta-testeurs qui ont consacré de leur temps personnel pour tester et nous fournir des retours précieux, permettant ainsi d'améliorer cette enquête.

Liste des bêta-testeurs :

Équipe Hacker Vaillant :

- cyberkaser
- CézarioSs
- esuh
- OiY
- l0giciel
- JeanPiffre

Équipe Incompetent Detectives :

- KrowZ
- Kortez
- Bouddah

Membre d'Hack'olyte :

- McBoux
- R3børn

Nous tenons à exprimer notre profonde gratitude envers **ozint.eu** (support de cette enquête) pour leur soutien indispensable durant toute la préparation de ce CTF. Un remerciement spécial est également adressé à **SilverBike**, dont la présence et les conseils précieux ont été d'une aide inestimable !

[i]

[i] Fin du Write Up Hack'osint CTF