



 **APTHUNTER**

WRITE UP OFFICIEL

Mot de l'équipe APT Hunter

Comme dans tout CTF qui se respecte, voici le write-up officiel. Ce document a pour but de montrer comment résoudre les challenges du CTF et regroupera les principales techniques pour y parvenir. Bien entendu, il existe une multitude de techniques pour résoudre les challenges en OSINT. Cependant, à travers ce write-up, nous allons vous présenter nos méthodes.

Nous espérons que certaines de nos explications éclaireront vos lanternes si vous étiez bloqués !

Encore un grand merci à tous pour votre participation !



Introduction : Une communication inquiétante

Cher Agent Mercier,

Les services de renseignements ont récemment intercepté des communications inquiétantes. Un groupe de hackers inconnu semble planifier une opération d'envergure.

Votre mission, si vous l'acceptez, consiste à identifier ce groupe APT, à retrouver des preuves de leur plan et à déterminer la cible de leur attaque.

Utilisez vos compétences en OSINT et déjouez ce complot malveillant. Le compte à rebours a commencé, et le temps presse..

Êtes-vous prêt à relever ce défi ?

Rassemblez votre équipe et préparez vos outils !

Flag : compris



Challenge 2 : La lettre

Vous voilà plongé au début d'une enquête sans savoir où vous allez aboutir. Les services de renseignements vous ont fourni une lettre comme premier élément et s'efforceront tout au long de l'enquête de vous fournir des éléments.

Quel est le premier pseudonyme que vous avez trouvé ?

Format de Flag : **J4s0n**

La lettre :

```
Qm9uam91ciwKCkNlbGEgZmFpdCB1biBtb21lbnQgcXVIIG5vdXMgbmUgbm9
1cyBzb21tZXMcGFzIHJlbmNvbnRy6XMuMAgY2V0dGUg6XBvcXVILCB2b3
VzIG4nYXZpZXogcGFzIGVuY29yZSBpbnTpZ3LpIGxlcycBzZXJ2aWNlcycBkZS
ByZW5zZWlnbmVtZW50cyBmcmFu52Fpcy4gTGVzIG9pc2VhdXggY2hhbnRh
aWVudCwgbGVzIHZvaXR1cmVzIHNPbGxvbm5haWVudCBsZXMc91dGVz
LCBsZSBjaWVsIOI0YWl0IGJsZXUsIGxhIHZpZSDpdGFpdCBiZWxsZS4uLgoK
TWFsaGV1cmV1c2VtZW50LCBjZXMc9udCBBy6XZvbHVzLiBKZ
SB2aWVucyB2ZXJzIHZvdXMgY2FyIGxhIEZyYW5jZSBjb3VydCB1biBncmFuZ
CBkYW5nZXluIEonYWkgZXUgdmVudCBkJ3VuZSBpbmZvcm1hdGlvbiBpbnF
1aeI0YW50ZSwgaW5kaXF1YW50IHf1J3VuIG9yZ2FuaXNtZSBjbGFuZGVzd
GlulHRIbnRIIGRlIHNIbWVyIGxhIHRlcnJldXluCgpKZSBuZSBzYWlzIHbhcycBjZ
SBxdWkgc2UgY2FjaGUgZGVycmnocmUgdG91dCBjZWxhLCBuaSBxdWFuZ
CBjZWxhIHZhIGFycml2ZXluIENlcGVuZGFudCwgaidhaSBy6XVzc2kg4CBpbn
RlcmNlcHRlciB1biBwc2V1ZG9ueW1lIDogX1RyMHRzazEulE1hbGhldXJldXNI
bWVudCwgamUgbmUgcGV1eCBwYXMgbWVuZXIgbCdlbnF16nRlCBjYXlgb
W9uIGlkZW50aXTpIGVzdCBjb25udWUuCgpKZSB2b3VzIGNvbmZpZSBkb25j
IGxhIGxvdXJkZSBzZXNwb25zYWJpbGI06SBkZSBk6WNvdXZyaXlgbGEgduly
aXTpIGV0IGRlIHZlbmlyIOAgYm91dCBkZSBjZXR0ZSBtZW5hY2UuIEplIHNa
XMgcXVIIHZvdXMgYXZleiB0b3V0ZXMcgbGVzIHf1YWxpdOlzIHJlcXVpc2VzIH
BvdXIgbWVuZXIg4CBiaWVuIGNldHRIIG1pc3Npb24uCgpCb25uZSBjaGFuY2
UuCgpCLg==
```



Nous tombons sur cette lettre, qui est plutôt difficile à comprendre au premier abord. Ainsi, nous décidons de l'analyser afin de déterminer de quelle manière elle a été chiffrée. Pour ce faire, nous utilisons le site <https://dcode.fr/identification-chiffrement> qui, après avoir analysé ce message, nous suggère d'utiliser le Base64 pour le déchiffrer, autrement dit ce message a simplement été encodé.

The screenshot shows the dCode website's 'RECONNAITRE UN CHIFFREMENT' (Recognize a cipher) tool. At the top, there's a search bar with placeholder text 'Tapez par exemple "sudoku"'. Below it is a link to 'PARCOURIR LA LISTE COMPLÈTE DES OUTILS'. The main area is titled 'IDENTIFIER UN MESSAGE CODÉ' (Identify a coded message). It displays a Base64 encoded string:

```
dxJkZSBvZXNwb25zYWJpbGJ06SBkZSBk6WnvdxZyaXigbGEgdu1yaxTp
IGVOIGR1IHZ1bmlyIOAgYm91dCBkZSBjZXROZSBtZW5hY2UuIEp1IHNh
axMgcxVlIHZvdXmgYZ1eiB0b3VOZXMgbGVzIHF1Ywxpd01zIHJ1CXVp
c2VzIHBvdXIgbWVuZXIg4CBiaWVuIGNldHR1IG1pc3Npb24uCgpCb25u
ZSBjaGFuY2UuCgpCLg==
```

Below the message, there's a section for 'INDICES//MOTS-CLÉS (FACULTATIF)' (Indices/Keywords (optional)) with a text input field and a '▶ ANALYSER' button. To the right, a sidebar lists various symbols: 1, +, -, d, +, n, +, c, +, u, +, t, +, i, +, r, +, e. At the bottom, there are links to 'Voir aussi : Analyse des Fréquences – Indice de Coïncidence', 'IDENTIFIER DES SYMBOLES', and 'Aller à : Chiffrements avec Symboles'.

Nous tentons donc de décoder le message en **Base64** via l'outil CyberChef (<https://gchq.github.io/CyberChef/>) et nous avons un résultat décodé en clair:

Bonjour,

Cela fait un moment que nous ne nous sommes pas rencontrés. À cette époque, vous n'aviez pas encore intégré les services de renseignements français. Les oiseaux chantaient, les voitures sillonnaient les routes, le ciel était bleu, la vie était belle...

Malheureusement, ces temps sont révolus. Je viens vers vous car la France court un grand danger. J'ai eu vent d'une information inquiétante, indiquant qu'un organisme clandestin tente de semer la terreur.

*Je ne sais pas ce qui se cache derrière tout cela, ni quand cela va arriver. Cependant, j'ai réussi à intercepter un pseudonyme : **_Tr0tsk1**. Malheureusement, je ne peux pas mener l'enquête, car mon identité est connue.*

Je vous confie donc la lourde responsabilité de découvrir la vérité et de venir à bout de cette menace. Je sais que vous avez toutes les qualités requises pour mener à bien cette mission.

Bonne chance.

B.

Ainsi nous découvrons que le pseudonyme intercepté est **_Tr0tsk1** et nous pouvons ainsi valider le challenge.

FLAG : **_Tr0tsk1**



Challenge 3 : Une inattention

Vous avez découvert ce qui semble être un pseudonyme. Chaque information est précieuse et peut mener à la vérité ; assurez-vous donc de la conserver avec soin ! Il s'agirait à présent de trouver une piste. Quelle est sa véritable identité ?

Format de Flag : Louis Dupont

Nous avons en notre possession le pseudo _Tr0tsk1 et nous devons découvrir sa véritable identité. Nous allons donc entreprendre des recherches sur différents réseaux sociaux. Afin de gagner du temps et d'éviter de faire toutes les recherches manuellement, nous utiliserons le site internet Whatsmyname.app. Parmi les 590 sites analysés, nous avons obtenu un résultat positif.

The screenshot shows a search interface for 'Whatsmyname.app'. In the search bar, the username '_Tr0tsk1' is entered. Below the search bar, a blue button labeled 'Category Filters' is visible. The main area displays a single result: 'Active Filter: All (exclude NSFW)'. Below this, a green box contains the following information: 'Found: 1 Processed: 583 / 590', 'Show Found', 'Show False Positives', 'Show Not Found', 'Show All', 'Open All Links' (which is highlighted in yellow), and a printer icon. The result details are: 'Twitter', 'Username: _Tr0tsk1', 'Category: social', and 'Account Found'.

Nous tentons donc d'accéder à ce compte X(Twitter) pour investiguer.



Andrejew
 @_Tr0tsk1

Joined November 2023

7 Following 2 Followers

Not followed by anyone you're following

Après une analyse succincte, nous concluons rapidement que la personne concernée est russe. En poursuivant notre examen du compte, nous découvrons un post incluant un CV où la personne exprime son désir de trouver un emploi, le tout rédigé dans un français approximatif.

A travers cette découverte nous apprenons donc son prénom : **Andrejew Vladlen**.

Andrejew @_Tr0tsk1 · 23 févr.

Bonjour le Twittosphere 😊 Je suis à la recherche d'une nouvel emploi dans le développement logiciel, spécialement dans l'Europe et pourquoi pas le France Pouvez vous me donner une avis sur mon CV?

ANDREJEW VLADLEN
SOFTWARE ENGINEER

CONTACT

- ✉️ trtsk211@gmail.com
- 📍 Tomsk

SKILLS

Programming languages

- Backend: Python, Java, C/C++, C#, Golang
- Frontend: JavaScript, TypeScript
- Database Query Languages: SQL
- Scripting: PHP, Ruby, Bash

Libraries, Tools, and Frameworks

- Backend Frameworks: Node.js, Express, Django, Ruby on Rails
- Frontend Frameworks: React
- Version Control: Git, SVN
- DevOps: Docker, Kubernetes
- Testing Frameworks: Jest
- Cloud Services: AWS, Azure, Google Cloud
- Web Servers: Nginx, Apache
- IDEs: Visual Studio Code, IntelliJ IDEA

Databases

- MySQL
- PostgreSQL
- MongoDB

Operating systems and environments

- Linux (Ubuntu, CentOS)
- Windows Server
- Windows 10/11

EDUCATION

Bachelor of Software Engineering
Tomsk State University
2013-2017

LANGUAGES

Russian ——————
English ——————

PROFILE

Experienced Software Engineer with a strong track record of delivering cutting-edge solutions through global collaborations. Proficient in end-to-end development, diverse programming languages, and emerging technologies such as AI, Blockchain, and Big Data. Committed to excellence and innovation, I am eager to contribute my expertise in solving complex challenges, optimizing projects, and exceeding client expectations. Valuable experience in cybersecurity, where I contributed to strengthening digital defenses and enhancing the security posture of technology infrastructures.

WORK EXPERIENCE

Software Engineer
Rubis
Tomsk, Russia
February 2022 - January 2023

- Collaborated with a diverse group of 150+ developers on various projects for clients such as IKEA, Samsung, IBM, and numerous other industrial and IT businesses.
- Engaged in end-to-end development processes, from concept and technical assignment creation to code writing, testing, deployment, and user education.
- Leveraged a wide range of programming languages and technologies, including C#, C++, and JavaScript, to develop software for different platforms (mobile, desktop, web).
- Contributed to projects involving AR/VR, Web & Cloud technologies (ASP.NET MVC, Node.js), and mobile development using Xamarin.
- Participated in advanced research initiatives related to AI, VR, and AR, keeping the company at the forefront of technological innovation.

Lead Penetration Tester
BI.ZONE
Moscow, Russia
March 2019 - January 2022

- Led extensive penetration testing efforts, both external and internal, to identify vulnerabilities and strengthen security postures for a wide range of industries.
- Specialized in the security analysis of web and mobile applications, employing deep dives into source code to unearth critical issues in Java, PHP, Golang, C#, Ruby, and Python applications.
- Contributed as an active member of the Red Team, devising and executing sophisticated cybersecurity attacks to test defenses, simulating real-world threat scenarios.

Software Engineer
NTR Labs
Tomsk, Russia
July 2017 - February 2019

- Collaborated with a team of 140+ world-class developers across different time zones, borders, and cultures to deliver exceptional software solutions.
- Specialized in core competencies such as AI, Blockchain, Big Data, computer vision, image recognition, and complex multi-platform systems.
- Contributed to the development of the world's first truly autonomous UAV for oil tank and structural inspections in 2016.
- Expanded expertise in outdoor navigation solutions, particularly in enabling drones to operate in the presence of GPS jammers.
- Worked on industrial solutions like the Smart Helmet, integrating navigation modules and video analytics systems for employee tracking and object recognition on factory floors.

• • •

Nous pouvons donc valider notre challenge.

FLAG : Andrejew Vladlen



Challenge 4 : La piste de l'emploi

Un CV ? Intéressant... S'il cherche du travail, il a forcément dû élargir son champ d'action.

Quel est le nom de la dernière entreprise où travaillait Andrejew ?

Format de Flag : **Ubik**

Nous reprenons nos investigations à partir du CV que nous venons de découvrir. Étant donné qu'Andrejew est en recherche d'emploi, il est probable qu'il ait également posté une annonce similaire sur le réseau LinkedIn. Nous lançons donc une recherche et trouvons un profil qui correspond au CV découvert sur X.

The image shows a LinkedIn profile for Andrejew Vladlen, a Software Engineer. The profile includes a photo, basic information, a summary section with 123 connections and 21 publications, and a 'View more' link. Below this, there's a 'Experience' section listing two roles:

- Software Engineer** at Rubius (Temps plein) from February 2022 to January 2023 (1 year). It mentions work with 150+ developers for clients like IKEA, Samsung, IBM, and others. A 'View more' link is present.
- Penetration Tester** at BI.ZONE (Temps plein) from March 2019 to January 2022 (2 years 11 months).

En confrontant nos deux sources, à savoir le CV et le compte Linkedin nous pouvons confirmer que la dernière entreprise où a travaillé Andrejew est : **Rubius**

Nous pouvons donc valider le challenge

FLAG : Rubius.



Challenge 5 : Coding

Vous vous trouvez face à un développeur plutôt junior ; il est temps d'en savoir plus.

Sur quel site publie-t-il son code ? (Uniquement le nom)

Format de Flag : Google

Nous poursuivons notre piste sur LinkedIn et trouvons un poste intéressant où Andrejew parle justement de codes qu'il aurait créés, notamment dans le langage de programmation Python.



A LinkedIn post from Andrejew Vladlen, Software Engineer, 3e et +, 2 mois. The post content is in Russian:

Je souhaitai vous partagé mon dernière creation ! Un jeu de roulette russe
💥💡 coder en Python 💡💥
J'espere que ca vous plait, dites moi votre avis 😊

The post also includes a link to "Русская рулетка - Pastebin.com" and social sharing options like J'aime, Commenter, Republier, and Envoyer.

Nous déduisons que le site qu'il utilise pour publier son code est **Pastebin**.

Nous pouvons valider le challenge.

FLAG : Pastebin.



Challenge 6 :

Python cela vous parle ?

Quel est le nom du programme de la roulette russe ?

*Format de Flag : **program.c***

Nous pouvons à présent poursuivre notre piste du Pastebin, et en parcourant le code nous tombons sur un commentaire (# For more scripts:

https://drive.google.com/drive/folders/1thBhACRzWCMbaPogfAbpaMTB4dZ32GTO?usp=drive_link) menant à un Google Drive.

```
18.     fatal_bullet = random.randint(1, int(chambers))
19.
20.    for x in range(1, int(chambers) + 1):
21.        input("Press enter to pull the trigger! ")
22.        if x == fatal_bullet:
23.            print("You just got served!")
24.            print("Game Over")
25.            break
26.        print("You will live to see another day")
27.
28.    start_again = input("Do you want to start again? (y/n): ")
29.    if start_again and start_again.lower()[0] != "y":
30.        break
31.
32. # For more scripts: https://drive.google.com/drive/folders/1thBhACRzWCMbaPogfAbpaMTB4dZ32GTO?usp=drive_link
```

Sur ce drive nous trouvons plusieurs fichiers en rapport avec la Russie.

- Un dossier dans lequel il y a un document texte avec une chaîne de caractères possiblement encodé
- Un document texte en russe
- Une photo du Kremlin
- Le code retrouvé précédemment sur le Pastebin nommé : **russian_roulette.py**
- Une vidéo d'une danse russe

Nous pouvons valider le challenge.



FLAG : [russian_roulette.py](#).

Challenge 7 : Petite baie

Vous avez maintenant accès à une information potentiellement utile, mais ce drive semble suspect.

Quel complice pourrez vous identifier grâce à ces informations sur le drive ?

Format de Flag : [G315tn1gm4](#)

Nous analysons les différents fichiers, et en ouvrant le document Word (document.docx), nous découvrons qu'au milieu de ce texte, un début d'URL de Google Drive(<https://drive.google.com/drive>) est dissimulé en blanc, car écrit en blanc sur fond blanc.

Мы, как нация, прошли через множество испытаний. Наша история учит нас быть сильными и единодушными. В трудные времена мы всегда находим пути преодолеть испытания вместе.

Образование и знания - ключ к нашему будущему. Поддерживая развитие науки и культуры, мы способствуем росту и благополучию нашего народа.
<https://drive.google.com/drive/>

Уважение к разнообразию нашей страны укрепляет нас. Разные культуры и традиции, сливаясь вместе, создают уникальное и богатое наследие нашей нации.

Nous continuons ainsi notre investigations et nous décidons d'analyser l'image Kremlin.png , on y découvres caché en bas à gauche en minuscule une autre partie d'un lien, surement la suite de notre liens google drive:
[folders/1eXT8Wxae6qgH52AkYmUvT](https://drive.google.com/drive/folders/1eXT8Wxae6qgH52AkYmUvT)



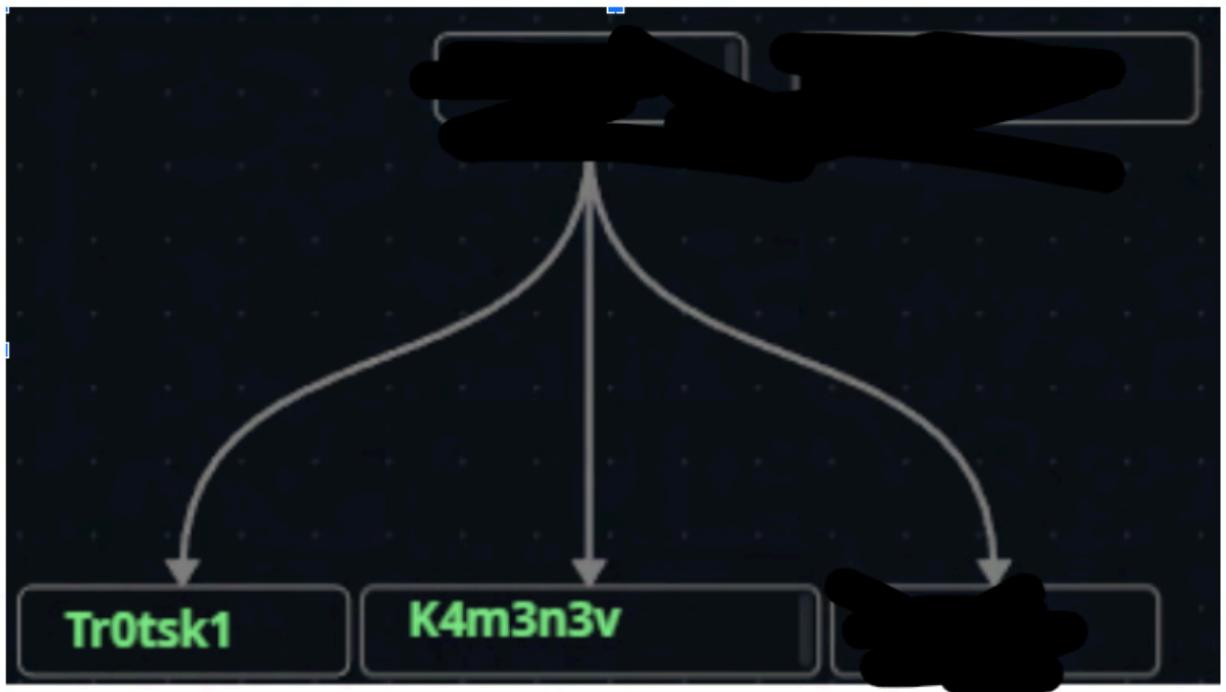


Puis en regardant attentivement la vidéo, nous remarquons une chaîne de caractères uniquement visible sur une image : "Mn6nDpQYbb6?usp=sharing" à 0:41. Nous pouvons en déduire que c'est une autre partie du lien.

Une fois le lien assemblé, cela donne :

<https://drive.google.com/drive/folders/1eXT8Wxae6qgH52AkYmUvTMn6nDpQYbb6?usp=sharing>

À travers ce drive, nous trouvons de nouveaux éléments, notamment un organigramme où seulement deux entités sont visibles. Nous apprenons également l'existence d'un second protagoniste : **K4m3n3v**.



Nous pouvons valider le challenge.

FLAG : **K4m3n3v.**

Challenge 8 : Here comes a new challenger !

Tiens, un nouvel arrivant ! Son pseudonyme vous interpelle. Vous l'avez déjà vu quelque part ou entendu quelqu'un en parler... mais où ?

Quel est le nom et prénom de la victime qui le mentionne ?

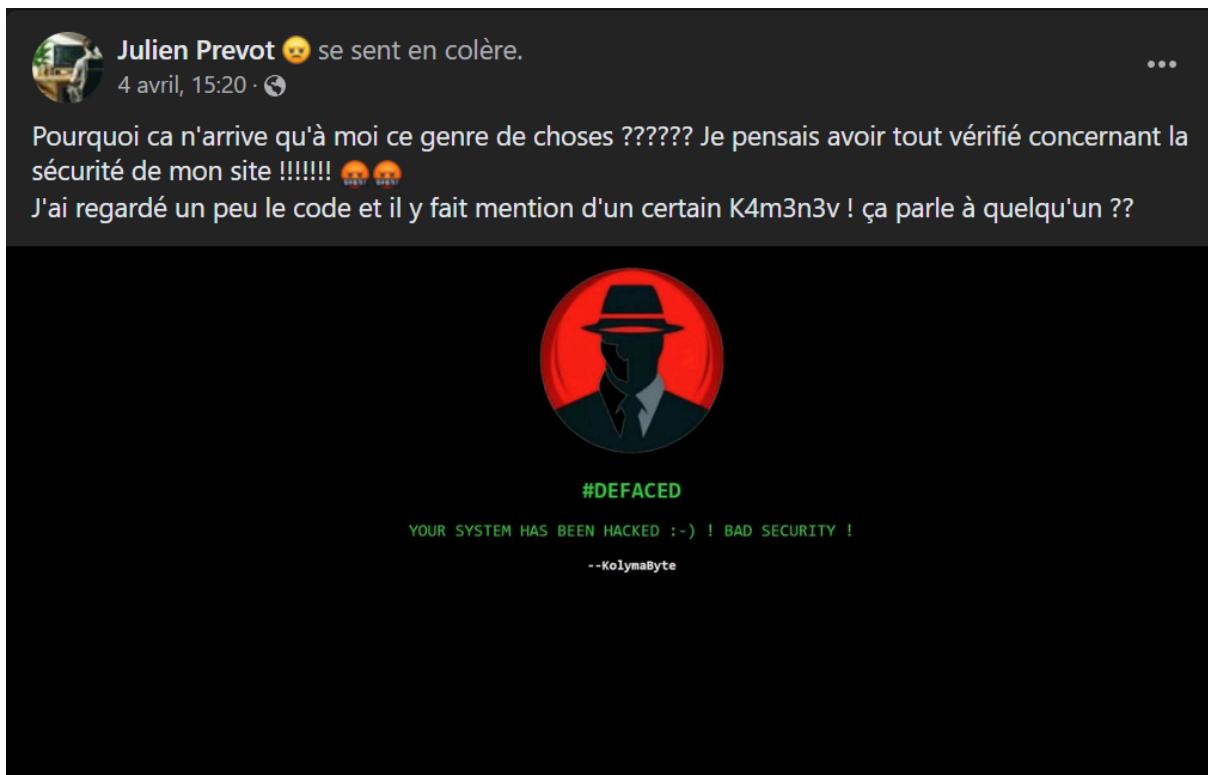
Format de Flag: **Lefebvre Jean**

La référence « Vous l'avez déjà vu quelque part ou entendu quelqu'un en parler » suggère que le nom de K4m3n3v a pu être mentionné quelque part, peut-être sur les réseaux sociaux.

En cherchant sur différents réseaux sociaux connus (X, Instagram, LinkedIn, etc.), nous trouvons une publication datée du 4 avril sur Facebook qui le mentionne.

Nous faisons la connaissance de **Julien Prevot**, qui se plaint que son site a été piraté et « défacé » par un certain K4m3n3v !





Nous pouvons donc valider le challenge.

FLAG : **Prevot Julien**

Challenge 9 : You have been h4ck3d !

Connaissez-vous le défacement ? C'est la méthode utilisée par un groupe de cybercriminels pour signaler qu'ils ont piraté un site.

Quel est le nom du groupe de hackers responsable de ce piratage ?

Format de Flag : *DarkSide*

En enquêtant davantage sur le compte Facebook de Julien Prévot, nous apprenons qu'il est développeur web et qu'il avait lancé un site consacré à la cryptomonnaie (SeaCipher). En visitant le site à l'adresse <https://sea-cipher.fr>, mentionnée dans une publication, nous constatons effectivement que le site a bien été piraté par une équipe nommée **KolymaByte**.





Nous pouvons valider le challenge.

FLAG : KolymaByte.

Challenge 10 : Infiltration virtuelle

Un défacement de site web est généralement causé par l'exploitation d'une vulnérabilité, permettant ainsi à un hacker de modifier facilement la page d'accueil.

Quel est le nom de l'outil utilisé par le hacker pour réaliser le défacement du site ?

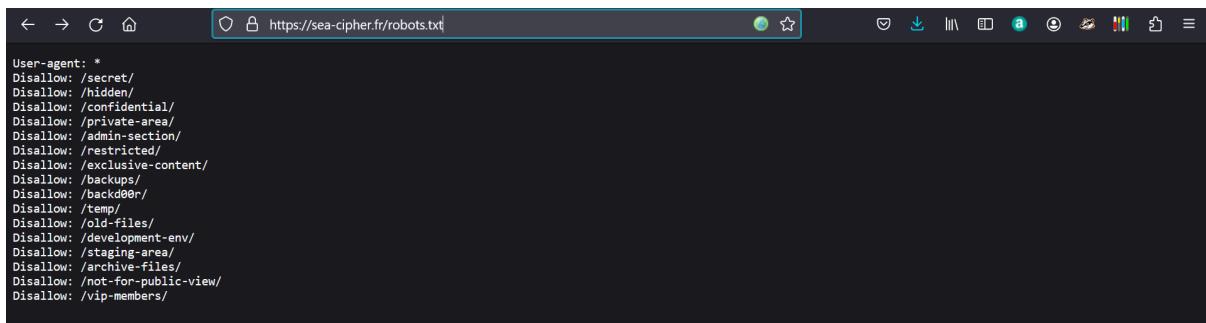
Format de Flag : MyMaliciousProgramV1

Comme mentionné précédemment, nous constatons que le site a été "défacé", ce qui indique qu'un attaquant a réussi à s'introduire sur le site web et y a probablement créé une voie d'accès permettant de modifier facilement les fichiers internes du site. Toutefois, ce "chemin" ne devrait pas être indexé par

les moteurs de recherche. Pour y parvenir, une technique consiste à indiquer aux robots d'indexation, via un fichier nommé robots.txt, de ne pas référencer certaines pages spécifiques.



Le fichier robots.txt révèle un lien plutôt suspect : "/backd00r". Nous allons donc poursuivre notre investigation sur cette piste.



Par acquis de conscience, nous examinons également le code source et le fichier sitemap.xml, mais rien ne nous aide à avancer.

En visitant le lien <https://sea-cipher.fr/backd00r>, nous découvrons un programme nommé **WebShellUploadV3**.



WebShellUploadV3

Current Path : /var/www/html/seacipher
PHP Version : 4.3.2
Upload File : Aucun fichier sélectionné.

Name	Size	Permissions
assets	--	drwxrwxrwx
index.html	5.044 KB	-rwxrwxrwx
exploit.php	7.753 KB	-rwxrwxrwx
robots.txt	1.245 KB	-rwxrwxrwx

Nous pouvons donc valider le challenge.

FLAG : WebShellUploadV3.

Challenge 11 : Update your system !

*Vous savez désormais comment le pirate a réussi à modifier le site.
Cependant, pour arriver à ce résultat, une inattention de la part du webmaster
a dû se produire.*

Quelle est la version de PHP installée sur le serveur ?

Format de Flag : 1.2.3

En consultant les détails du WebShell, nous identifions facilement la version de PHP installée qui est là **4.3.2**



Current Path : /var/www/html/seacipher
PHP Version : 4.3.2
Upload File : Aucun fichier sélectionné.

Nous pouvons donc valider le challenge

FLAG : **4.3.2.**

Challenge 12 : Crypto

Par curiosité, vous vous penchez sur le business de ce site internet, il semble être tourné sur l'univers de la cryptomonnaie.

Quel était le cours du SeaCipher fin Mars 2024 ?

Format de Flag : 0.000000018

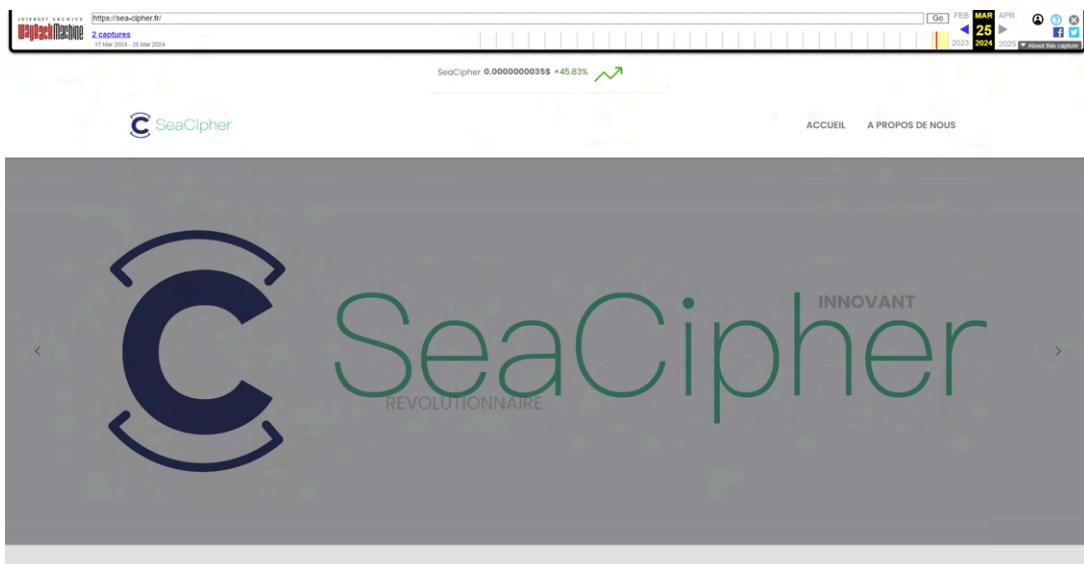
Nous devons retrouver le cours du SeaCipher à la fin de mars 2024, mais actuellement le site n'est plus accessible. Cependant, en examinant la publication Facebook du 2 avril sur le compte de Julien Prévot, nous pouvons voir sur la capture d'écran le cours du SeaCipher tout en haut du site.



The screenshot shows a Facebook post from Julien Prevot. The post includes a profile picture of a person with glasses, the name "Julien Prevot", the date "2 avril à 13:17", and a link "https://sea-cipher.fr !!". Below the post is a screenshot of the SeaCipher website homepage. The website features a large stylized "C" logo and the word "SeaCipher" in green. A banner at the top says "UNE NOUVELLE CRYPTOMONNAIE EST ARRIVÉE" and "La prochaine cryptomonnaie dans votre portefeuille". Below the banner, there is a brief welcome message about the new digital currency.

Cependant, la publication date du 2 avril et il est possible que le cours du SeaCipher ait changé entre la fin mars et le 2 avril. Pour en être sûr, il faudrait pouvoir remonter dans le temps pour trouver une sauvegarde. Nous allons donc vérifier si des sauvegardes du site ont été réalisées sur WaybackMachine.org.

Ainsi, nous retrouvons une sauvegarde du site datant du 25 mars 2024 qui affiche le même cours que celui observé sur la capture d'écran de la publication du 2 avril.



En haut de la page nous pouvons donc voir que le cours du SeaCipher est de **0.0000000035\$**.

Nous pouvons valider le challenge.

FLAG : 0.0000000035.

Challenge 13 : Signature

Les hackers aiment laisser leur signature sur leurs « œuvres ».

Sous quel autre pseudonyme le hacker est-il également connu ?

FLAG : L4p5u5

Nous examinons en détail l'outil utilisé par le hacker le WebShellUploadV3, en particulier le code source, et nous trouvons rapidement le pseudonyme dans la balise "content"

```
1 <!DOCTYPE html>
2 <html lang="en">
3 <head>
4   <meta charset="UTF-8" />
5   <meta name="author" content="_v3n3m4K_">
6   <meta name="viewport" content="width=device-width, initial-scale=1.0" />
7   <title>HACKED BY KOLYMABYTE</title>
8   <link rel="stylesheet" href="styles.css" />
9 </head>
10
```

Nous remarquons la différence entre le pseudo K4m3n3v et _v3n3m4K_

Nous pouvons valider le challenge.

FLAG : _v3n3m4K_



Challenge 14 : L'entreprise sous attaque

Vous commencez maintenant à esquisser un profil. Poursuivez vos investigations.

Quelle entreprise le pirate cible-t-il à travers ses actions ? (Son nom complet)

Format de Flag : Lightning Cyber Technologies

Grâce à notre nouvelle découverte, nous allons enquêter sur ce nouveau profil (**_V3n3m4K_**) pour voir ce qu'il en découle. Nous effectuons donc une recherche avec WhatsMyName et obtenons des résultats, désormais sur le site Mastodon.

Enter the username(s) in the

v3n3m4K

≡ Category Filters ▾

Active Filter: All (exclude NSFW)

Found: 2 Processed: 590 / 590

[Show Found](#) [Show False Positives](#) [Show Not Found](#) [Show All](#) [Open All Links](#)

Mastodon-API

Username: _v3n3m4K_
Category: social
Account Found

Mastodon-mastodon

Username: _v3n3m4K_
Category: social
Account Found

The screenshot shows a Mastodon profile page for the user `_v3n3m4K_`. At the top left is a blue elephant icon. To the right are three buttons: a grey square with a white icon, a grey square with three dots, and a blue rounded rectangle labeled "Follow". Below the icon is the handle `_v3n3m4K_`, the URL `mastodon.social`, and a lock icon. A message "Follow me github.com/k4menev/" is displayed. A grey box indicates the user joined on Mar 13, 2024. At the bottom, the stats are shown: 11 Posts, 3 Following, and 0 Followers.

En analysant le compte Mastodon, nous trouvons des publications assez génériques qui apportent peu à notre enquête, mais nous découvrons surtout un lien vers un compte GitHub:

The screenshot shows a GitHub profile page for the user `k4menev`. The profile picture is a purple pixelated logo. Below it is an "Edit profile" button. The main area displays six popular repositories: `rootkit` (forked from `iyli/rootkit`, Public, Sample Rootkit for Linux, TeX), `Reptile` (forked from `f0rb1dd3n/Reptile`, Public, LKM Linux rootkit, C), `BlackMamba` (forked from `loseys/BlackMamba`, Public, C2/post-exploitation framework, Python), `PoshC2` (forked from `nettitude/PoshC2`, Public, A proxy aware C2 framework used to aid red teamers with post-exploitation and lateral movement, PowerShell), `Cronos-Rootkit` (forked from `XaFF-XaFF/Cronos-Rootkit`, Public, Cronos is Windows 10/11 x64 ring 0 rootkit, able to hide processes, protect and elevate them with token manipulation, C++), and `first-try` (Public, C). A "Customize your pins" section is visible at the top right.

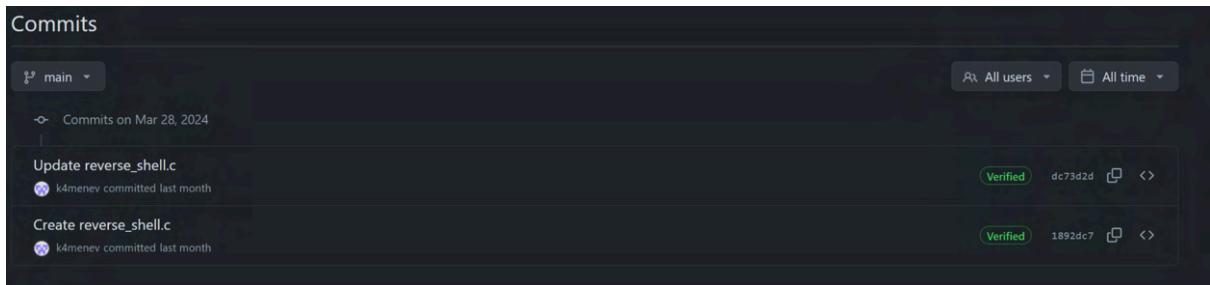
Sur le compte GitHub, nous trouvons des dépôts de malwares en tout genre (Rootkit, C2, etc.), mais surtout un repo d'un reverse shell écrit en C :

The screenshot shows a GitHub repository page for 'first-try'. The repository is public and has 1 branch and 0 tags. There is one commit by 'k4menev' titled 'Update reverse_shell.c' made 2 months ago. The file 'reverse_shell.c' is listed with its last update 2 months ago. Below the file list, there is a section to 'Add a README' with a button to do so.

En analysant succinctement le code, nous voyons qu'il est possible de spécifier une cible au niveau de la ligne 9 :

```
1 // Alpha version test
2 #include<stdio.h>
3 #include<string.h>
4
5 unsigned char code[] = \
6
7 // To encode ! /!\'
8 "section .data
...
9     text db 'target_website', length
10    section .TEXT
11    global _start _start:
12        xor eax, eax
13        xor ebx, ebx
```

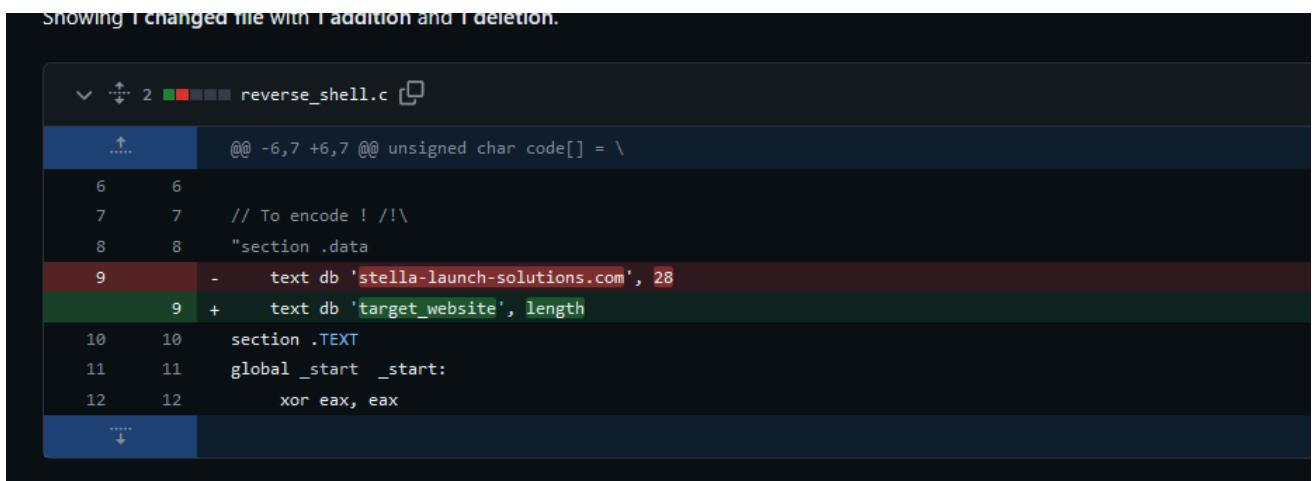
La dernière version du reverse shell ne permet d'avoir des infos intéressantes, cependant en consultant l'historique du repo, nous constatons qu'il y a eu une création et une mise à jour du reverse shell.



The screenshot shows a GitHub commit history for a repository. The main dropdown menu is set to 'main'. The search bar shows 'Commits on Mar 28, 2024'. There are two commits listed:

- Update reverse_shell.c** by k4menev committed last month. This commit has a green 'Verified' badge and a commit hash dc73d2d. It includes a copy and paste icon and a diff view icon.
- Create reverse_shell.c** by k4menev committed last month. This commit also has a green 'Verified' badge and a commit hash 1892dc7. It includes a copy and paste icon and a diff view icon.

On retrouve le commit de base pour ajouter le code sur GitHub et une mise à jour du code. En cliquant sur la mise à jour, nous voyons que cette dernière a mis à jour la target.



The screenshot shows a GitHub diff view for the file 'reverse_shell.c'. The title indicates there is 1 changed file with 1 addition and 1 deletion. The diff shows the following code changes:

```
@@ -6,7 +6,7 @@ unsigned char code[] = \  
 6      6  
 7      7      // To encode ! /!\\  
 8      8      "section .data  
 9      -      text db 'stella-launch-solutions.com', 28  
 9      +      text db 'target_website', length  
10     10      section .TEXT  
11     11      global _start _start:  
12     12          xor eax, eax  
.....
```

Nous découvrons donc une nouvelle entité, **Stella Launch Solutions**.

Nous pouvons valider le challenge.

FLAG : **Stella Launch Solutions**



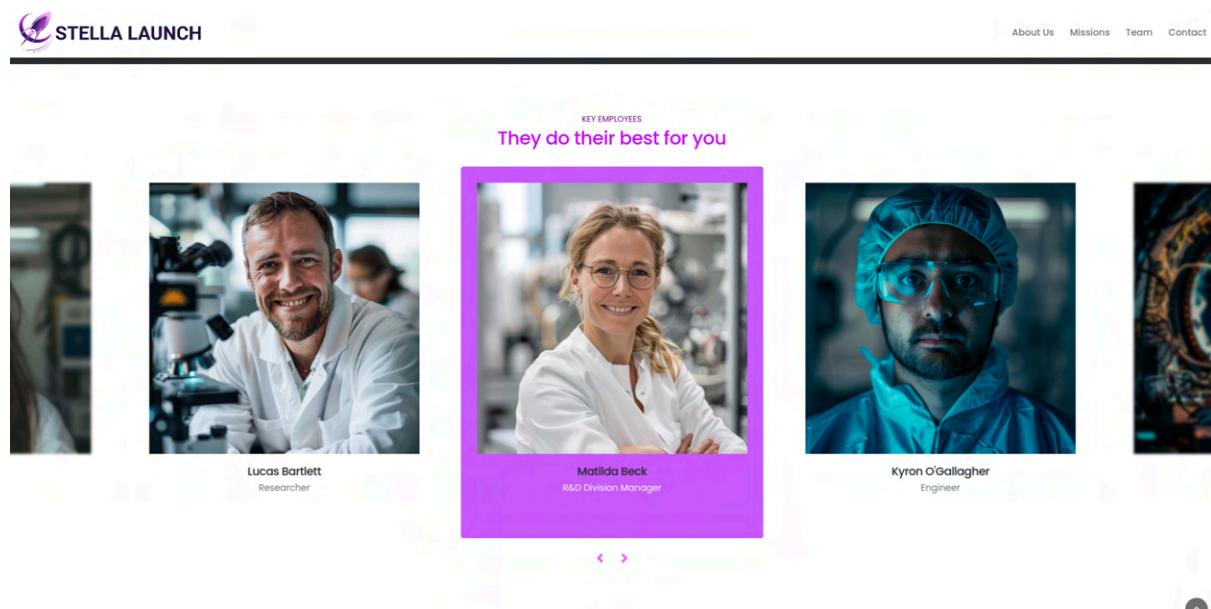
Challenge 15 : Mise en orbite

Le pirate envisage de pirater le site d'une entreprise spécialisée dans la mise en orbite de satellites, mais dans quel but ?

Quel est le nom du responsable de la section R&D ? (Respectivement Prenom et Nom)

Format de Flag : Jeanne Dupont

En consultant le site actuel de Stella Launch (stella-launch-solutions.com), nous trouvons rapidement la responsable de la section R&D, grâce à la section “Team” du site.



Il s'agit de : **Matilda Beck**

Nous pouvons valider le challenge.

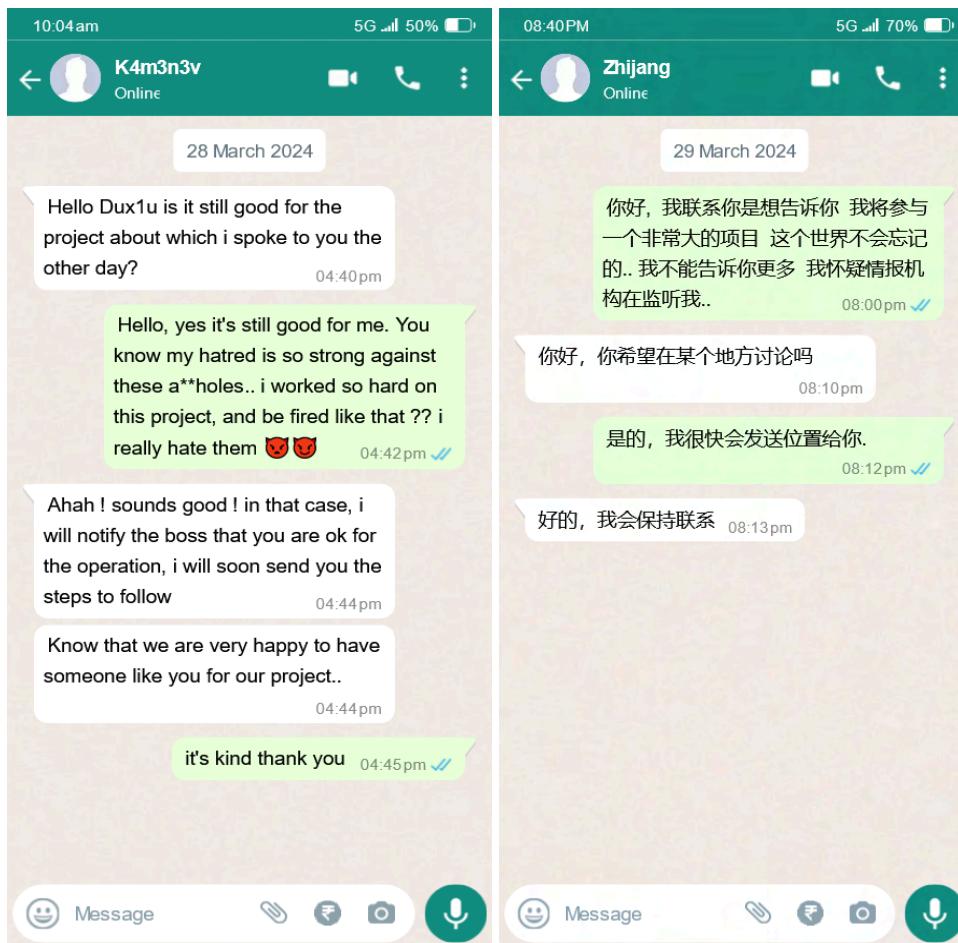
FLAG : Matilda Beck

Challenge 16 : Enigme des ondes

Nos services de renseignement ont intercepté une communication. Il semble qu'une personne cherche à établir un contact.

Quel nouveau pseudonyme pouvez-vous en déduire ?

Format de Flag : M4x1m3



En analysant la première capture d'écran, nous voyons K4m3n3v discutant avec un certain **Dux1u**, ce dernier à l'air énervé envers une certaine société qui l'aurait viré ! Est-ce Stella Launch ? Quoi qu'il en soit, nous pouvons valider le challenge.

FLAG : Dux1u



Challenge 17 : Un bon ami

A travers ces communications, vous avez pu en tirer certaines informations.

Quel est le prénom de l'ami de Dux1u ?

Format de Flag : Alexandre

Dans la deuxième capture d'écran, nous pouvons voir le nom de son ami en haut de la conversation : **Zhijang**.

Nous pouvons valider le challenge.

FLAG : Zhijang

Challenge 18 : L'identité Révélée

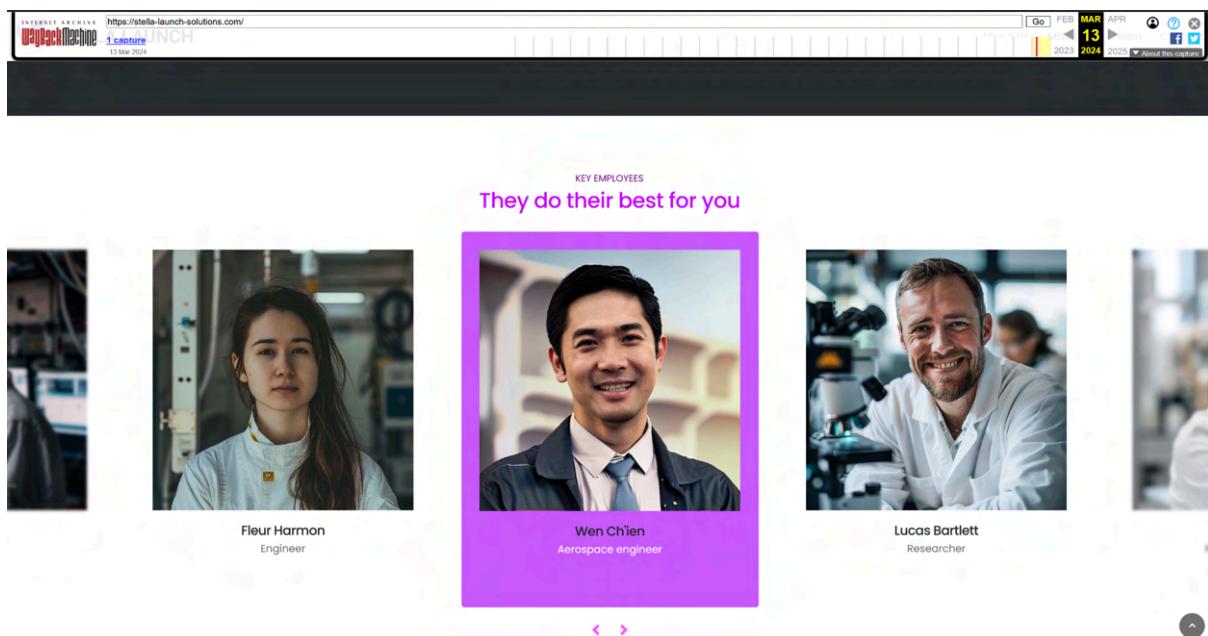
Progressivement, vous commencez à saisir ce qui se trame. Continuez votre enquête.

Quelle est la véritable identité de Dux1u ? (Nom suivi du prénom)

Format de Flag : Dupont Arnaud

En analysant les captures d'écran, nous comprenons qu'il y a eu un possible accrochage entre Dux1u et l'entreprise Stella Launch Solutions. Il est donc tout à fait probable que ce dernier ait été dans l'entreprise avant d'être licencié. Nous cherchons donc un moyen de remonter dans le temps vis-à-vis d'un site internet. Ainsi, nous allons une nouvelle fois nous pencher sur WayBackMachine, où nous trouvons une capture du 13 mars 2024. Dans la section Team, nous retrouvons une personne d'origine asiatique se prénommant Wen Ch'ien, qui semble correspondre à notre suspect !





Nous pouvons valider le challenge.

FLAG : Ch'ien Wen

Challenge 19 : Command & Control

Vous êtes désormais au courant de la menace qui plane sur la société Stella Launch Solutions. Il est possible qu'une compromission ait eu lieu.

Quel est le nom de la backdoor utilisée ?

Note : Une backdoor, ou porte dérobée, est un programme malveillant conçu pour permettre aux pirates un accès à distance non autorisé.

Format de Flag : MyMaliciousProgramV1.2

Si nous reprenons la logique de la première backdoor, nous pouvons en déduire que la personne à l'origine de la seconde backdoor n'est autre que K4m3n3v lui-même. Nous tentons donc d'appliquer la même logique et effectuons une recherche sur le fichier robots.txt, mais celle-ci se révèle infructueuse :

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

Nous tentons donc avec un autre fichier, le **sitemap.xml**, également présent sur différents sites internet pour gérer le référencement des pages.

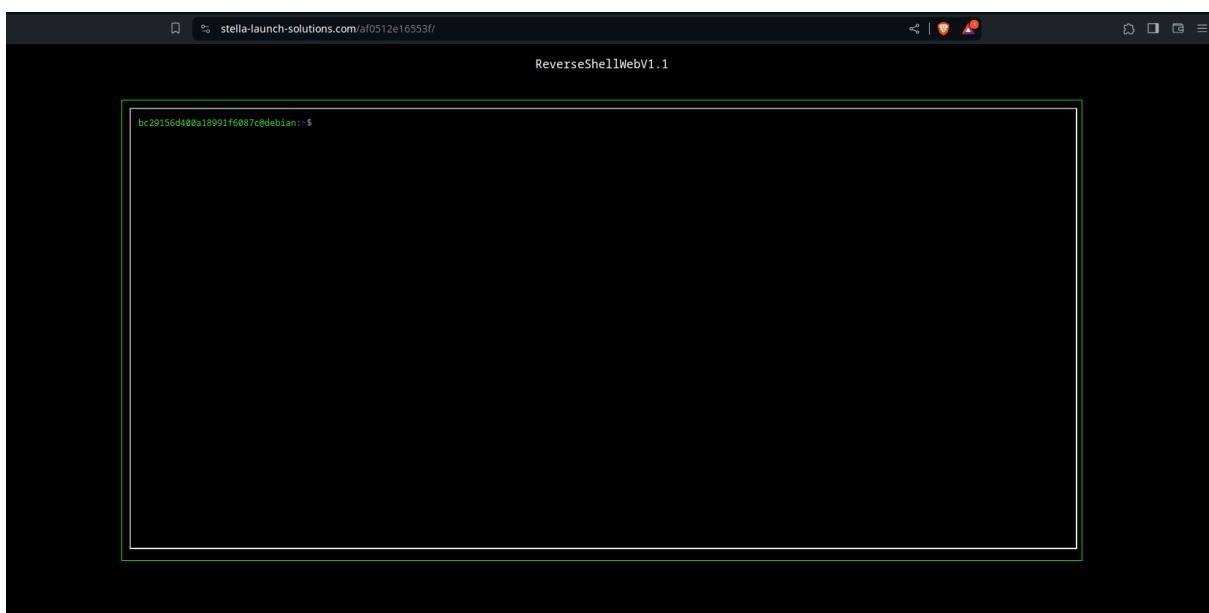
En saisissant donc l'URL (<https://stella-launch-solutions.com/sitemap.xml>) et en fouillant, nous tombons sur une URL suspecte :



```
-<url>
--<loc>
    https://www.stella-launch-solutions.com/undisclosed-partners
</loc>
<changefreq>never</changefreq>
<priority>0.1</priority>
</url>
-<url>
--<loc>
    https://www.stella-launch-solutions.com/launch-archive
</loc>
<changefreq>never</changefreq>
<priority>0.1</priority>
</url>
-<url>
--<loc>
    https://www.stella-launch-solutions.com/af0512e16553f
</loc>
<changefreq>never</changefreq>
<priority>0.1</priority>
</url>
-<url>
--<loc>
    https://www.stella-launch-solutions.com/secret-project-x
</loc>
<changefreq>never</changefreq>
<priority>0.1</priority>
</url>
-<url>
--<loc>
    https://www.stella-launch-solutions.com/undisclosed-blueprints
```

En nous rendant sur cette URL

(<https://www.stella-launch-solutions.com/af0512e16553f>), nous tombons sur un accès terminal du serveur web de Stella Launch. Ce dernier se nomme **ReverseShellWebV1.1**.



Nous pouvons valider le challenge.

FLAG : ReverseShellWebV1.1

Challenge 20 : Traffic dissimulé

Un serveur C2, ou Command & Control, sert à contrôler des appareils infectés et à dérober des données. Ce système fonctionne grâce à l'utilisation d'un agent et d'un serveur.

Quelle est la version de l'agent installé ?

Format de Flag : 1.2.3

Afin de pouvoir utiliser le serveur C2, nous utilisons la commande help pour connaître la liste des commandes possibles. Nous constatons que la commande **startc2server** permet de l'activer. Suite à son utilisation, le serveur s'allume et nous pouvons constater que l'Agent est en version 1.1.3.

ReverseShellWebV1.1

```
bc29156d400a18991f6087c@debian:~$ help
Available commands: help, startc2server, id, pwd, extractpasswd
bc29156d400a18991f6087c@debian:~$ id
uid=1000(bc29156d400a18991f6087c) gid=1000(bc29156d400a18991f6087c) groups=1000(www-data), 4(adm), 24(cdrom), 27(sudo)
bc29156d400a18991f6087c@debian:~$ startc2server
[i] starting server.....
[i] Try to connect to the remote server !
[+] Connect to the remote server !
.
.
.
.
.

[i] Session detail
[i] Host : DzT(X*bSyIGHq+43GHv*kG4Rygp^+kjVE^=RrF+f@Rt0C0^=DYk+kA6}JNF#jw^8HgkpTt5Wt)qCB
[i] Agent : v1.1.3
[+] Status : Connected
bc29156d400a18991f6087c@debian:~$
```

Nous pouvons valider le challenge.

FLAG : 1.1.3



Challenge 21 : Revente

Maintenant que vous disposez d'un outil qui semble avoir été développé par notre pirate, K4m3n3v, il est essentiel de découvrir son fonctionnement !

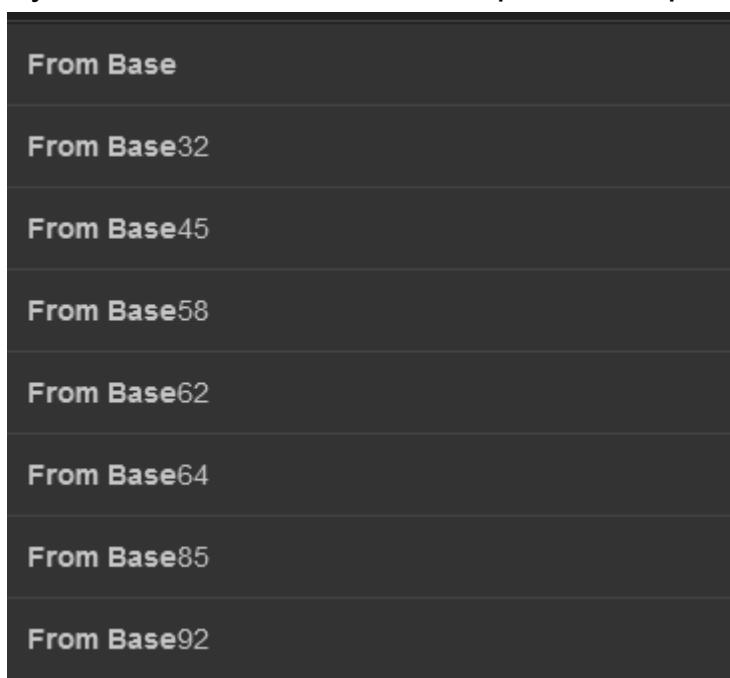
À quelle URL le serveur de commande et de contrôle (C2) est-il connecté ?

Format de Flag : <https://3g2up14pq6kufc4m.xyz>

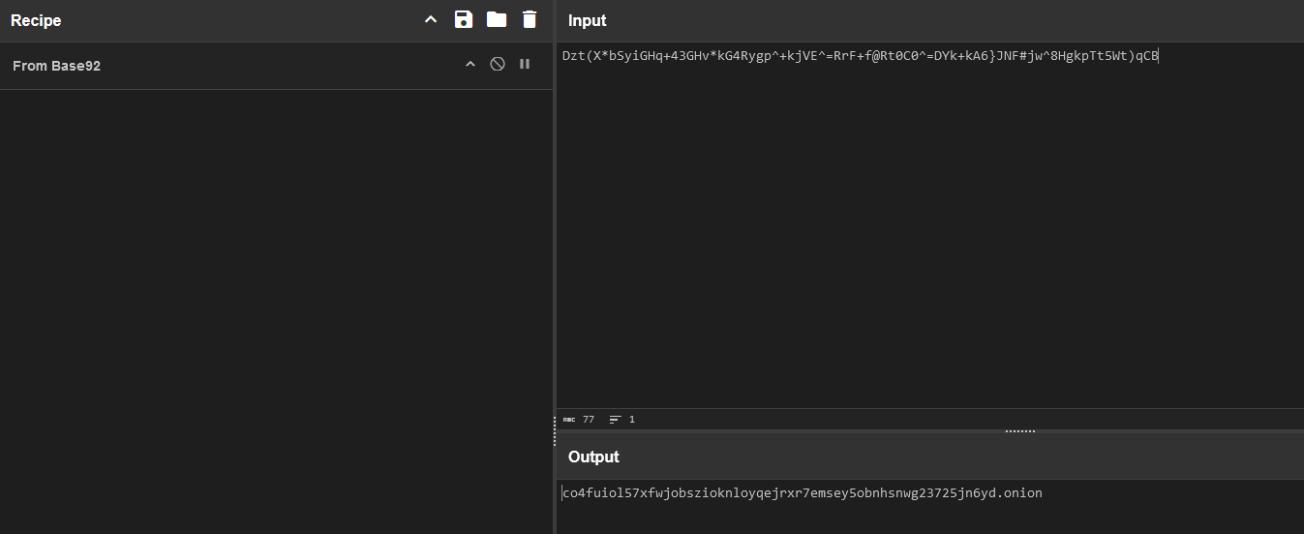
En exécutant la commande **startc2server**, celle-ci nous donne quelques détails sur la session, notamment sur un host. Cependant, ces informations semblent être chiffrées ou encodées.

"Dzt(X*bSyiGHq+43GHv*kG4Rygp^+kjVE^=RrF+f@Rt0C0^=DYk+kA6}JNF #jw^8HgkpTt5Wt)qCB"

En examinant tous nos éléments, nous n'avons aucune indication sur une quelconque clé de chiffrement. Ainsi, pour éviter de tester tous les chiffrements possibles, nous pouvons partir de cette théorie. Afin de faciliter les transferts et la représentation des données, la plupart des développeurs utilisent le Base64 (comme nous avons pu le voir dans la lettre au début du CTF). Cependant, notre chaîne ne ressemble pas à du Base64. En utilisant notre outil CyberChef, nous constatons qu'il existe plusieurs bases.



Nous les testons une par une et trouvons un résultat intéressant avec le Base92.



The screenshot shows the Base92 application window. On the left, there's a 'Recipe' section with a dropdown menu set to 'From Base92'. The main area is divided into 'Input' and 'Output' sections. In the 'Input' section, there is a large, complex string of characters: 'Dzt(X*bSyiGHq+43GHv*kG4Rygp^+kjVE^=RrF+f@Rt0C0^=DYk+kA6}JNF#jw^8HgkpTt5wt)qCB|'. Below this, in the 'Output' section, the converted string is shown: 'co4fuiol57xfwjobszioknloyqejr7emsey5obnhsnwg23725jn6yd.onion'. At the bottom of the window, there are some status indicators: 'REC 77', 'F 1', and a progress bar.

Nous trouvons un lien .onion

“co4fuiol57xfwjobszioknloyqejr7emsey5obnhsnwg23725jn6yd.onion”

Nous pouvons valider le challenge.

FLAG :

<http://co4fuiol57xfwjobszioknloyqejr7emsey5obnhsnwg23725jn6yd.onion>

Challenge 22 : Monnaie virtuelle

La cryptomonnaie est la monnaie de prédilection sur le darknet.

Quelle est l'adresse du portefeuille crypto utilisé pour acheter des données ?

Format de Flag : 0xFa21BcD45E67A89fBc12De34Fa567BcD890EaF12

En accédant au site .onion via TOR, nous découvrons qu'il s'agit d'un marché de vente de données. D'ailleurs, nous y retrouvons d'anciennes connaissances...

The screenshot shows a dark-themed website for 'KolymaByte'. At the top, there's a navigation bar with 'Рынок KolymaByte' and 'прием Как купить'. Below the header is a large circular logo featuring a silhouette of a man wearing a fedora hat against a red background. The text 'Требуйте только качества' (Demand only quality) is centered below the logo. The main content area displays four items for sale in boxes:

Название	Описание	Цена
"SeaCipher"	Все базы данных с приватным ключом кошелька администратора	97,589 ETH
"Les Enfants d'Hades"	Фамилия, Имя, Адрес, Социальное страхование, Номер телефона, Кредитная карта	0,836 ETH
"StellaLaunch"	База данных, фамилия, имя, адрес, номер телефона, пароль	41,824 ETH
"Tech Consulting"	База данных, фамилия, имя, адрес, номер телефона, пароль	39,035 ETH

En fouillant le site internet, nous tombons rapidement sur un message contenant ce qui semble être une adresse de wallet crypto.

A message box with a light gray background and a thin black border. It contains the following text:

Как купить

Для покупки просто отправьте точную сумму в ETH на этот криптовалютный кошелек 0xCec4748becc7eC74214cA0BD**b3bC8DDAf68D4108**. Затем вам будет отправлено подтверждающее сообщение, и вы сможете загрузить данные в течение 5 дней.

Спасибо за ваше доверие!

En traduisant le message, nous confirmons notre hypothèse

The screenshot shows a translation tool interface. At the top, there are language selection buttons: 'Déetecter la langue' (Detect language), 'Russe' (Russian) which is selected, 'Arabe' (Arabic), 'Français' (French), and a dropdown arrow. Below these are buttons for 'Turc' (Turkish), 'Anglais' (English), and 'Français' (French). On the right side of the interface are buttons for 'Copier le texte' (Copy text) and 'Télécharger la traduction' (Download translation). There is also a close button 'X'. The main area contains two text boxes. The first box, labeled 'Comment acheter', contains the text: 'Pour acheter, envoyez simplement le montant exact en ETH sur ce portefeuille de crypto-monnaie 0xSes4748becc7eC74214cA0BDb3bC8DDAf68D4108. Un message de confirmation vous sera alors envoyé et vous pourrez télécharger vos données sous 5 jours.' The second box, labeled 'Merci pour la confiance!', contains the text: 'Merci pour la confiance!'. At the bottom right of the interface, there is a link 'Envoyer des commentaires' (Send comments).

Nous avons donc le porte-monnaie crypto :

0xCec4748becc7eC74214cA0BDb3bC8DDAf68D4108

Nous pouvons valider le challenge.

FLAG : 0xCec4748becc7eC74214cA0BDb3bC8DDAf68D4108

Challenge 23 : Achat

Des individus mal intentionnés ou avides de pouvoir seraient probablement intéressés par ce que propose KolymaByte.

Quelle est l'adresse du portefeuille crypto qui a acheté les données de « Gourmet Brasserie » ?

Format de Flag : 0xAb34FcD89e76BfA12CdE45B3a7890cD2EaF56B78

Étant donné que nous avons l'adresse du portefeuille crypto et sachant qu'il est possible de suivre les transactions sur une blockchain via des sites spécialisés (comme EtherScan, par exemple), et sachant que nous sommes sur le réseau Sépolia (comme annoncé par le staff lors du CTF), nous pouvons donc utiliser le site <https://sepolia.etherscan.io>.



Nous rentrons donc l'adresse du porte-monnaie crypto en question

The screenshot shows the Etherscan Sepolia Testnet Explorer interface. The search bar at the top contains the address `0xCec4748becc7eC74214cA0BDb3bC8DDAf68D4108`. Below the search bar, there are sections for "Latest Blocks" (block 5854801, 28 secs ago) and "Transactions". The "Transactions" section displays 8 transactions from the address, with columns for Transaction Hash, Method, Block, Age, From, To, Value, and Txn Fee.

Transaction Hash	Method	Block	Age	From	To	Value	Txn Fee
<code>0x2d7634b1c3...</code>	Transfer	5626415	33 days ago	<code>0xff374A42...A318aa200</code>	<code>0xCec4748b...Af68D4108</code>	1.4240613 ETH	0.0000315
<code>0xc98d285672...</code>	Transfer	5626210	33 days ago	<code>0xCec4748b...Af68D4108</code>	<code>0xD1C7d77...43faC36C4</code>	2.42354676 ETH	0.0000315
<code>0x4f57753eb4e...</code>	Safe Mint	5622674	33 days ago	<code>0xCec4748b...Af68D4108</code>	<code>0x9F64932B...921f372B6</code>	0 ETH	0.00043491
<code>0x6675c8c349...</code>	Safe Mint	5622662	33 days ago	<code>0xCec4748b...Af68D4108</code>	<code>0x9F64932B...921f372B6</code>	0 ETH	0.00043931
<code>0xf0dc112e846...</code>	Safe Mint	5622633	33 days ago	<code>0xCec4748b...Af68D4108</code>	<code>0x9F64932B...921f372B6</code>	0 ETH	0.00044013
<code>0x067b85c029...</code>	Transfer	5578939	39 days ago	<code>0xee70bdE4...A73D3eF52</code>	<code>0xCec4748b...Af68D4108</code>	1.337 ETH	0.00003773
<code>0xbe4b96914d...</code>	Transfer	5578937	39 days ago	<code>0xFB4F595...681496F85</code>	<code>0xCec4748b...Af68D4108</code>	4.12345 ETH	0.00003749
<code>0x17274242d2...</code>	Transfer	5578934	39 days ago	<code>0xD5e107b...54f60d6ff</code>	<code>0xCec4748b...Af68D4108</code>	6.997 ETH	0.00003906

Et nous voyons effectivement qu'il y a eu des transactions entrantes et sortantes.

The screenshot shows the Etherscan Sepolia Testnet Explorer interface, focusing on the latest transactions for the address `0xCec4748becc7eC74214cA0BDb3bC8DDAf68D4108`. The transactions listed are all "Safe Mint" operations, which are indicated by the "IN" icon in the "To" column. These transactions show funds being sent to the address from other accounts.

Transaction Hash	Method	Block	Age	From	To	Value	Txn Fee
<code>0x4f57753eb4e...</code>	Safe Mint	5622674	33 days ago	<code>0xCec4748b...Af68D4108</code>	<code>0x9F64932B...921f372B6</code>	0 ETH	0.00043491
<code>0x6675c8c349...</code>	Safe Mint	5622662	33 days ago	<code>0xCec4748b...Af68D4108</code>	<code>0x9F64932B...921f372B6</code>	0 ETH	0.00043931
<code>0xf0dc112e846...</code>	Safe Mint	5622633	33 days ago	<code>0xCec4748b...Af68D4108</code>	<code>0x9F64932B...921f372B6</code>	0 ETH	0.00044013

En nous penchant un peu plus sur ces trois transactions sortantes, nous voyons qu'un contrat a été transmis. Puis, en cliquant sur « See more details »

Additional Info	Age
Status: Success (232244 Block Confirmations)	33 days ago
Token Transfer: ERC-721 Faucet (FA721) Token ID 42 From 0x00000000...00000000 To 0xcD5e107b...54f60c	33 days ago
Transaction Fee: 0.00044013788135 ETH (\$0.00)	33 days ago
Gas Info: 291,553 gas used from 442,551 limit @ 0.00000000150963249 ETH (1.50963249 Gwei)	39 days ago
Nonce: 0 (in the position 18)	39 days ago
See more details ↗	to receive funds f

Nous avons une page qui s'ouvre avec tous les détails de la transaction, y compris des données encodées.



En décodant, nous tombons sur un lien :

#	Name	Type	Data
0	to	address	0xcD5e107b4A3884dA16db5ef4f73d48954f60d6ff
1	uri	string	https://nftstorage.link/ipfs/bafybeicrzmtvergh5dedb3dtnkdq5svbr2dunlidodrs126iy742fm7equ/f8209d17-6cae-44f6-aad0-75debbca2f37.json

[Switch Back](#)

Puis en rentrant ce lien, nous trouvons un second lien menant vers un fichier PDF.

```
JSON    Données brutes    En-têtes
Enregistrer Copier Tout réduire Tout développer Filtrer le JSON
name: "invoice-01235"
description: "Invoice 01235"
▼ image: "https://nftstorage.link/ipfs/bafybeicxbfgp2ea3cgrblptdxao3iqa4feea46xol2vzi7sshdl5rh5wsi/invoice-01235.pdf"
animation_url: null
external_url: "https://darkcodi.github.io/nft-faucet/"
```

Et nous tombons à présent sur une facture, qui semble correspondre à une vente de données.





INVOICE

Invoice Number: INV-01235

INVOICE SUMMARY

To: 0xCec4748becc7eC74214cA0BD**b**3bC8DDAf68D4108

From: 0xaFB4F59507C1E055A61c360Bd29F90c681496F85

Description of Item: Ancien Salon de thé

Content: База данных, фамилия, имя, адрес, номер телефона, пароль

Price: 4.12345 ETH

Note: "Dans le silence des mots non prononcés, réside la profondeur des sentiments inexplorés." #AU

Nous répétons les mêmes actions pour les deux autres factures, et nous trouvons la facture concernant la vente de données du “Gourmet Brasserie”

INVOICE SUMMARY	
To:	0xCec4748becc7eC74214cA0BDb3bC8DDAf68D4108
From:	0xee70bdE4Bc29F2491b8aeF671298E0bA73D3eF52
Description of Item:	Gourmet Brasserie

Nous avons donc notre acheteur :

0xee70bdE4Bc29F2491b8aeF671298E0bA73D3eF52

Nous pouvons valider le challenge.

FLAG : 0xee70bdE4Bc29F2491b8aeF671298E0bA73D3eF52



Challenge 24 : La clé financière

Vous prenez désormais du recul par rapport aux éléments en votre possession. La plupart des groupes organisés font appel à un ou une trésorière pour gérer les finances. Cependant, un détail vous intrigue...

Quel pseudonyme trouvez-vous ?

Format de Flag : Nova_Eclipse

En analysant les différentes factures, un élément nous interpelle : il s'agit des notes apposées en fin de page.

Note: "Chaque cœur possède une mélodie secrète, attendante qu'une âme sœur vienne l'orchestrer." #AU

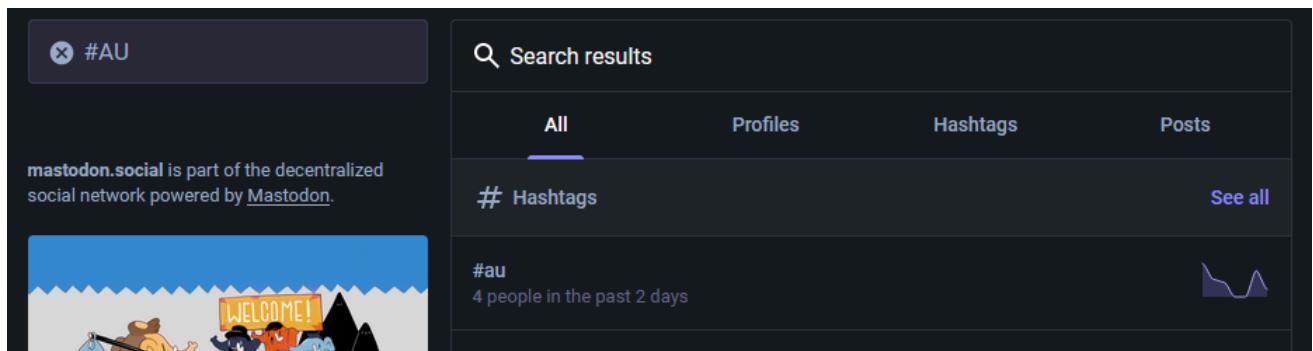
Note: "Sous la voûte étoilée, nos rêves tissent le fil d'or de notre destinée, invisibles mais éternellement présents." #AU

Note: "Dans le silence des mots non prononcés, réside la profondeur des sentiments inexplorés." #AU

Nous pouvons effectuer une recherche sur les différentes notes à travers les réseaux sociaux ainsi que sur le hashtag #AU, qui semble être une signature, peut-être des initiales ?

Les recherches sur Facebook, Twitter, LinkedIn et Instagram ne donnent rien. Cependant, en recherchant sur Mastodon.social via le hashtag #AU, nous voyons qu'il existe des posts associés.



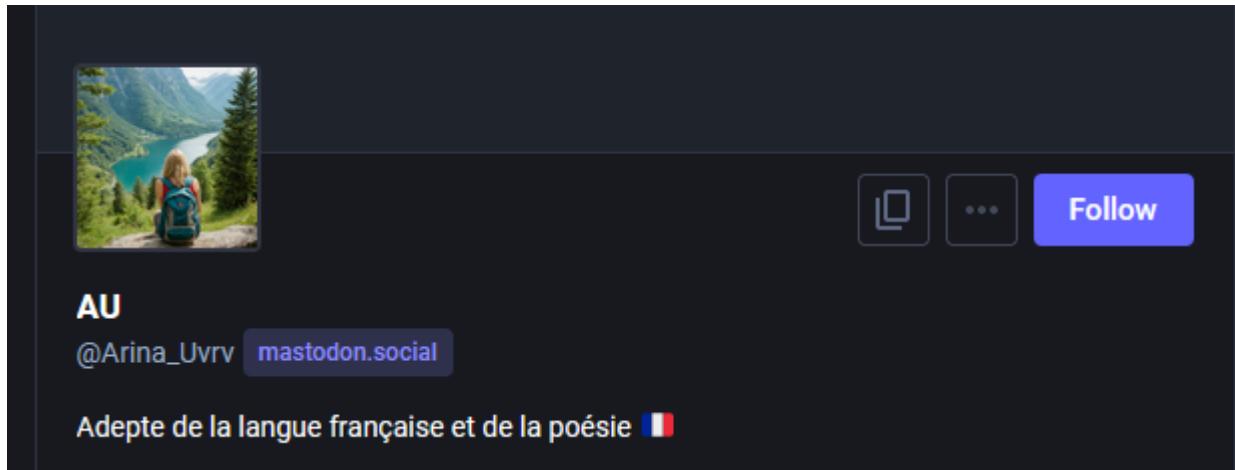


This screenshot shows the Mastodon hashtag page for #au. At the top left is a back arrow and the text "au". In the center, the hashtag "#au" is displayed in large white text. To the right is a blue button labeled "Follow hashtag". Below this, the text "68 posts · 10 participants · 5 posts today" is shown. The background features a dark theme with some decorative icons.

Puis, en faisant défiler la page, nous trouvons des poèmes semblables à ceux que nous avons découverts sur les factures.

This screenshot displays three consecutive Mastodon posts from a user named AU. Each post includes a profile picture of a person in a green jacket and blue pants standing in a forest. The first post, dated April 16, contains the quote: "Chaque épreuve est un fil sur le métier à tisser de notre caractère." The second post, also dated April 16, contains the quote: "Les étoiles brillent pour tous, mais c'est à chacun de choisir son étoile à suivre." The third post, dated April 16, contains the quote: "L'avenir est une porte, le passé en est la clé." Each post has two tags: "#citation" and "#AU". Below each post are standard Mastodon interaction icons: a reply arrow, a retweet arrow, a star, a bookmark, and a more options menu.

Note : Initialement, le pivot de ce challenge résidait sur les citations, mais hélas, elles ne ressortent pas systématiquement. Ainsi, le pivot se reposait sur le #AU, bien que cela soit indépendant de notre volonté, nous avons tenu à vous aiguiller au maximum afin que vous puissiez vous débloquer et continuer le CTF !



En cliquant sur le profil nous trouvons un premier pseudo : [Arina_Urv](#)

Nous pouvons valider ce challenge.

FLAG : [Arina_Urv](#)

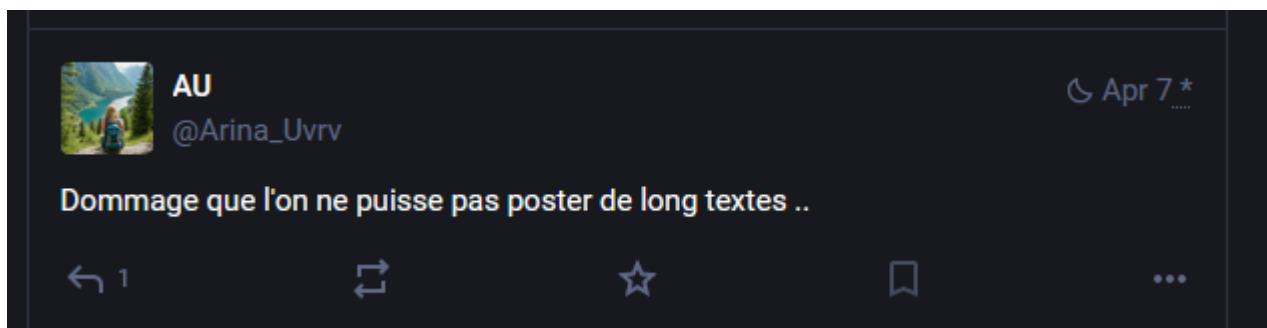
Challenge 25 : La traque financière

Au-delà des publications, vous êtes conscient de la menace qui pèse sur Stella Launch Solutions et le temps est compté. A partir de ce que vous trouvez, vous pouvez déduire une identité de la trésorière.

Quelle est la véritable identité de la trésorière ?

Format de Flag : Dupont Michelle

En analysant le compte Mastodon, au-delà de trouver des textes et citations, nous voyons un post intéressant qui exprime un regret de ne pas pouvoir publier des textes plus longs. Est-ce un début de pivot pour nous orienter vers une autre plateforme où elle pourrait poster des messages et poèmes plus longs ?



En observant attentivement le post, nous pouvons remarquer une étoile qui n'apparaît pas sur les autres posts

En cliquant dessus, nous voyons que le post a été créé le 7 avril puis édité le même jour.

AU
@Arina_Uvrv@mastodon.social

Dommage que l'on ne puisse pas poster de long textes ..

Apr 07, 2024, 07:04 PM · 🌙 · Web

Last edited **Apr 07, 07:04 PM**

0 bo Edited 1 time

Arina_Uvrv edited Apr 7

Arina_Uvrv created Apr 7

En remontant le fil des éditions et créations, nous pouvons observer à quoi ressemblait le post lors de sa création.

Arina_Uvrv created Apr 7

Dommage que l'on ne puisse pas poster de long textes .. RDV sur Tumblr !

@a--uvarova 😊

Nous avons à présent notre pivot ! En nous rendant donc sur Tumblr, nous découvrons l'identité de notre trésorière, qui s'appelle donc **Arina UVAROVA**

Arina Uvarova
@a--uvarova
Ajouter des badges

Nous pouvons donc valider le challenge.

FLAG : **Uvarova Arina**

Challenge 26 : Sous le ciel d'adieu

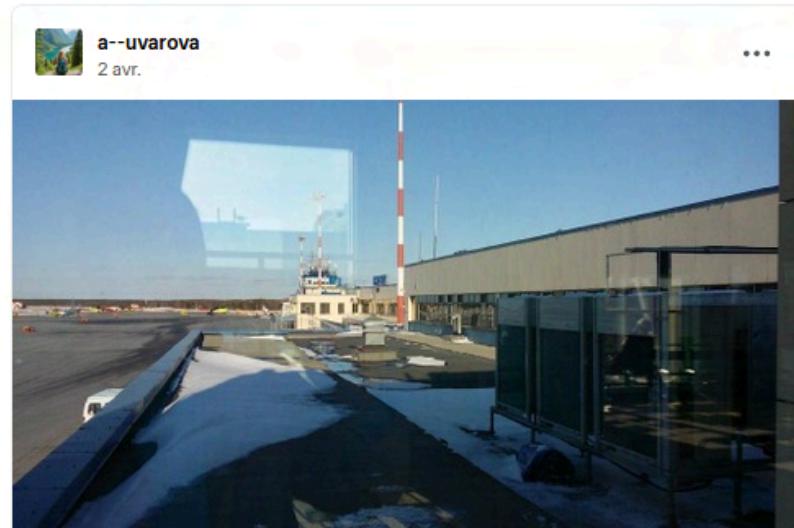
En découvrant ce nouveau profil, vous notez une publication intéressante qui laisse entendre que notre trésorière quitte sa terre natale pour une autre destination.

Quel est le code OACI de l'aéroport de départ ?

Format de Flag : LFPG

Avant toute chose, nous devons savoir ce qu'est un code OACI. Selon Wikipédia, « le code d'aéroport ou indicateur de localisation de l'OACI est un code à quatre lettres désignant les aérodromes du monde entier ».

En parcourant son profil Tumblr, nous trouvons un post faisant référence à un départ, avec une image montrant un aéroport. Il s'agit donc de savoir où ce dernier se situe !



a--uvarova
2 avr.

...

Sous le ciel d'adieu, mes pas vers l'avant se hâtent,
Vers l'aéroport, où mon cœur autrefois battait.
Bagages en main, un soupir dans l'air froid,
Je laisse derrière moi ce que je ne retrouverai pas.

La voix annonce mon vol, c'est l'heure de partir,
Vers des terres lointaines, sans jamais revenir.
Chaque pas sur le tarmac est un adieu silencieux,
À ce pays, mon passé, sous un ciel moins bleu.

La montée dans l'avion, un dernier regard jeté,
Sur cette terre natale, à jamais éloignée.
Les nuages défilent, emportant mes souvenirs,
Dans ce voyage sans fin, où je dois m'épanouir.

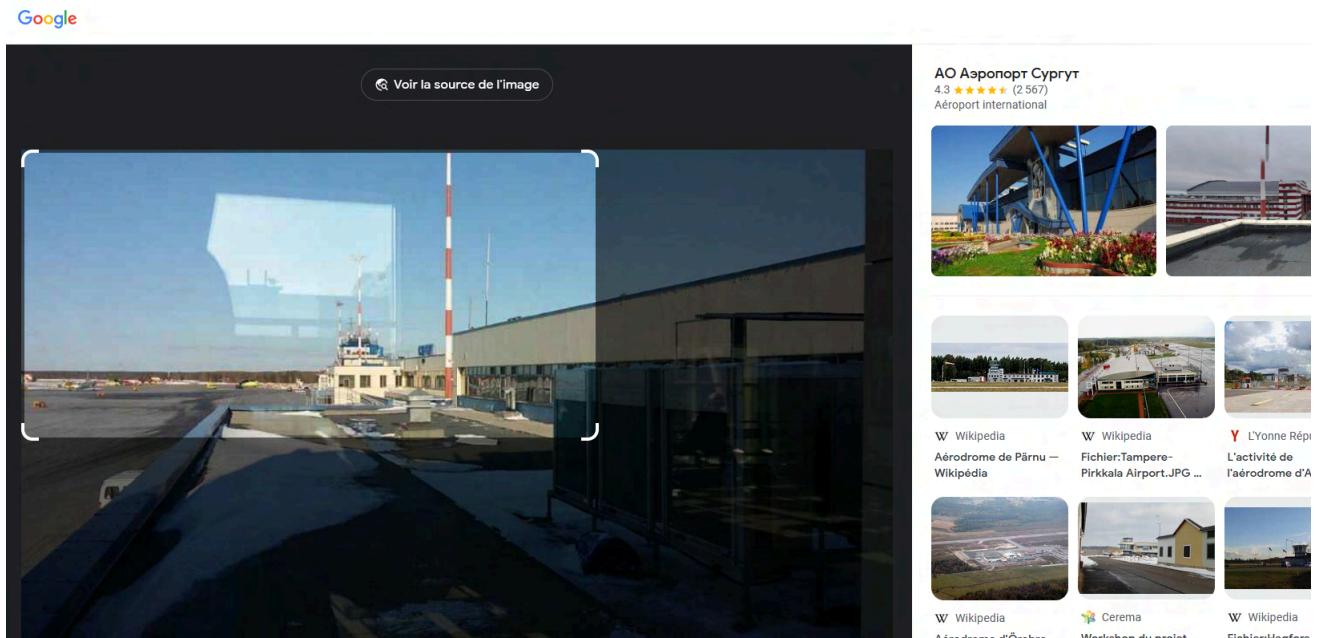
Nouvel horizon, promesse d'un recommencement,
Où chaque aurore sera le début d'un printemps.
Mais dans mon cœur, une larme de nostalgie,
Pour ce pays lointain, où mon âme fut bâtie.

#AU

Nous commençons donc par faire une recherche d'image inversée via Google



Images. En ajustant la zone de recherche, celle-ci nous donne immédiatement le nom d'un aéroport en Russie.



En effectuant des recherches complémentaires sur cet aéroport et en comparant avec les différents marqueurs de l'image, nous pouvons confirmer qu'il s'agit bien de l'« АО Аэропорт Сургут ».





De son code OACI : **USRR**

Международный аэропорт Сургут имени Ф. К. Салманова^[2] (IATA: **SGC**, ICAO: **USRR**) — международный Уральском Федеральном округе [России](#). Обслуживает как сам Сургут, так прилежащие к нему районы Ханты-Имеет статус аэропорта федерального значения^[3] с аэродромом класса «Б».^[4]

Nous pouvons donc valider le challenge.

FLAG : **USRR**

Challenge 27 : Un bon bol d'air

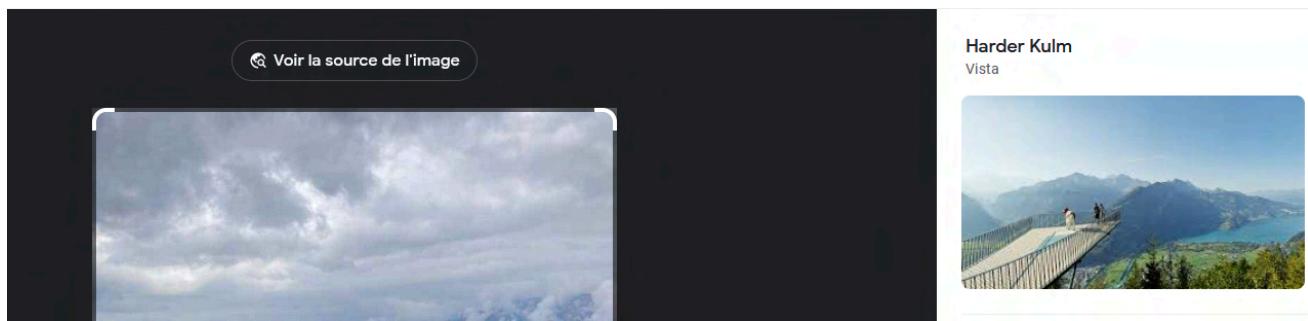
Vous avez désormais découvert un aspect de cette personne qui semble aimer partager des moments de sa vie.

Quel est le nom de la ville où la photo a été prise le 4 avril 2024, celle montrant un lac ?

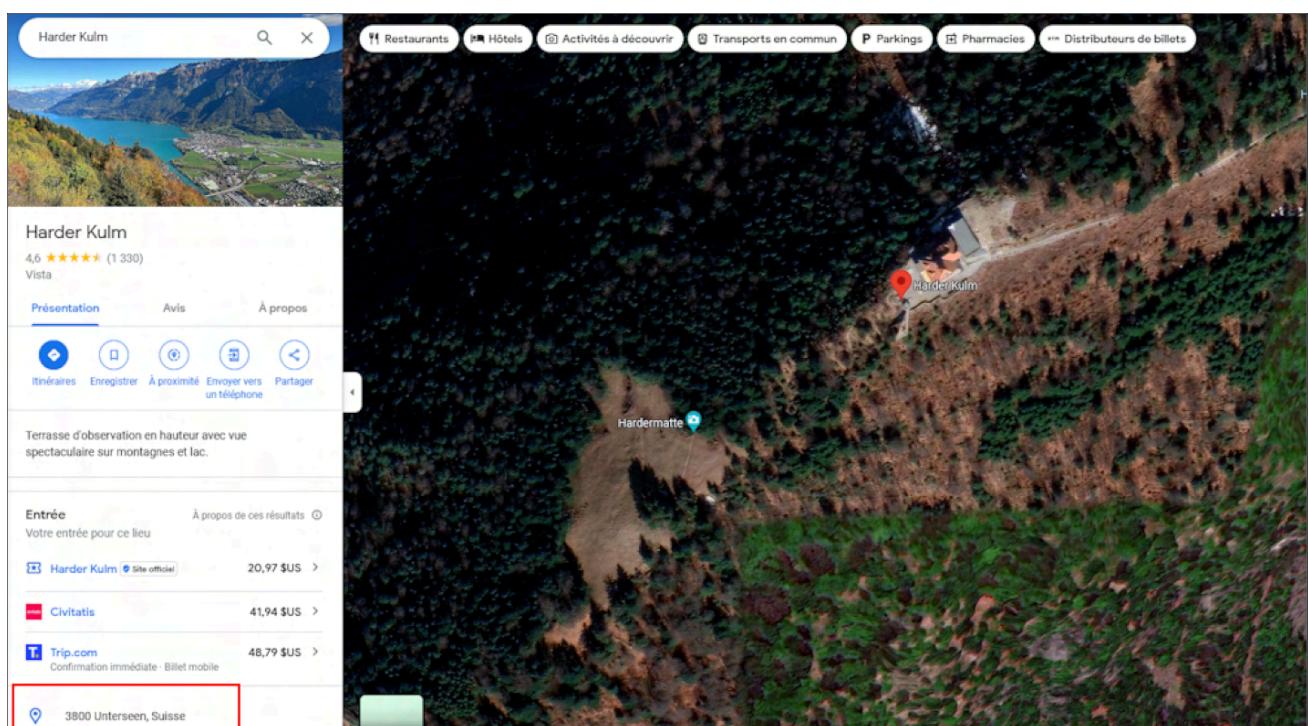
Format de Flag : Paris

En reprenant la photo, nous allons tenter de trouver le lieu précis en débutant par une recherche inversée.





En effectuant la recherche inversée, nous obtenons directement sur un résultat. Puis, en recherchant sur Google Maps, nous trouvons directement la ville : 3800 **Unterseen**, Suisse



Nous pouvons donc valider le challenge.

FLAG : **Unterseen**

Challenge 28 : Mise au point

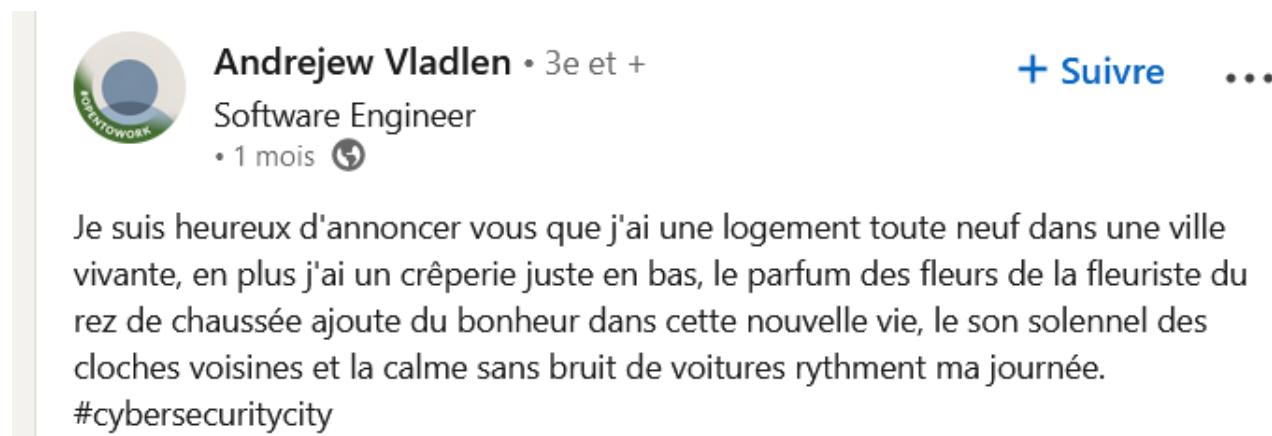
Vous décidez d'accélérer l'enquête. Pourquoi ne pas interroger un de nos suspects ? Ils est probablement plus proche que vous ne le pensez...

Où habite Andrijew Vladlen ?

Format de Flag : 36 quai des Orfèvres, 75001 Paris

En reprenant nos éléments, nous supposons qu'Andrijew est en France (au vu de son profil LinkedIn), et la trésorière en Suisse. Cependant, nous ne connaissons pas l'emplacement de Ch'ien Wen et de K4m3n3v. Ainsi, nous allons tenter de retrouver l'adresse exacte d'Andrijew.

Nous reprenons à partir de la publication sur LinkedIn.



LinkedIn profile of Andrijew Vladlen:

Andrijew Vladlen • 3e et +
Software Engineer
• 1 mois

+ Suivre ...

Je suis heureux d'annoncer vous que j'ai une logement toute neuf dans une ville vivante, en plus j'ai un crêperie juste en bas, le parfum des fleurs de la fleuriste du rez de chaussée ajoute du bonheur dans cette nouvelle vie, le son solennel des cloches voisines et la calme sans bruit de voitures rythment ma journée.
#cybersecuritycity

Nous allons maintenant identifier les différents marqueurs, à savoir 'en jaune) :





Andrejew Vladlen • 3e et +
Software Engineer
• 1 mois

+ Suivre ...

Je suis heureux d'annoncer vous que j'ai une logement toute neuf dans une ville vivante, en plus j'ai un crêperie juste en bas, le parfum des fleurs de la fleuriste du rez de chaussée ajoute du bonheur dans cette nouvelle vie, le son solennel des cloches voisines et la calme sans bruit de voitures rythment ma journée.
#cybersecuritycity

Avant de commencer à chercher, il faut définir notre périmètre. Nous savons qu'Andrejew est en France, mais où exactement ? À travers son post, il nous livre un indice : #cybersecuritycity. En faisant une rapide recherche, nous tombons directement sur un résultat.



Google ville de la cybersécurité en france

Tous Images Actualités Vidéos Livres Plus Outils

Rennes, une implantation historique de la cybersécurité
La métropole rennaise possède actuellement 76 entreprises de cybersécurité privées, notamment Thalès et Orange Cyberdéfense, mais aussi des petites start-ups.

Campus des écoles https://www.campus-des-ecoles.fr, design-digital, renn... Rennes, pôle de la cybersécurité en France

À propos des extraits optimisés Commentaires

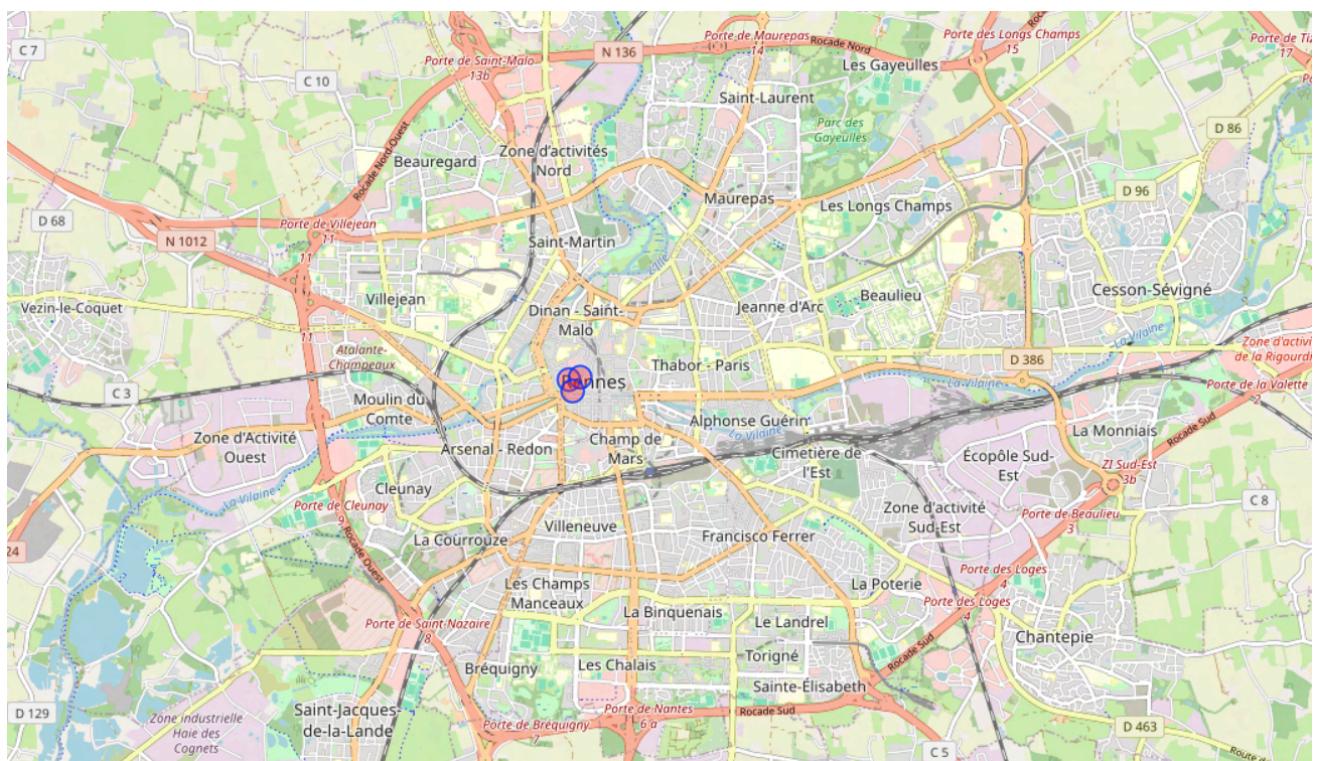
Cela colle bien, étant donné que Rennes se situe en Bretagne, et que la spécialité de la Bretagne, ce sont bien les crêpes !

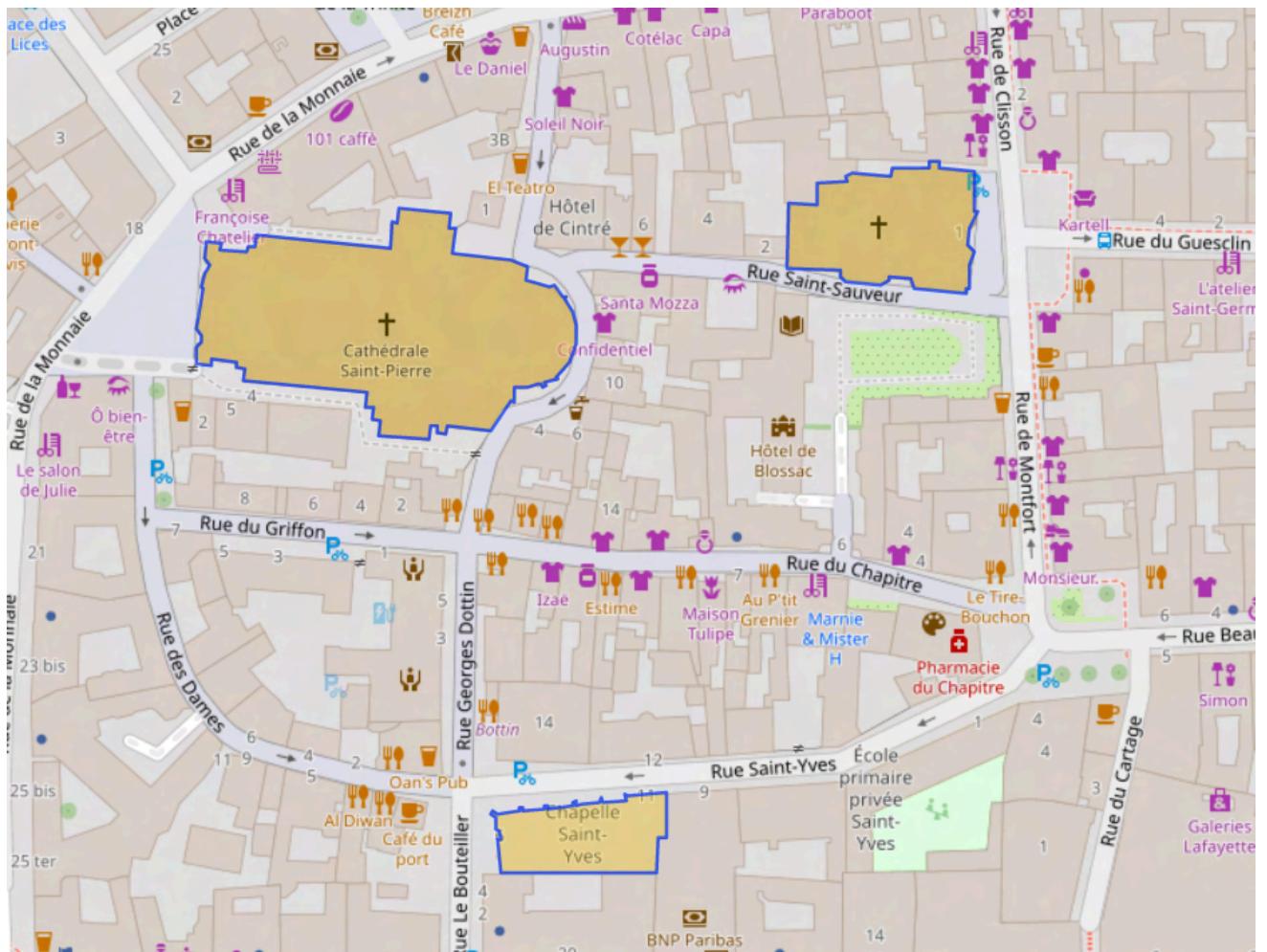
Autrement dit, nous cherchons une adresse à Rennes, à proximité immédiate d'une crêperie ainsi que d'un fleuriste. À proximité, il devrait également y avoir une église ou une cathédrale, comme le laisse sous-entendre sa mention du son solennel de cloches voisines. Enfin, la rue devrait être piétonne, étant donné qu'il mentionne l'absence de bruit de voiture.

Pour rechercher plus efficacement, nous allons utiliser l'outil OverPass Turbo, qui, à travers des requêtes scriptées, nous permet d'obtenir des résultats précis sur OpenStreetMap.



Nous obtenons donc ce résultat :



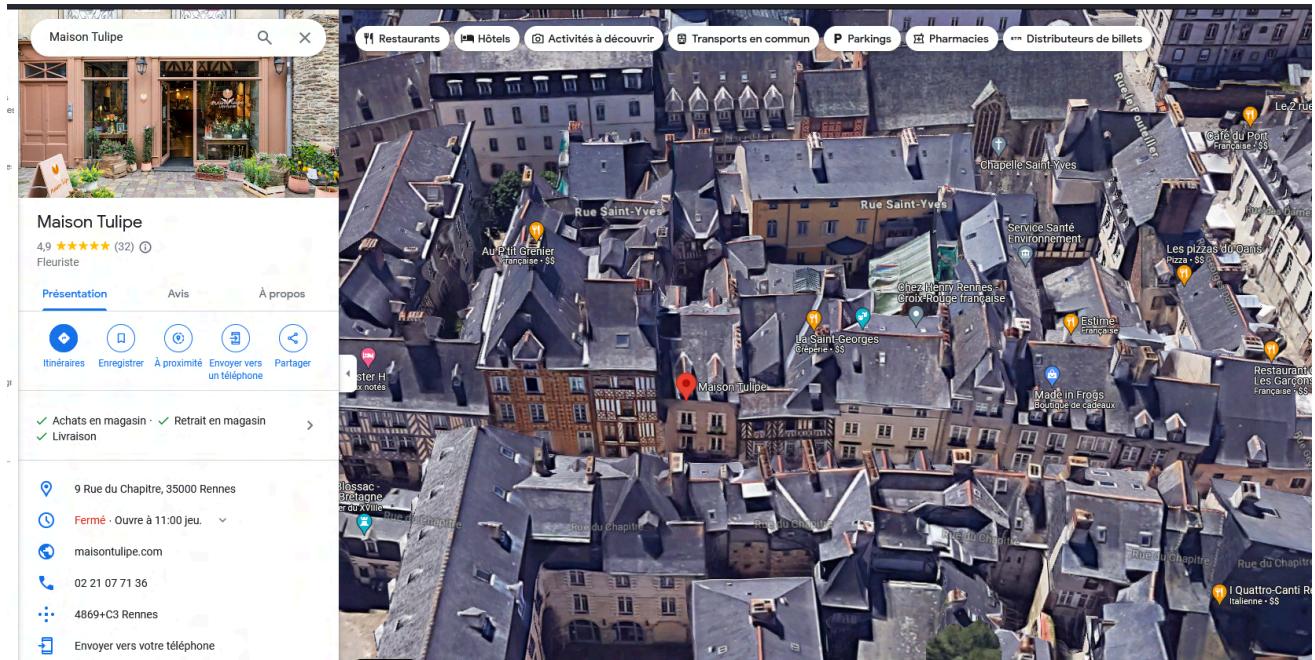


En nous projetant sur Google Maps au niveau de la crêperie (marqué comme restaurant) et du fleuriste (Maison Tulipe), nous voyons bien le restaurant, mais pas de fleuriste.



Cependant, attention, car cette vue StreetView date en réalité de juillet 2013 !

En prenant un peu de hauteur, nous voyons bien qu'il existe un fleuriste.



Nous pouvons donc en déduire que son adresse est le **9 rue du Chapitre, 35000 Rennes**

Nous pouvons valider le challenge.

FLAG : 9 rue du Chapitre, 35000 Rennes

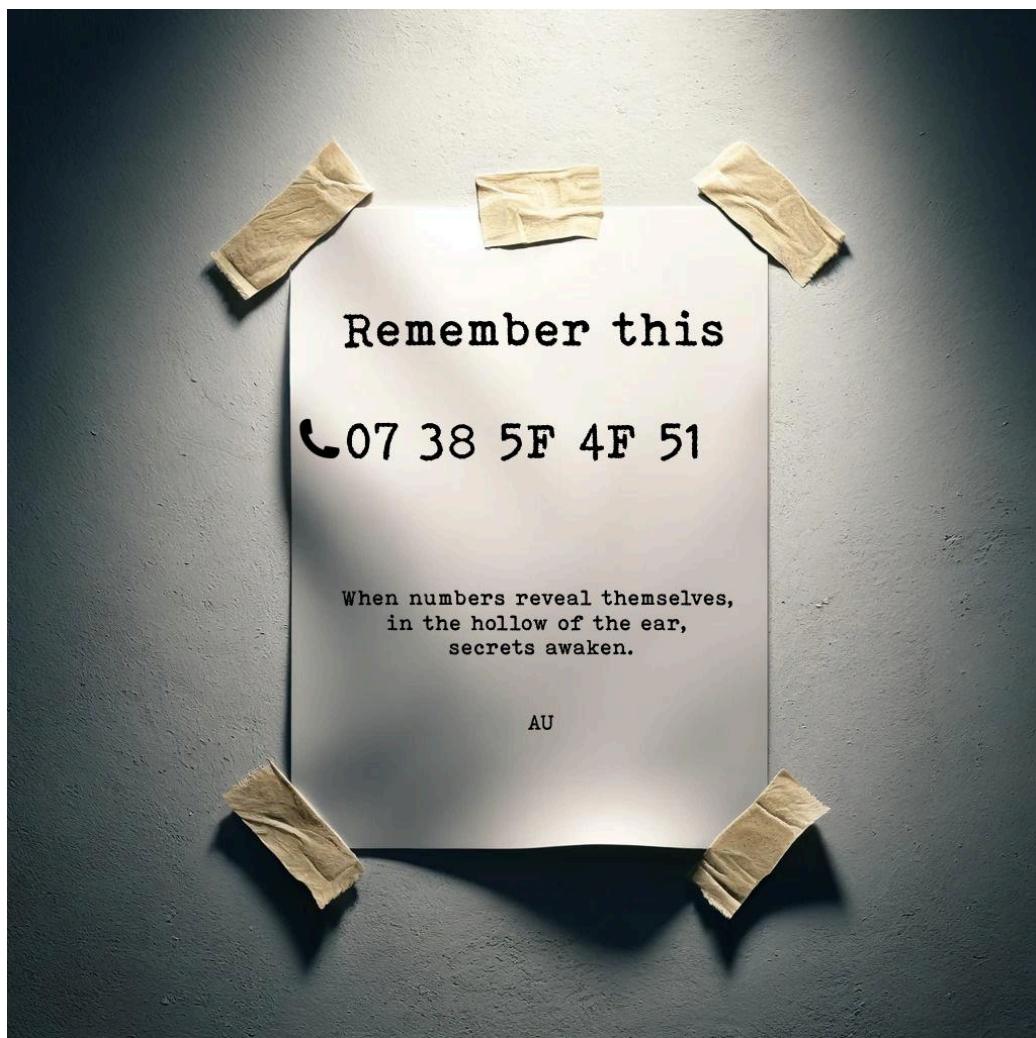


Challenge 29 : 6h00

Tôt ce matin, les unités d'intervention ont enfoncé la porte du domicile d'Andrejew. Ce dernier, surpris et choqué par un tel déploiement de force alors qu'il était derrière son ordinateur, se rend sans résister. Rapidement mis en garde à vue, il commence à parler, mais vous ne parvenez pas à obtenir les informations souhaitées. En effectuant la perquisition vous trouvez une feuille accrochée au mur qui attire votre attention.

Quel est le premier lien que vous découvrez ?

Format de Flag : <https://google.com/ABCD123>



En analysant ce poème nous trouvons tout d'abord ce qui s'apparente être un numéro de téléphone encodé en hexadécimal, puis un poème signé par notre trésorière nous laisse penser qu'il faille appeler ce numéro pour avoir des renseignements supplémentaires. Nous allons donc utiliser CyberChef afin de décoder le numéro, ce qui nous donne : **07 56 95 79 81**

The screenshot shows the CyberChef interface with a "From Hex" recipe and an "Input" field containing the hex values "07 38 5F 4F 51". The output is displayed in "To Decimal" format, resulting in the decimal values "7 56 95 79 81".

En contactant le numéro de téléphone, nous tombons sur la boîte vocale qui nous délivre un message en alphabet OTAN :
BRAVO, INDIA, TANGO, LIMA, YANKEE, 'SLASH', ALPHA, PAPA, JULIETTE,
DELTA, ROMEO, OSCAR, ZULU

Soit : BITLY/APJDROZ, nous pouvons donc en déduire le liens
<https://bit.ly/APJDROZ>

Nous pouvons donc valider le challenge

FLAG : <https://bit.ly/APJDROZ>



Challenge 30 : La dernière pièce du puzzle

Bingo ! Vous avez trouvé un drive chiffré très intéressant. Vous découvrez à présent l'unique pièce manquante de votre enquête.

Quelle est la véritable identité du chef de l'équipe ?

Format de Flag : *Mercier Albert*

En analysant avec attention le Proton Drive, nous trouvons une affiche de recherche émise par le FBI.



Nous retrouvons donc Andrejew, qui a depuis été arrêté, Arina la trésorière, et Ch'ien l'expert en aérospatial. Nous apprenons également la véritable identité de K4m3n3v, qui est marqué comme décédé, comme le montre l'article de presse. Zhirov était également impliqué dans des affaires de trafic d'armes et a été retrouvé sans vie, dans sa voiture immergée dans un lac.

НЕЗАВИСИМАЯ

SINE IRA
№ 46-4
ПЯТНИЦА
СУББОТА
2020 ГОД
ВЫХОДИТ
1990 ГОД
ПОДПИСЬ
50089, 10

ГАЗЕТА 16+

	ПОЛИТИКА Еще одна роль для присяжных Сферу юрисдикции заседателей предлагают расширить >> СТР. 3	В МИРЕ Евросоюз укрепит границу Греции Поток мигрантов Брюссель остановит жесткими методами >> СТР. 6	
ЭКОНОМИКА Эксбюро возьмут прямо на границе Вице-премьер Абрамченко рассказала, каким будет новый налог на импорт >> СТР. 4	В СТРАНАХ СНГ Белорусская оппозиция раскололась до начала выборов Противники Лукашенко не верят в свою победу >> СТР. 5	АНТРАКТ Маэстро Спинози поздравит меломанок с 8 Марта >> СТР. 7	 COVID-19 опустошил мечети и стадионы В КНР военные помогают врачам, храм Рождества Христова в Вифлееме пуст >> СТР. 3, 5, 6, 8

Хакер, подозреваемый в причастности к террористической деятельности против Франции, найден мертвым

Анастасия Башкатова

В результате ужасающего поворота событий было подтверждено, что безжизненное тело, обнаруженное в отдаленном лесу, принадлежало преступному киберпреступнику, известному в глубинах цифрового преступного мира как K4m3n3v, по имени Тигран Зирев. Учитывая предполагаемые связи с хакерской группой, причастной к недавней террористической деятельности во Франции, смерть Тиграна поднимает тревожные вопросы о пересечении киберпреступности и терроризма.

Прежде чем заняться неизвестной кибердеятельностью, Тигран Зирев в значительной степени использовал свои навыки разработки программного обеспечения. Тем не менее, в конечном итоге он оказался втянутым в секретный мир незаконной деятельности, что привело его на опасный путь, где его техническими способностями манипулировали со злыми намерениями.



Тигран Зирев занимал видное положение в группе, известной как «колимабайт», с тайными операциями. Подозреваемый в организации запланированной атаки на Подозреваемый Зирево Франции. Тигран Зирев благодаря своим навыкам разработки вредоносного ПО сделал его стержнем гибких начинаний группировки. Недавние события, в том числе едва

предотвращенное нападение на спутник, принадлежащий StellaLaunch Solutions, известной фирме, занимающейся космическими технологиями, подчеркивают смелые амбиции группы.

Неудачная находка умершего человека была сделана в уединенном лесном уголке с большой осторожностью. Первоначальная находка произошла,

когда турист заметил автомобиль, частично затопленный в близлежащем озере в лесу. Это наблюдение побудило правоохранительные органы провести тщательное расследование, которое в конечном итоге привело к тревожному обнаружению затонувшего автомобиля и его содеримого. Транспортное средство, замаскированное под водой,

намекало на нераскрытые тайны под, казалось бы, спокойной гладью лесного озера.

Местные правоохранительные органы в настоящее время расследуют обстоятельства смерти Тиграна, но подробной информации общественности не предоставили. В заявлении департамента полиции подчеркивается серьезность ситуации и содержится призыв к тщательному расследованию событий, приведших к смерти Тиграна.

Новость о кончине Тиграна оказалась значительное влияние как внутри киберсообщества, так и среди правоохранительных органов. Службы об инциденте распространяются, особенно в России, где информация по-прежнему ограничена, что усиливает обеспокоенность международной безопасности, связанную с деятельностью киберпреступников. По мере того, как следователи работают над выяснением обстоятельств смерти Тиграна, связь между киберпреступностью и терроризмом становится все более очевидной в глобальном масштабе.

[>> СТР. 4](#)

article fictif dans le cadre d'une compétition CTF



APT HUNTER

Et enfin nous apprenons la véritable identité du chef, **GOLUBOV Sviatoslav**.

Nous pouvons valider le challenge

FLAG : **GOLUBOV Sviatoslav**



Challenge 31 : Lieu secret

Comme toute organisation, ils doivent nécessairement disposer d'un lieu pour mener leurs activités. Vous devez localiser cet endroit.

Quelles sont les coordonnées en latitude et longitude de leur planque ?

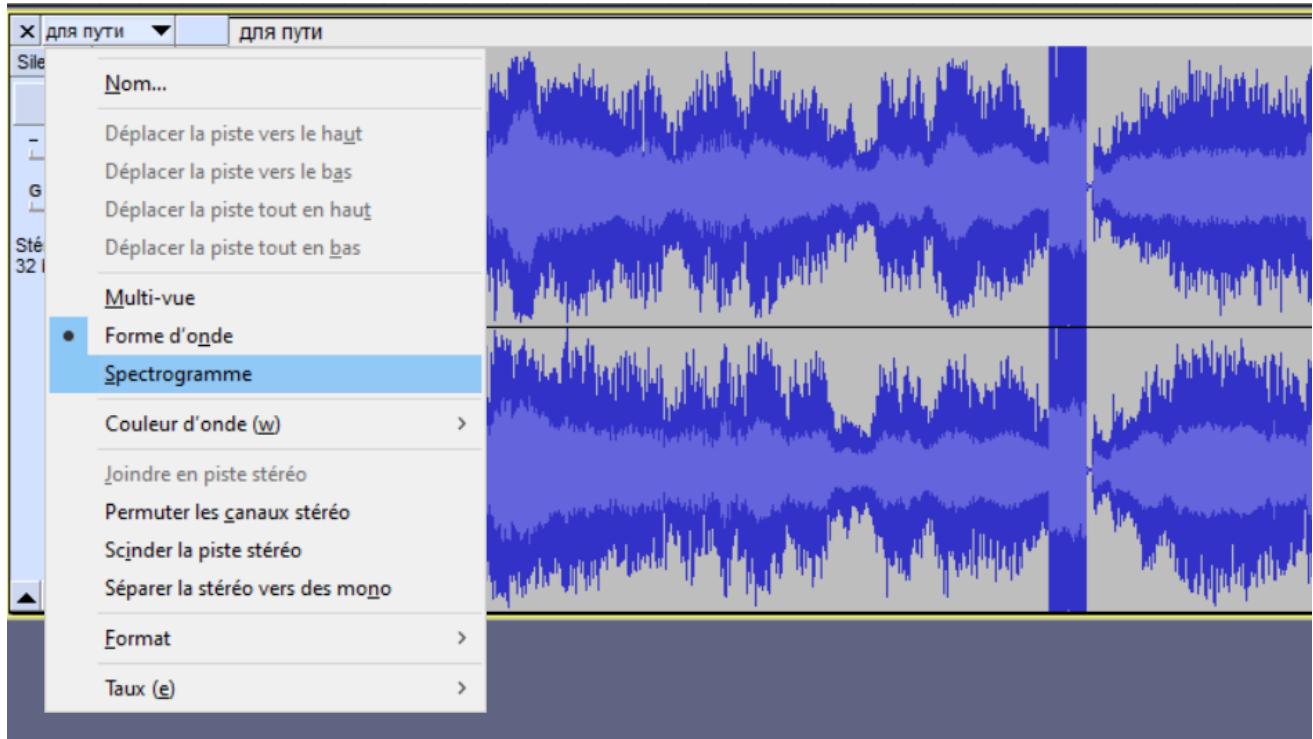
Format de Flag : 1.111, 2.222

En reprenant les différents éléments du drive, nous trouvons un fichier PDF d'une affiche de recherche du FBI, suivi d'un article de presse mentionnant le décès de K4m3n3v. Nous découvrons également une musique au format MP3 et un fichier texte en russe qui, une fois traduit, donne ceci :

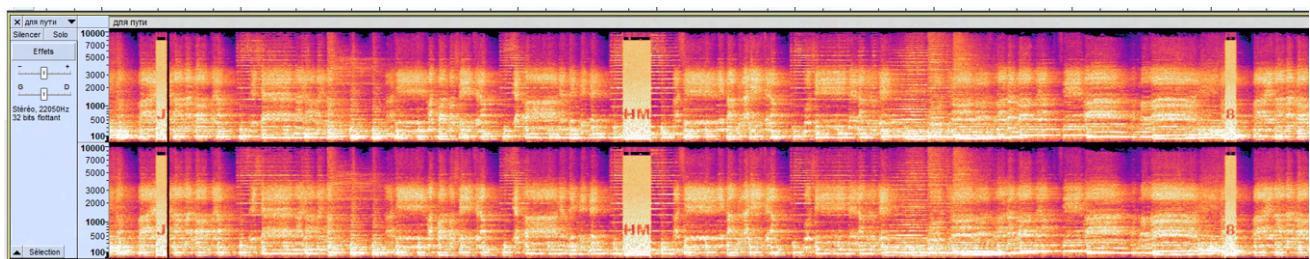
À la **s**ortie du **c**afé commence un voyage **v**ers l'**e**st,
Tu prendras la **v**oiture qui t'attend,
Passant près de la **r**éserve **M**uraveinik, un voyage sans **f**in.
Sans arrêts ni détours, il continue sur exactement **t**rente-sept **k**ilomètres,
Jusqu'à ce qu'un **n**ouveau **c**hemin s'ouvre sur la **d**roite.
Là, un **p**ont apparaît, au-dessus d'une **re vivante,
Reconnaissable à sa **be **rIl continue, emporté par le courant,
Tourne toujours à gauche, puis tout droit
Jusqu'à ce que tu passes là où les gens se reposent.
Non loin, une **é**glise, là tu pourras trouver
Монетка, appelle-moi quand tu seras là,
Au **détage**, nous t'attendrons,
Dans le bâtimen**t** où les **balcons rouges** scintillent.******

Il s'agit d'un poème qui dirige probablement son destinataire vers la cache du groupe. Nous surlignons donc les éléments importants. Cependant, nous ne savons pas où commencer notre quête, ni même où se situe le fameux « café » mentionné au début du poème.

En examinant plus en détail le ProtonDrive, nous avons utilisé tous les éléments sauf le fichier MP3. En l'écoulant, nous remarquons des coupures. Est-ce un message caché ? Nous décidons donc d'afficher le spectrogramme de la musique via Audacity.

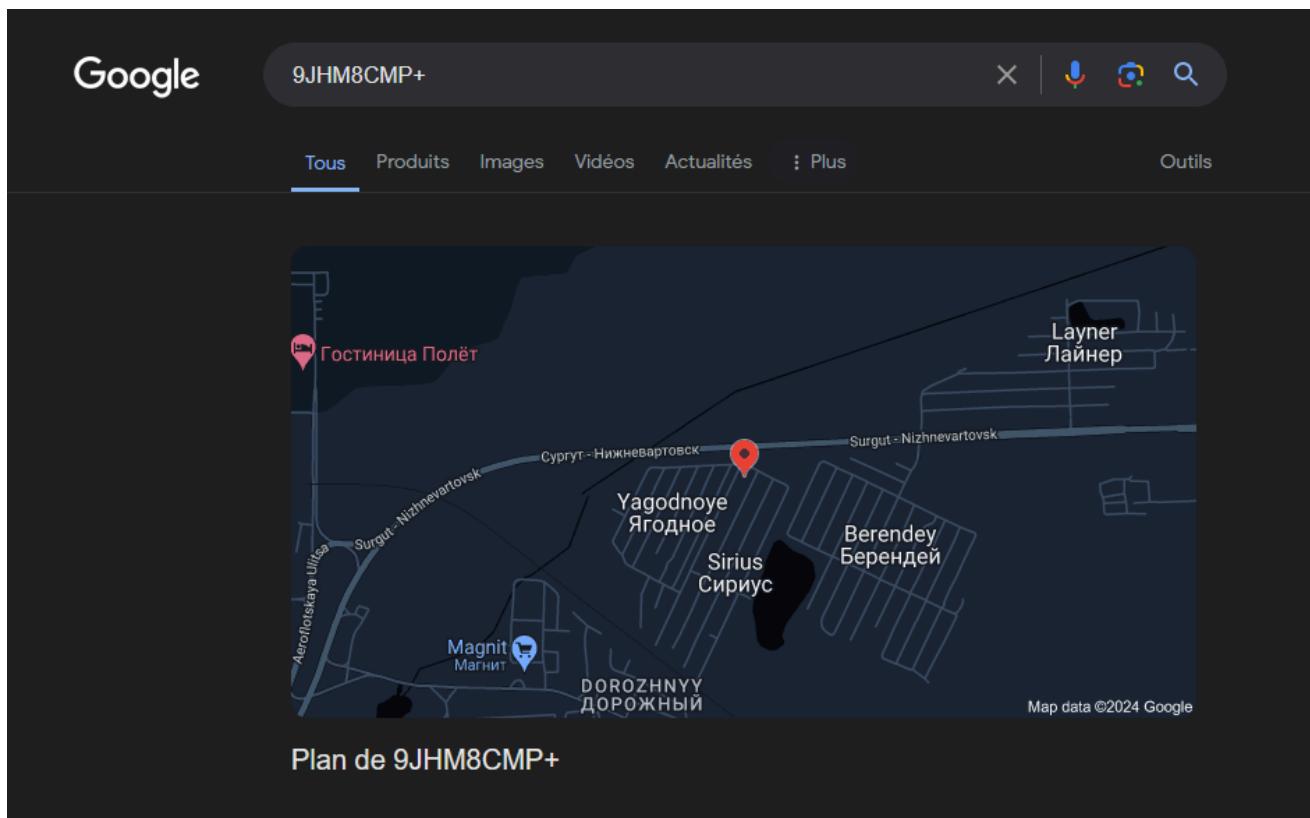


Et nous trouvons effectivement des lettres inscrites dans les différentes coupures.

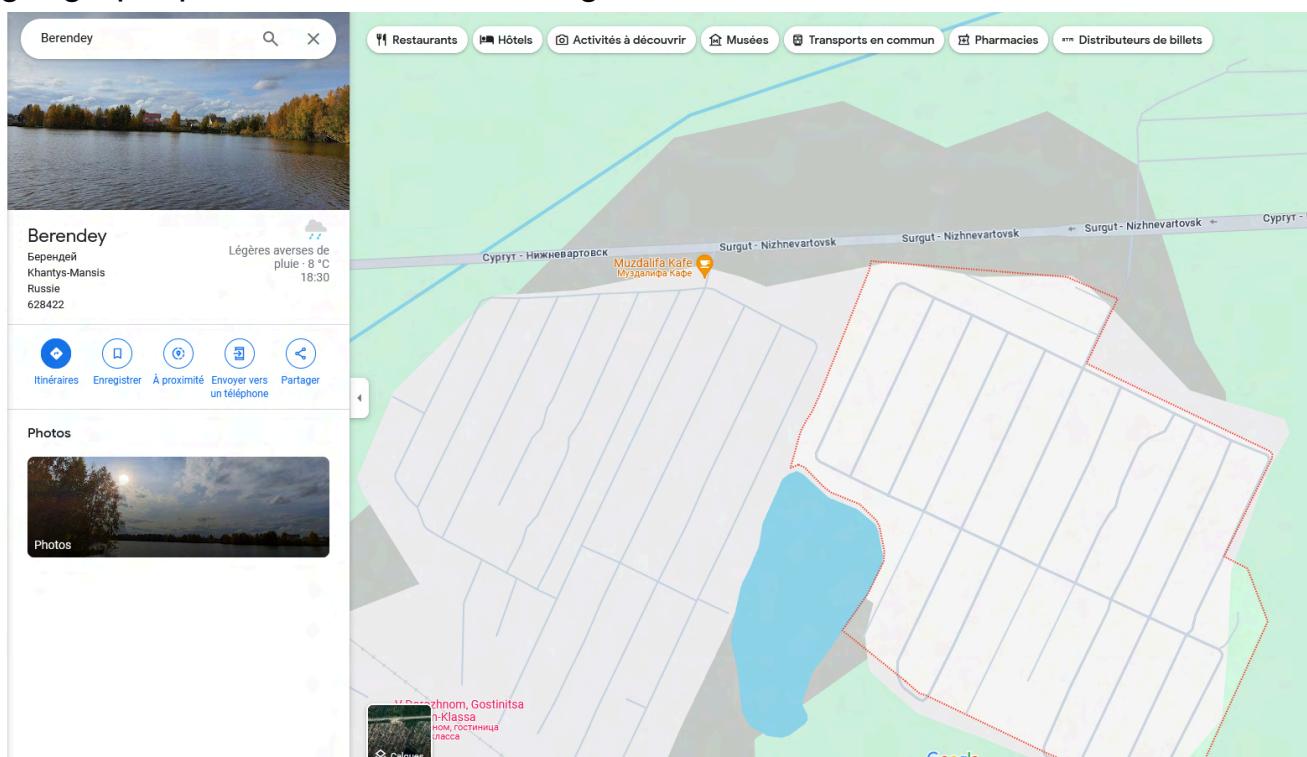


En mettant bout à bout nous trouvons le code suivant : **9JHM8CMP+**

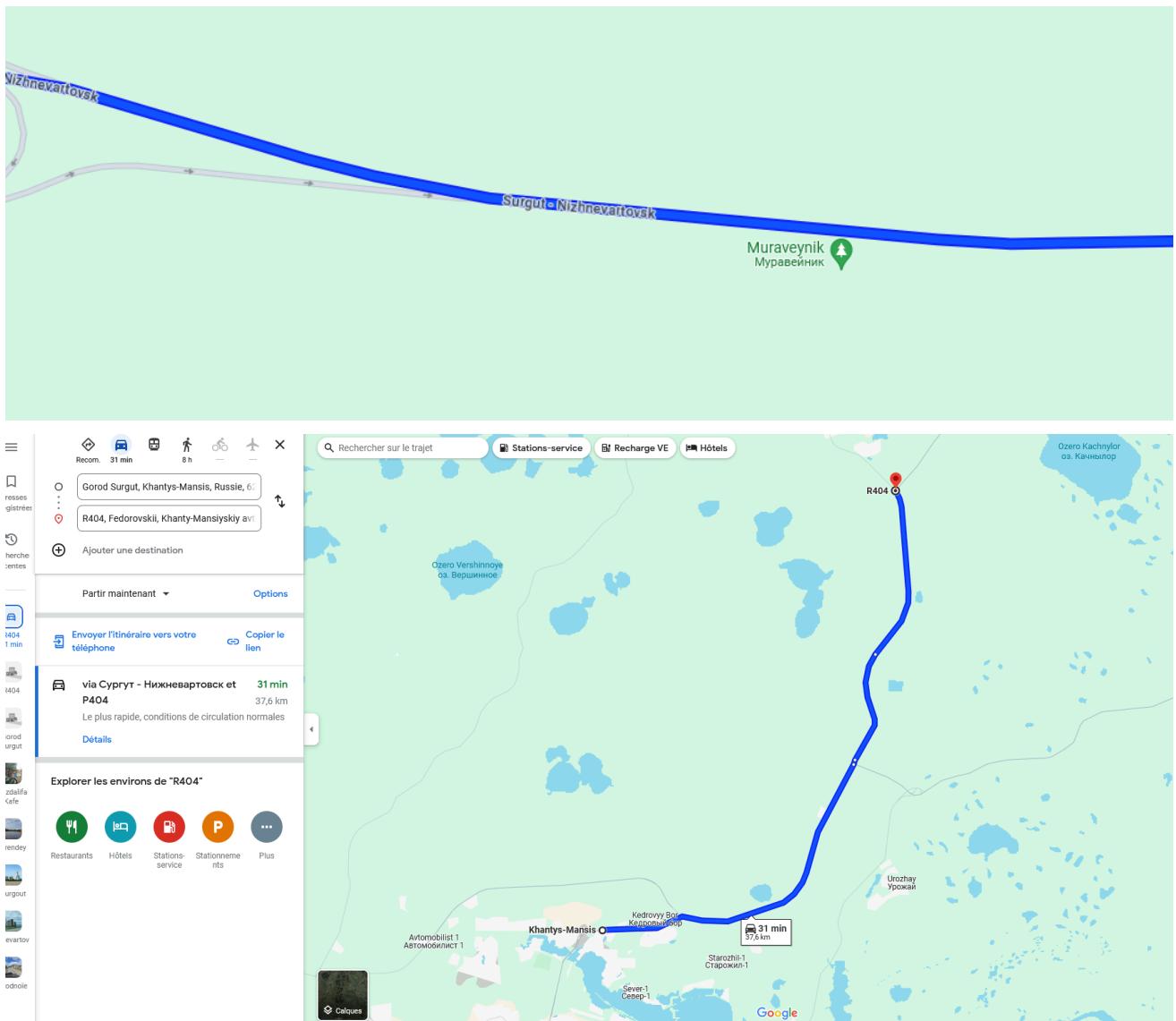
En renseignant ce résultat sur Google nous avons une localisation



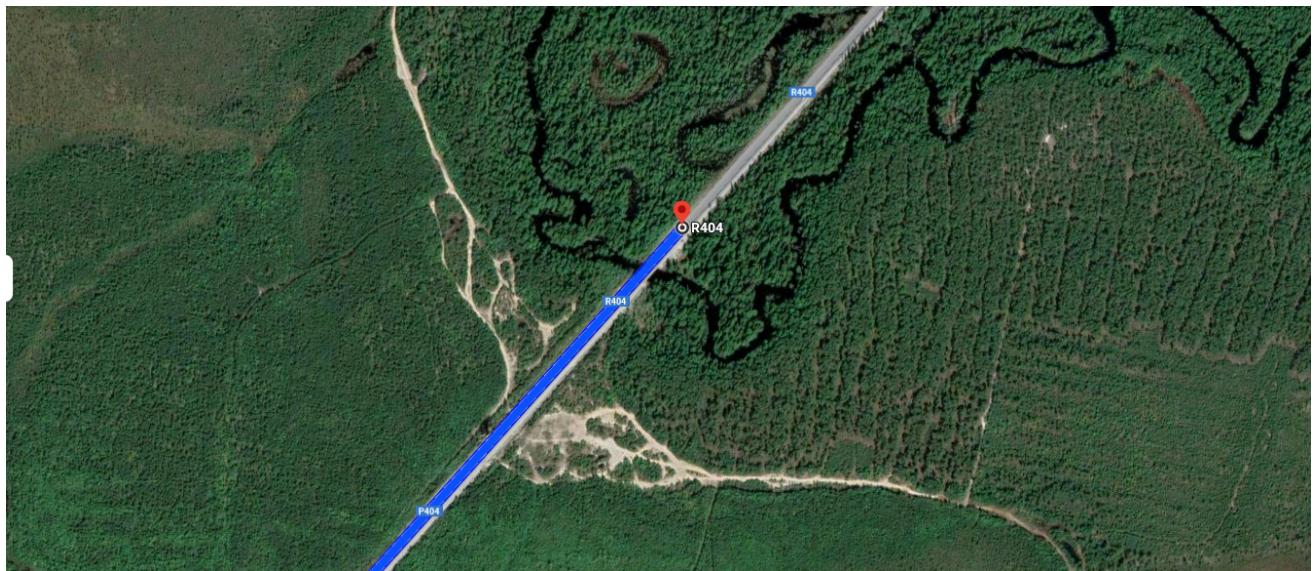
En cherchant sur Google Maps, nous confirmons qu'il s'agit de la bonne zone géographique et nous retrouvons également le café mentionné dans le texte.



Nous partons donc du “Муздалифа Кафе” et partons vers l’Est pendant 37km en passant devant la réserve naturelle de Muraveynik



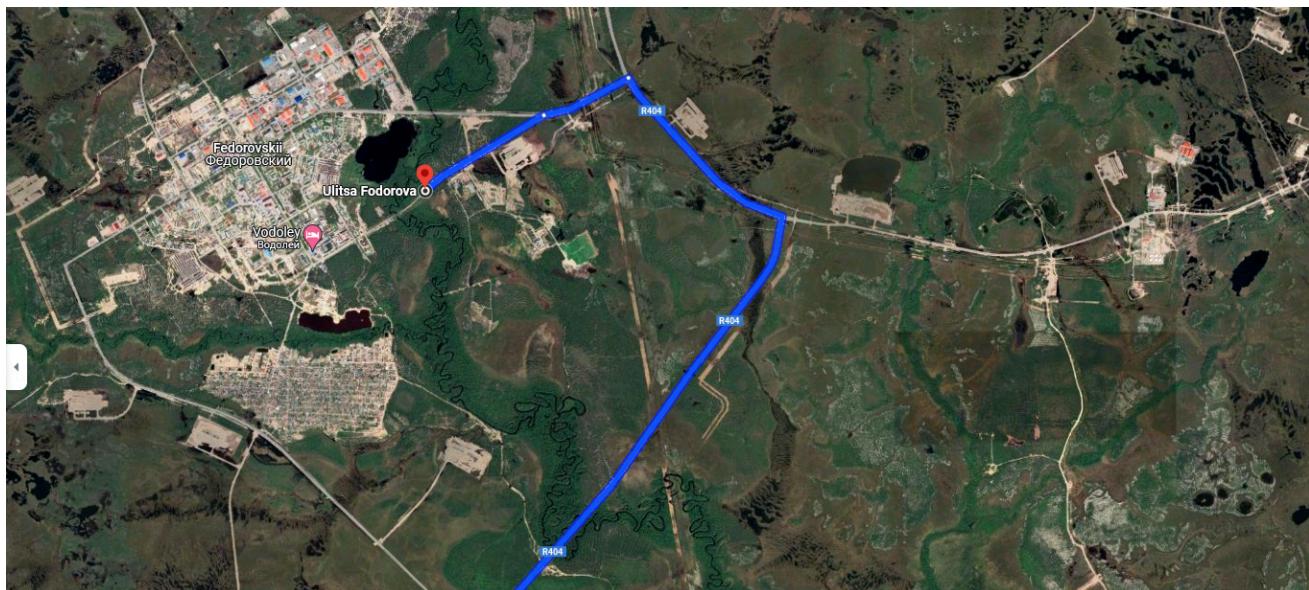
Ensuite nous tournons à droite et nous passons au dessus d'une rivière



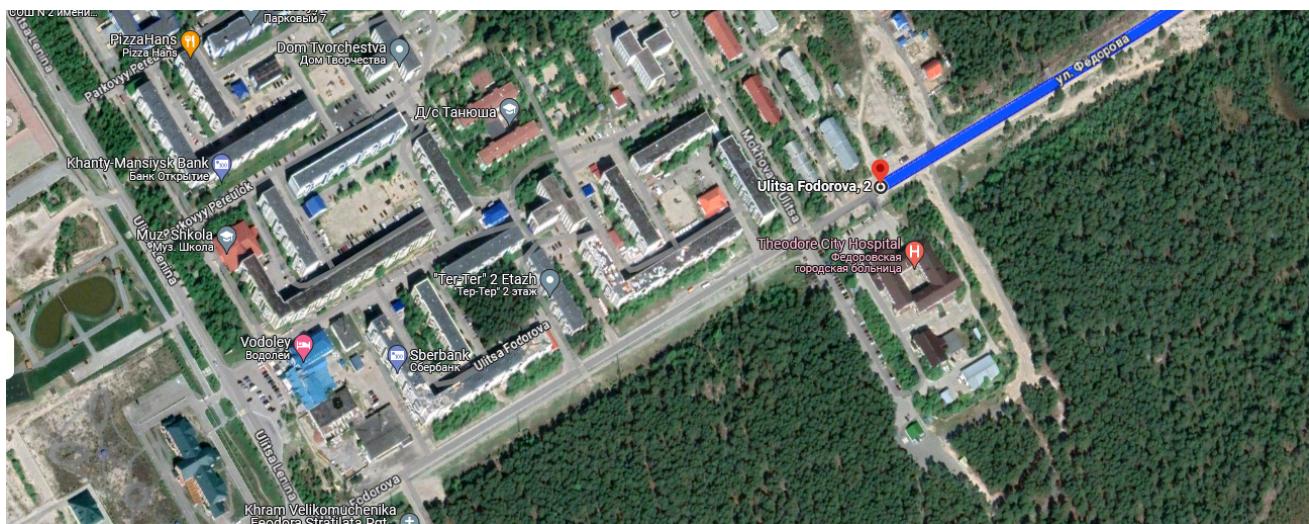
En nous mettant en StreetView nous voyons bien le pont de couleur rouge,



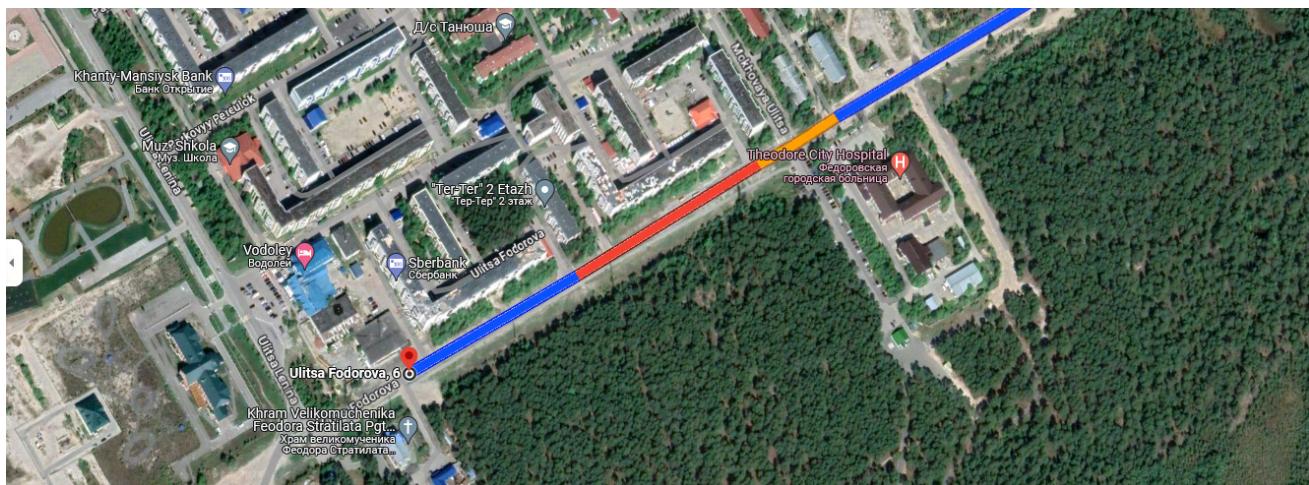
Ensuite, nous tournons toujours à gauche puis tout droit



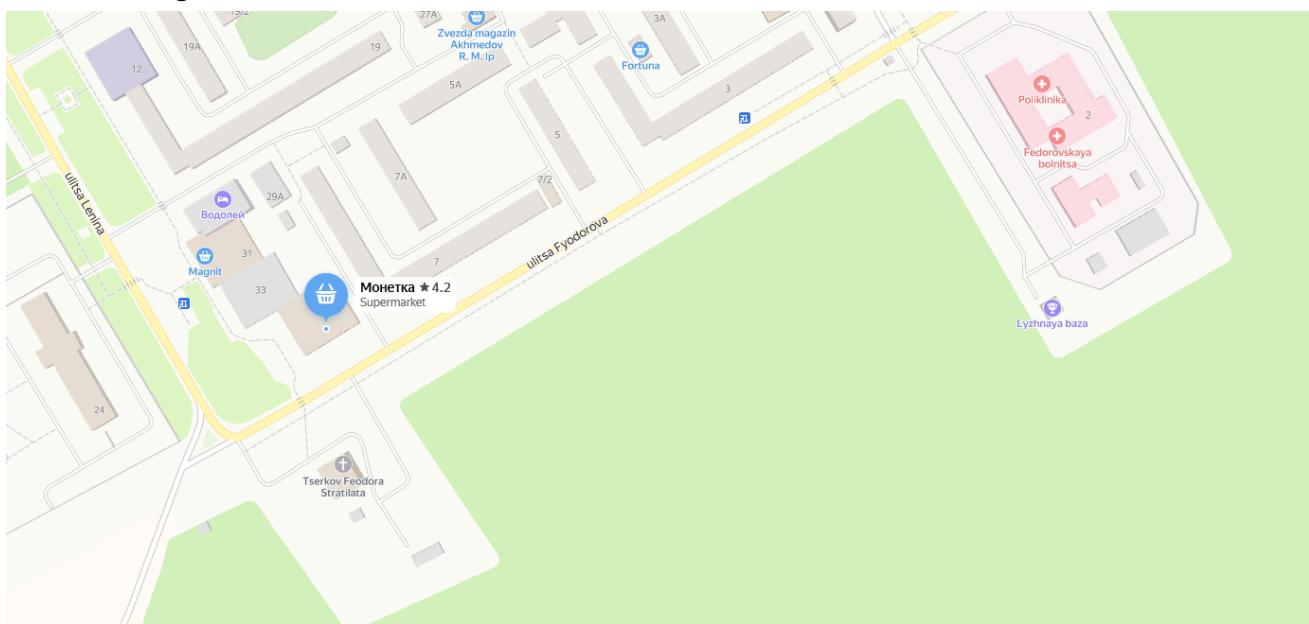
Nous entrons donc dans la ville de "Fedorovskii", puis nous trouvons le lieu où les gens se reposent, soit l'hôpital.



Nous tombons par la suite directement sur l'église, mais en face de cette dernière il n'y a pas de “Монетка” comme annoncé dans le texte.



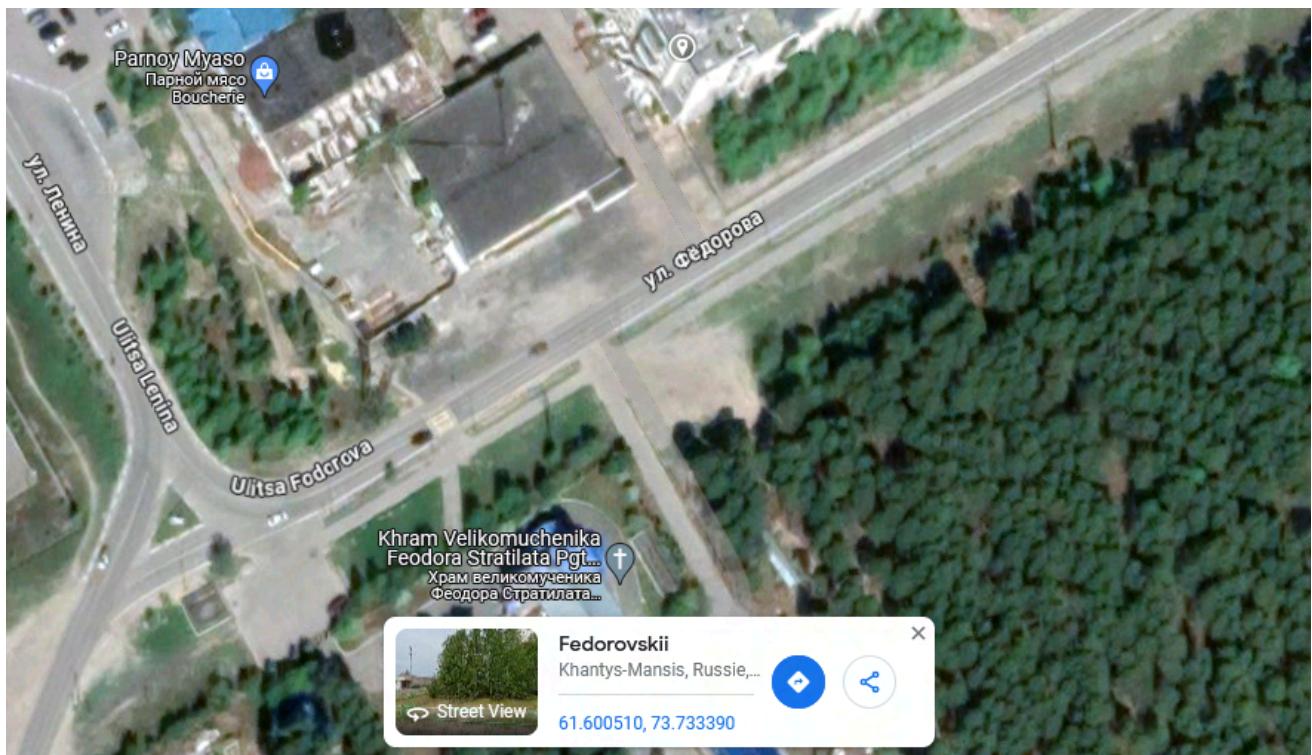
Cependant, n'oublions pas que Google est un service américain et que nous sommes en Russie. Ainsi, nous allons croiser nos sources avec Yandex Maps (Une sorte de Google Map russe) et nous voyons à présent le « Монетка » en face de l'église.



En utilisant Street View, nous voyons effectivement l'immeuble avec le balcon rouge au second étage.



En plaçant le curseur sur la carte, nous pouvons récupérer la latitude et la longitude.



Soit **61.600, 73.733**

Nous pouvons valider le challenge.

FLAG : 61.600, 73.733

Challenge 32 : Opération spéciale

Maintenant que la planque a été découverte, un agent des renseignements extérieurs français a réussi à s'y rendre. L'endroit étant assez isolé, cela n'a éveillé aucun soupçon. Lors de la fouille de l'appartement, il n'a trouvé que des ordinateurs déconnectés, des cartes mères brûlées et trouées, ainsi que des disques durs disparus. Parmi les documents éparpillés au sol, l'un d'eux lui a paru suspect, et il a réussi à nous l'envoyer.

Qui est le signataire du document ?

Format de Flag : Sp4rr0w

Dans ce challenge nous avons accès à une lettre que voici, traduite :

Mes chers amis,

Le jour où ce satellite entrera en collision avec notre ennemi commun entrera dans l'histoire, et nos noms seront à jamais gravés dans la mémoire collective. Je remercie chacun d'entre vous pour votre participation dévouée à ce projet. Je vais me retirer pour quelque temps dans un lieu secret que je préfère garder confidentiel. J'espère que vous utiliserez également ce temps pour vous.

Sans votre contribution et le soutien financier de nos partenaires, cette opération n'aurait jamais eu lieu.

Au revoir, et j'espère, à bientôt, L3n1n3

Note pour K4m3n3v, souviens-toi, si le satellite dévie de sa trajectoire prévue et menace notre patrie, utilise la clé d'arrêt pour tout interrompre, corrige l'orbite et relance le programme.

Si tu as oublié la clé : Dans le nom de celui qui a construit le mausolée du leader, réside la force pour arrêter la tempête.



N'oublie pas :

`oignon/4ec0ce6db63dd91893187c4c2348dc2c1008d6443014da4dab569e3e4
d724ceb/`

Au travers de cette lettre, nous obtenons plusieurs informations très intéressantes. Tout d'abord, nous avons le pseudonyme utilisé par le chef du groupe, **L3n1n3**. Ensuite, il est question d'une clé et d'un programme à arrêter si nécessaire, suivis d'une énigme concernant cette clé. Enfin, une chaîne de caractères oignon , accompagnée de ce qui semble être un hash SHA256. Nous y reviendrons plus en détail ultérieurement.

Nous pouvons valider le challenge.

FLAG : L3n1n3

Challenge 33 : Lieu secret

Parfait ! Il est temps de mettre un terme à cette machine infernale. Vous vous trouvez désormais devant votre ordinateur, le destin du satellite reposant entre vos mains. Il est l'heure de désactiver le malware !

Quel est le code de sortie une fois le malware désactivé ?

Format de Flag : 0x1234AB

En analysant les trois derniers paragraphes voici ce que nous pouvons en déduire :

Note pour K4m3n3v, souviens-toi, si le satellite dévie de sa trajectoire prévue et menace notre patrie, utilise la clé d'arrêt pour tout interrompre, corrige l'orbite et relance le programme.

Cette note laisse à penser qu'il doit y avoir un panneau de contrôle pour gérer un possible malware implémenté dans le satellite.



Si tu as oublié la clé : Dans le nom de celui qui a construit le mausolée du leader, réside la force pour arrêter la tempête.

Cette note laisse penser que la clé est la réponse à cette énigme. Si l'on prend en compte le pseudo du chef et la mention "leader", qui pourrait désigner la personne à l'origine du parti communiste, à savoir Vladimir Ilitch Lénine, une recherche sur Google nous permet d'identifier facilement le nom de la personne qui a construit le Mausolée.

Présentation	
Type	Mausolée
Partie de	Nécropole du mur du Kremlin 
Commémoré	Lénine 
Style	Éclectisme égyptien 
Architecte	Alekseï Viktorovitch Chtchoussov
Matériaux	granite, labradorite et porphyre 
Construction	1930

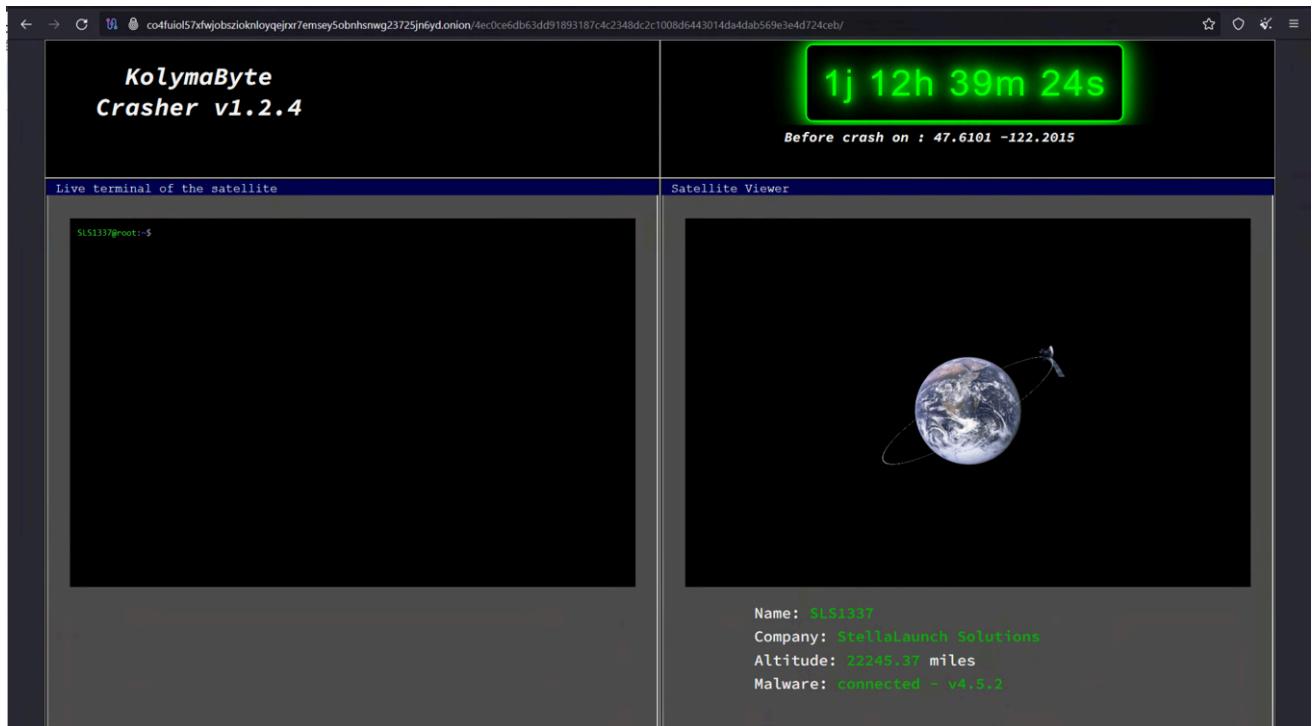
Soit **Chtchoussov**.

Enfin nous avons ce dernier paragraphe

N'oublie pas :

*oignon/4ec0ce6db63dd91893187c4c2348dc2c1008d6443014da4dab569e3e4
d724ceb/*

En analysant la structure, et notamment le mot « oignon » qui prend toute son importance, il pourrait s'agir d'un « path » d'un site. Sachant qu'il existe un site TOR de revente de données, nous pouvons essayer d'ajouter cette chaîne de caractères après le .onion.



Nous tombons effectivement sur une interface qui semble servir à contrôler le malware dans le satellite. En haut à droite, un compteur indique le moment où le satellite entrera en collision aux coordonnées 47.6101, -122.2015. En bas à gauche, un terminal semble avoir un accès root au satellite, et à droite, les spécifications du satellite, notamment son nom, la compagnie à laquelle il appartient, son altitude et la version du malware. Enfin, le must du must (car on a du budget) : une superbe animation du satellite en orbite autour de la Terre.

Mais pas de temps à perdre ! Penchons-nous sur le terminal et arrêtons ce processus dangereux !

En exécutant la commande *help*, nous identifions rapidement les commandes disponibles.

Live terminal of the satellite

```
SLS1337@root:~$ help
Available commands: help, cd, ls, resume-crash, stop-crash
SLS1337@root:~$
```

Parmi les commandes basiques, *resume-crash* et *stop-crash* nous intéressent particulièrement.

En entrant la commande `stop-crash`, celle-ci nous demande une clé.

```
SLS1337@root:~$ stop-crash  
Please use : stop-crash key  
SLS1337@root:~$
```

Nous pouvons tenter "Chtchoussey"

Et bingo ! nous avons un code de sortie : **0x95BF4A**

Et notre action a bien été effective, comme en témoigne la mention « Aborted » en haut à droite.





Nous pouvons valider le challenge.

FLAG : 0x95BF4A

Challenge 34 : Échec et mat

Vous tremblez encore, mais vous réalisez peu à peu l'ampleur de ce qui vient de se passer : vous avez neutralisé une grave menace et sauvé des vies !

Vous informez immédiatement StellaLaunch Solutions, qui a procédé à un nettoyage complet du satellite à distance.

Dans le même temps, vous apprenez l'arrestation par la police suisse de la trésorière, dont l'extradition vers la France est prévue dans les jours à venir pour un procès majeur. Toutefois, en raison des relations diplomatiques entre la France et la Russie, vous ne parvenez pas à appréhender le chef du groupe ni l'expert en aérospatial. Peut-être réapparaîtront-ils un jour ? Seul l'avenir le dira.

Les preuves que vous avez recueillies joueront un rôle crucial lors du procès. Bien que la victoire ait un goût amer, car vous n'avez pas réussi à capturer tous les coupables, vous pouvez à présent clôturer ce dossier.

Félicitations pour cette enquête !

Nous espérons que cette dernière vous aura plu ! Nous avons hâte de lire vos write-up et d'avoir vos retours ! A très bientôt je l'espère

Toute l'équipe de APT Hunter

*Flag : **finish***

C'est avec cette vidéo très bien réalisée que vous terminez le CTF ! Bravo à vous pour votre persévérance lors de cette enquête !

Nous pouvons valider le challenge.

FLAG : **finish**



Challenge bonus 1 : Une politique non respectée

En parcourant le terminal, vous trouvez une commande intrigante.

Quel est le mot de passe en clair du compte root ?

Format de Flag : mypassword987

En nous rendant sur le terminal du site StellaLaunch, nous voyons effectivement la commande extractpasswd, qui doit sûrement extraire les mots de passes administrateur.

```
bc29156d400a18991f6087c@debian:~$ help
Available commands: help, start2server, id, pwd, extractpasswd
bc29156d400a18991f6087c@debian:~$
```

En la lançant, nous voyons effectivement les mots de passe des comptes root et stellalaunchsolutions affichés, mais chiffrés.

```
bc29156d400a18991f6087c@debian:~$ extractpasswd
[i] Try to find /etc/shadow
[+] Credentials found !
[i] Gaining access...
.
.
.
[i] root : 240be518fabd2724ddb6f04eeb1da5967448d7e831c08c8fa822809f74c720a9
[i] stellalaunchsolutions : 008c70392e3abfb0fa47bbc2ed96aa99bd49e159727fcba0f2e6abeb3a9d601
```

En examinant la chaîne de caractères, nous constatons qu'il s'agit probablement d'un hash SHA-256, encore utilisé de nos jours pour sécuriser les mots de passe en les rendant illisibles. La particularité d'un hash est qu'il fonctionne à sens unique, ce qui signifie qu'il est très compliqué à craquer. Cependant, il existe des listes de hash associées à des chaînes de caractères (le plus souvent des mots de passe) qui permettent de faire une comparaison avec un hash donné. Ainsi, en allant sur le site CrackStation, nous trouvons très facilement le mot de passe.

The screenshot shows the CrackStation interface. At the top, it says "Free Password Hash Cracker". Below that, there's a text input field containing the hash: "240be518fabd2724db6f04eeb1da5967448d7e831c00c8fa822809f74c720a9". To the right of the input field is a reCAPTCHA checkbox labeled "Je ne suis pas un robot". Below the input field, it says "Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(shai_bin)), QubesV3.1BackupDefaults". Underneath the input field, there's a table with three columns: "Hash", "Type", and "Result". The first row in the table has a green background and shows "240be518fabd2724db6f04eeb1da5967448d7e831c00c8fa822809f74c720a9" in the Hash column, "sha256" in the Type column, and "admin123" in the Result column. Below the table, it says "Color Codes: Green Exact match, Yellow Partial match, Red Not found." and provides a link to "Download CrackStation's Wordlist".

Il s'agit d'un mot de passe, hélas plus que commun de nos jours ! **admin123**

Nous pouvons valider le challenge.

FLAG : **admin123**



Challenge bonus 2 : Altitude

En examinant ses photos, vous trouvez une publication qui semble avoir été capturée depuis une altitude très élevée.

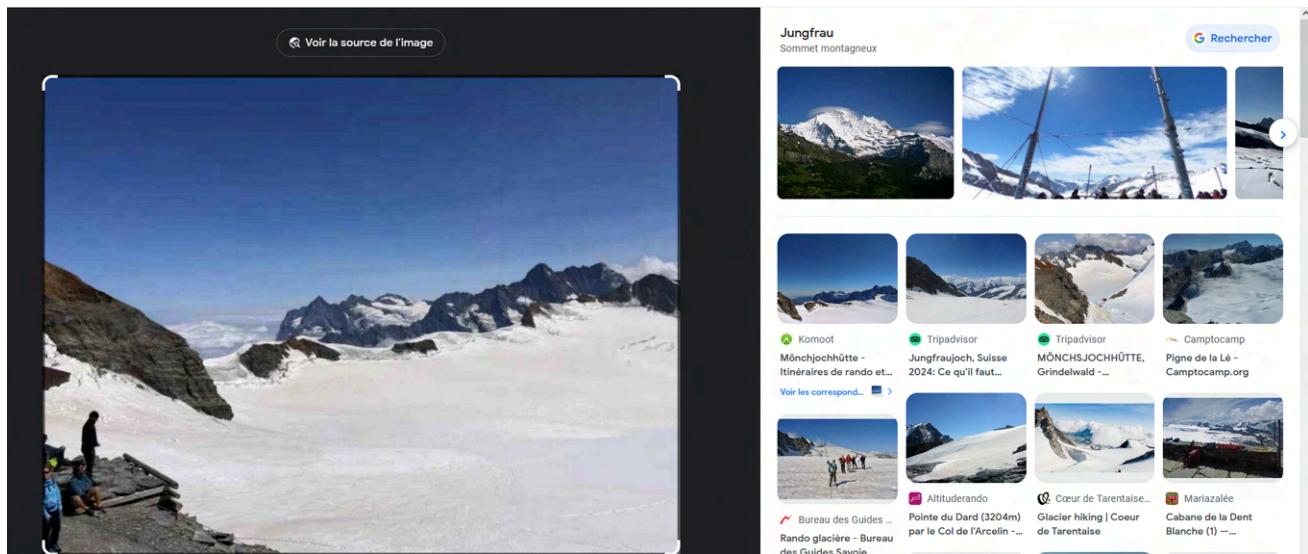
Quelles sont les coordonnées de latitude et longitude où la photo a été prise ? (une précision de trois chiffres après le point est attendue).

Format de Flag : 11.111, 2.222

En reprenant la photo disponible sur le compte Mastodon d'Arina, nous trouvons cette image qui semble en effet avoir été capturée depuis une très haute altitude.



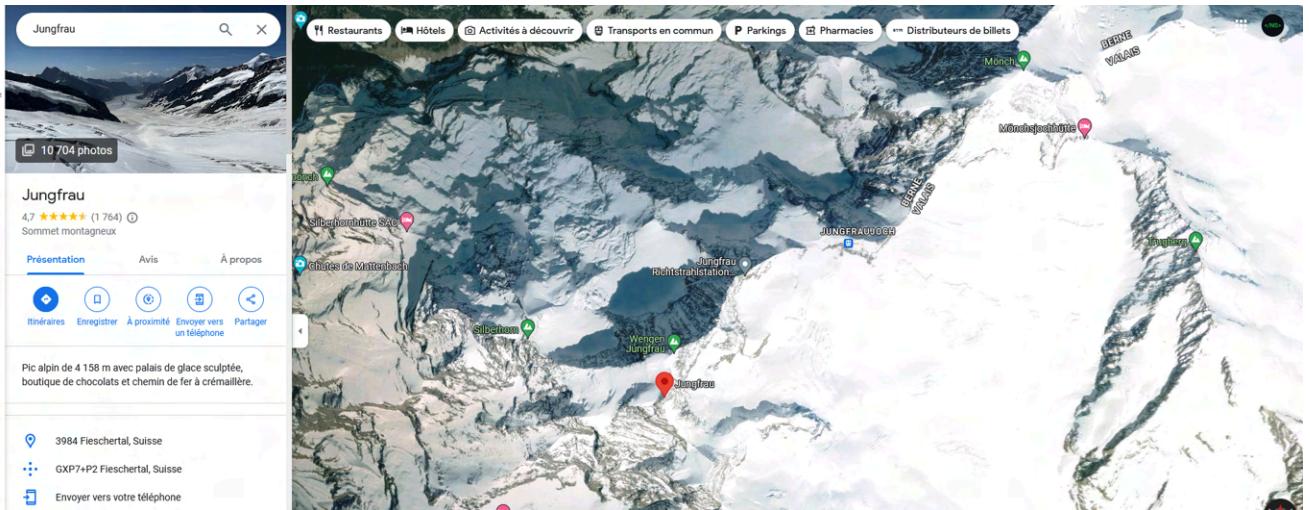
En effectuant une première recherche via Google Images, celle-ci nous donne directement la localisation.



En recherchant sur Google ce qu'est la Jungfrau, nous trouvons qu'il s'agit d'un sommet en Suisse

A screenshot of a Google search results page for the query 'Jungfrau'. The search bar at the top shows the query 'Jungfrau'. Below the search bar, there are tabs for 'Tous', 'Images', 'Vidéos', 'Maps', 'Shopping', and 'Plus'. On the right side, there is a 'Outils' (Tools) section. The main content area features a large image of a red and yellow train (the Jungfraubahn) traveling through a green, flower-filled valley towards a massive, snow-capped mountain range. To the right of this image is a map of the Jungfrau region, showing towns like Wilderswil, Gsteigwiler, Männlichen, Wengen, Lauterbrunnen, Mürren, Eiger, Mönch, and Jungfrau. Below the map is a weather forecast for Friday, Saturday, and Sunday, with temperatures of 0°, 1°, and 1° respectively. There is also a link to the website 'jungfrau.ch' and a thumbnail image of the Jungfrau mountain peak.

Cela colle bien avec notre suspecte. À présent, nous allons tâcher de trouver le lieu exact d'où a été prise la photo.



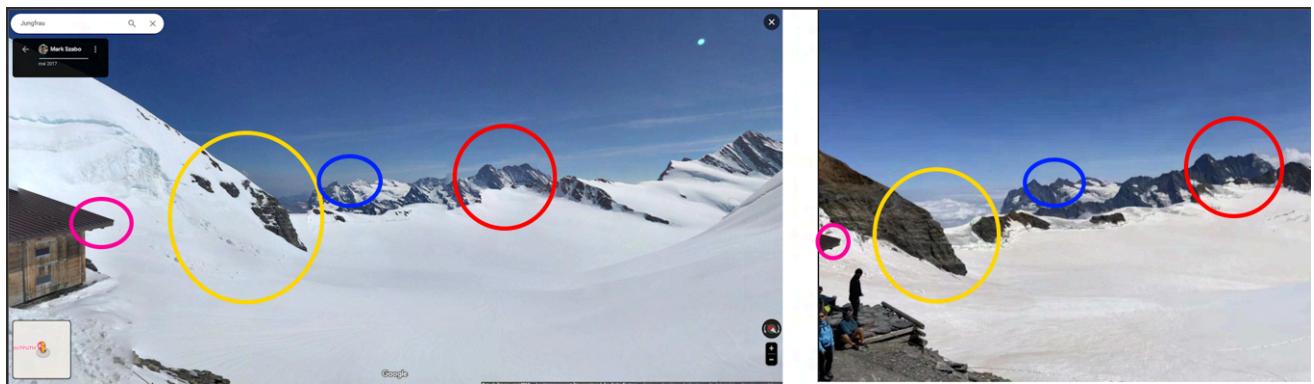
En regardant sur Google Maps, nous voyons à droite ce qui semble être un gîte ou un refuge.



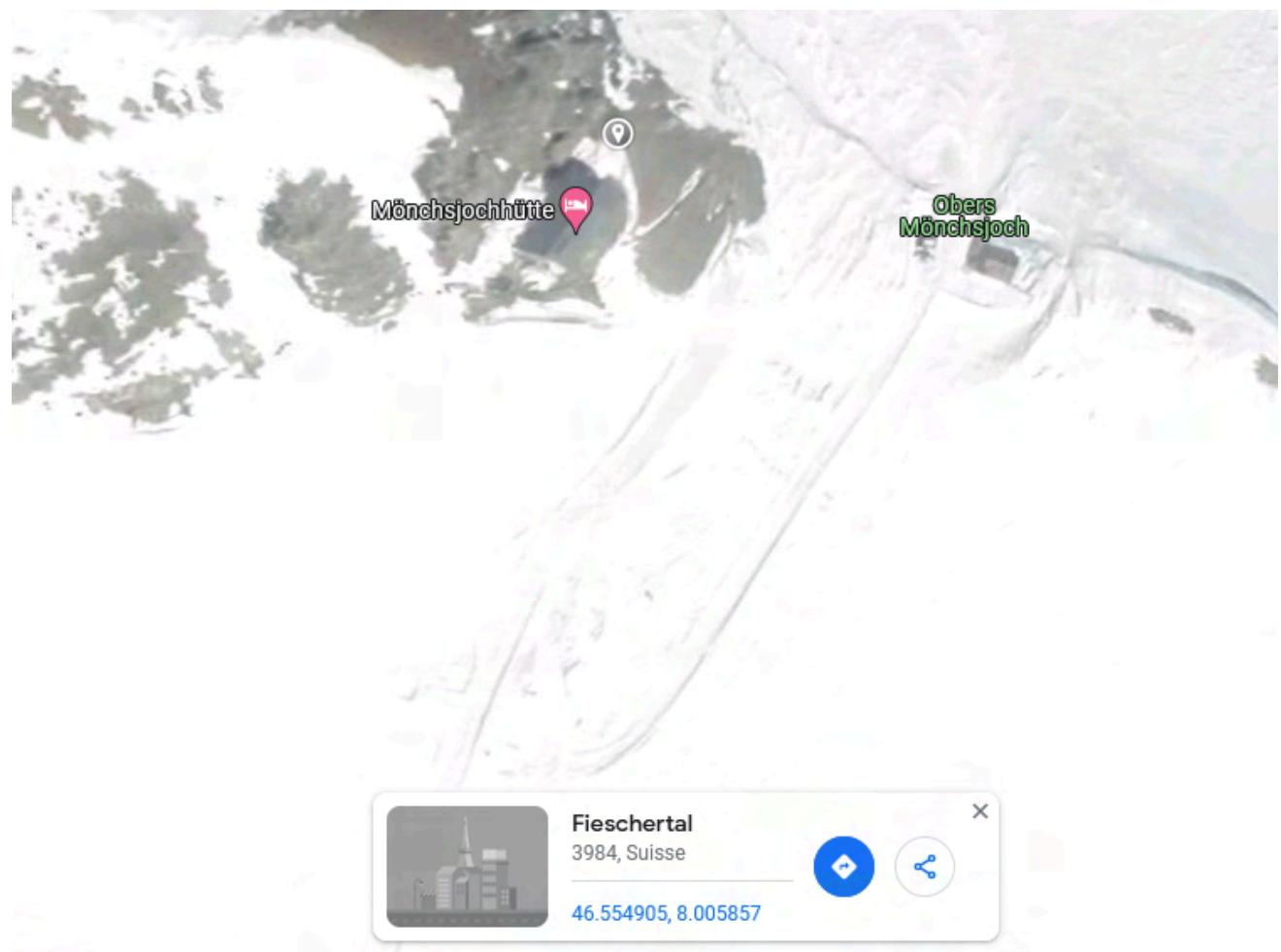
En nous positionnant en Street View sur ce chalet, nous obtenons ce résultat :



En effectuant les comparaisons, nous retrouvons les mêmes marqueurs que ceux sur la photo prise par Arina.



En positionnant le curseur sur Google Maps nous avons : **46.554, 8.005**



Nous pouvons valider le challenge.

FLAG : **46.554, 8.005**

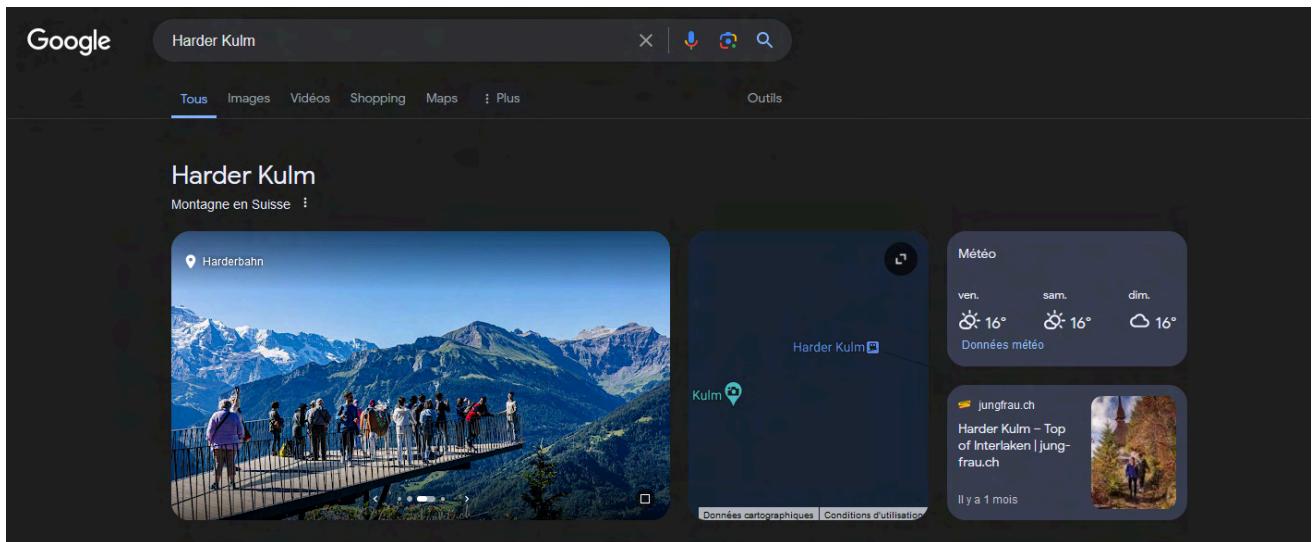
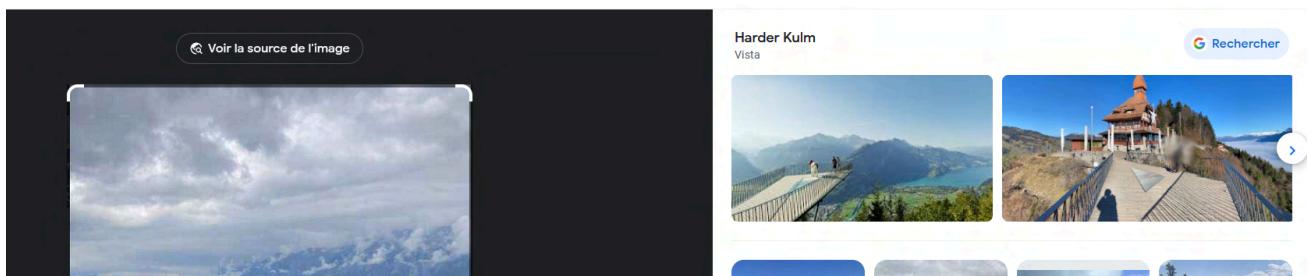
Challenge bonus 3 : Sur les traces de l'amende helvétique

A quelques mètres du lieu où la photo du 4 avril où l'on aperçoit le lac a été prise se trouve un élément emblématique du pays en question.

Quel était le montant de l'amende associée à cet élément en juillet 2016 ?

Format de Flag : 30

En reprenant l'image, nous avons pu définir que cette dernière a été prise à Harder Kulm



À partir de cela, nous savons qu'à quelques mètres du lieu où la photo a été prise, un élément emblématique du pays en question se trouve.

Ainsi, nous allons nous positionner en Street View, en cherchant un cliché datant de juillet 2016.



Sur ce cliché, nous voyons clairement notre élément symbolique, qui est bien situé à quelques mètres de là où la photo a été prise. Il s'agit donc de la vache.



Google

En zoomant davantage, nous pouvons apercevoir un papier, mais notre cliché n'est pas assez net pour voir ce qu'il y a écrit dessus. Nous devons trouver un autre point de vue.



Ce cliché est propre ; nous allons pouvoir l'exploiter.



En zoomant davantage, nous arrivons à lire : "Dont go up the cow, Penalty \$ 50"

Nous pouvons valider le challenge.

FLAG : 50