



Writeup APT Hunter CTF

Press Hunter

J1, J2, J3, J4



Mai 2024

Table des matières

1 Challenge	3
1.1 Introduction	3
1.2 Une communication inquiétante	4
1.3 La lettre	4
1.4 Une inattention ?	5
1.5 La piste de l'emploi	5
1.6 Coding	6
1.7 Python	7
1.8 Petite baie	7
1.8.1 Analyse du document Word	8
1.8.2 Analyse de l'image	8
1.8.3 Analyse de la vidéo	9
1.8.4 Analyse du Google Doc	9
1.8.5 Conclusion	9
1.9 Here comes a new challenger	10
1.10 You have been h4ck3d !	11
1.11 Infiltration Virtuelle	11
1.12 Update your system !	12
1.13 Crypto	12
1.14 Signature	13
1.15 L'entreprise sous attaque	13
1.16 Mise en orbite	14
1.17 Énigmes des ondes	15
1.18 Un bon ami	16
1.19 L'Identité Révélée	16
1.20 Entrée secrète	17
1.21 Command and Control	18
1.22 Une politique non respectée	18
1.23 Trafic dissimulé	19
1.24 Revente	20
1.25 Monnaie virtuelle	20
1.26 Achat	21
1.27 La clé financière	22
1.28 La Traque Financière	22
1.29 Sous le ciel d'adieu	23
1.30 Un bon bol d'air	26
1.31 Altitude	27
1.32 Un abri temporaire	28
1.33 Mise au point	30
1.34 6h00	31

1.35 La dernière pièce du puzzle	32
1.35.1 для пути - Pour le chemin	33
1.35.2 позволяет получить доступ к месту - Vous permet d'accéder au lieu	34
1.35.3 Статья в прессе - Article dans la presse	34
1.35.4 Фото на память - Photo pour mémoire	35
1.36 Lieu secret	35
1.36.1 Micro-remarque	38
1.37 Opération spéciale	39
1.38 La tête dans les étoiles	39
1.39 Arrêt net	40
1.40 Echec et mat	41
1.41 Sur les traces de l'amende helvétique	41
2 Conclusion	43
3 Flags	44
3.1 Flag - Introduction	44
3.2 Flag - Une communication inquiétante	44
3.3 Flag - La lettre	44
3.4 Flag - Une inattention ?	44
3.5 Flag - La piste de l'emploi	44
3.6 Flag - Coding	44
3.7 Flag - Python	44
3.8 Flag - Petite baie	44
3.9 Flag - Here comes a new challenger	45
3.10 Flag - You have been h4ck3d !	45
3.11 Flag - Infiltration Virtuelle	45
3.12 Flag - Update your system !	45
3.13 Flag - Crypto	45
3.14 Flag - Signature	45
3.15 Flag - L'entreprise sous attaque	45
3.16 Flag - Mise en orbite	45
3.17 Flag - Énigmes des ondes	45
3.18 Flag - Un bon ami	46
3.19 Flag - L'Identité Révélée	46
3.20 Flag - Entrée secrète	46
3.21 Flag - Command and Control	46
3.22 Flag - Une politique non respectée	46
3.23 Flag - Trafic dissimulé	46
3.24 Flag - Revente	46
3.25 Flag - Monnaie virtuelle	46
3.26 Flag - Achat	46
3.27 Flag - La clé financière	47
3.28 Flag - La Traque Financière	47

3.29 Flag - Sous le ciel d'adieu	47
3.30 Flag - Un bon bol d'air	47
3.31 Flag - Altitude	47
3.32 Flag - Un abri temporaire	47
3.33 Flag - Mise au point	47
3.34 Flag - 6h00	47
3.35 Flag - La dernière pièce du puzzle	47
3.36 Flag - Lieu secret	48
3.37 Flag - Opération spéciale	48
3.38 Flag - La tête dans les étoiles	48
3.39 Flag - Arrêt net	48
3.40 Flag - Echec et mat	48
3.41 Flag - Sur les traces de l'amende helvétique	48

1 Challenge

1.1 Introduction

Nous ne voulons pas vous submerger de règles, mais veuillez garder à l'esprit ces deux principes qui, à mon avis, relèvent simplement du bon sens :

1. Veuillez vous abstenir de lancer des scans ou tout autre type d'attaque red teaming sur les serveurs.
2. La tricherie et le partage de flags entre équipes sont strictement interdits et entraîneront la disqualification immédiate des équipes concernées.

[...]

Pour valider : **lu et accepté**

Un rappel des règles du CTF.

Flag - Introduction

1.2 Une communication inquiétante

Cher Agent,

Les services de renseignement 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 !

Entrez **compris** pour démarrer !

RAS.

Flag - Une communication inquiétante

1.3 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 première piste et s'efforceront tout au long de l'enquête de vous fournir des informations complémentaires.

Quel est le premier pseudonyme que vous avez trouvé ?

Qm9uam91ciwKCKnIbGEgZmFpdCB1biBtb21lbnQgcXVIIG5vdXMgbmUgbm91cyBzb21tZXMcGFzIHJlbmNvbnRy6XMuIMAgY2V0dGUg6XBvcXVLICB2b3VzIG4nYXZpZXogcGFzIGVuY29yZSBpbnTpZ3LpIGxlcyBzZXJ2aWNlcycBkZSByZW5zZWlnbmVtZW50cyBmcmFu52Fpcy4gTGVzIG9pc2VhdXggY2hhbnRhaWVudCwgbGVzIHZvaXR1cmVzIHNPbGxvbm5haWVudCBsZXMgcm91dGVzLCBsZSBjaWVsIOl0YWl0IGJsZXUsIGxhIHZpZSDpdGFpdCBiZWxsZS4uLgoKTWFsaGV1cmV1c2VtZW50LCBjZXMgdGVtcHMgc29udCBy6XvbHVzLiBKZSB2aWVucyB2ZXJzIHZvdXMgY2FylGxhIEZyYW5jZSBjb3VydCB1biBncmFuZCBkYW5nZXIuIEonYWkgZXUgdmVudCBk3VuZSBpbmZvcm1hdGlvbiBpbnF1ael0YW50ZSwgaW5kaXF1YW50IHFIJ3VuIG9yZ2FuaXNtZSBjbGFuZGVzdGluiHRIlbWVylGxhIHRIcnJldXIuCgpKZSBuZSBzYWlzIHhcBjZSBxdWkgc2UgY2FjaGUgZGVycmnocmUgdG91dCBjZWxhLCBuaSBxdWFuZCBjZWxhIHZhIGFycml2ZXIuIENlcGVuZGFudCwgaidhaSBy6XVzc2kg4CBpbnRlcmNlcHRlciB1biBwc2V1ZG9ueW1lIDogX1RyMHRzazEulE1hbGhldXJldXNlbWVudCwgamUgbmUgcGV1eCBwYXMgbVVuZXIgbCdlbnF16nRILCBjYXlgbW9ulGlkZW50aXTpIGVzdCBjb25udWUUcgpKZSB2b3VzIGNvbmZpZSBkb25jIGxhIGxvdXJkZSByZXNwb25zYWJpbGl06SBkZSBk6WNvdXZyaXIgbGEgdulyaXTpIGV0IGRIIHZlbmlyIOAgYm91dCBkZSBjZXR0ZSBtZW5hY2UuIEplIHNhaXMgcXVIHZvdXMgYXZleiB0b3V0ZXMgbGVzIHFIJ3VuIG9yZ2FuaXNtZSBjbGFuZGVzdGluiHRIlbWVylGxhIHRIcnJldXIuCgpKZSBpC25uZSBjaGFuY2UuCgpCLg==

Ca ressemble fortement à du Base64. Pour se simplifier la tâche, on passe ça dans [CyberChef](#):

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.

Le pseudonyme est directement indiqué dans ce texte.

Flag - La lettre

1.4 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 ?

Une recherche du pseudonyme sur les réseaux sociaux nous mènent à un [profil Twitter](#) et plus précisément un [tweet](#) où [_Tr0tsk1](#) poste son CV avec sa vraie identité :

The image shows two screenshots. On the left is a LinkedIn profile for 'ANDREJEW VLADLEN' with the title 'SOFTWARE ENGINEER'. It includes sections for 'CONTACT' (email: trtsk21@gmail.com, location: Tomsk) and 'SKILLS'. On the right is a tweet from the user '@_Tr0tsk1' (@Andrejew). The tweet reads: '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?' It was posted at 9:44 AM · Feb 23, 2024 · 585 Views.

Flag - Une inattention ?

1.5 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 ?

En ce qui concerne les activités professionnelles, LinkedIn reste le réseau social de prédilection. On y trouve effectivement le profil de [Andrejew Vladlen](#) et sa dernière entreprise.



Andrejew Vladlen
Software Engineer

Experience

 **Software Engineer**
Rubius · Full-time
Feb 2022 - Jan 2023 · 1 yr
Tomsk, Russia · On-site

- 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.

Flag - La piste de l'emploi

1.6 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)

Dans un de ces posts LinkedIn, Andrejew donne un lien vers un [Pastebin](#).



Andrejew Vladlen • 3rd+
Software Engineer
2mo • 

Je souhaitai vous partager mon dernière création ! Un jeu de roulette russe  coder en Python 
J'espère que ça vous plait, dites moi votre avis 😊

[See translation](#)

Русская рулетка - Pastebin.com

pastebin.com • 1 min read
Pastebin.com is the number one paste tool since 2002. Pastebin is a website...

 [SHARE](#)

PBKB112 NOV 574 ⭐ 0 NEVER  [TWEET](#)

Not a member of Pastebin yet? [Sign Up](#), it unlocks many cool features!

[text](#) 1.05 KB | None | [raw](#) [download](#) [clone](#) [embed](#)

 0  0 [print](#) [report](#)

```

1. # Russian Roulette game made in python. The rules
   are simple: Each player has to press enter to pull
   the trigger
2. # and the player that hits the chambers that
   contains the bullet, losses!

```

Flag - Coding

1.7 Python

Python cela vous parle ?
Quel est le nom du programme de la roulette russe ?

La fin du script Python contient un commentaire avec un lien vers un Google Drive.

```
if start_again and start_again.lower()[0] != "y":  
    break  
# For more scripts: https://drive.google.com/drive/folders/1  
thBhACRzWCMbaPogfAbpaMTB4dZ32GT0?usp=drive_link
```

Nom	Propriétaire
BAJH0	trtsk211@gmail.com
document.docx	trtsk211@gmail.com
kremlin.png	trtsk211@gmail.com
russian_roulette.py	trtsk211@gmail.com
video Kalinka russian dance.mp4	trtsk211@gmail.com

On y trouve différents fichiers dont le programme Python recherché. A noter qu'on voit également l'adresse mail du propriétaire trtsk211@gmail.com qu'on suppose être celle de Andrejew.

Flag - Python

1.8 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 ?

Nom	Propriétaire
BAJH0	trtsk211@gmail.com
document.docx	trtsk211@gmail.com
kremlin.png	trtsk211@gmail.com
russian_roulette.py	trtsk211@gmail.com
video Kalinka russian dance.mp4	trtsk211@gmail.com

Le Google Drive contient 5 fichiers :

- Le Python [russian_roulette.py](#) qui nous a donné le lien.

- document.docx
- kremlin.png
- video Kalinka russian dance.mp4
- Un dossier **ВАЖНО** (important en russe) qui contient un Google Doc **очень важно** (très important).

1.8.1 Analyse du document Word

Le document Word contient un long texte en russe qui une fois traduit peut ressembler à un manifeste. Un paragraphe en particulier a retenu notre attention :

L'éducation et la connaissance sont la clé de notre avenir. En soutenant le développement de la science et de la culture, nous contribuons à la croissance et au bien-être de nos citoyens. <https://drive.google.com/drive/> Le respect de la diversité de notre pays nous renforce. Différentes cultures et traditions fusionnent pour créer le patrimoine unique et riche de notre nation.

Nous avons un début de lien de Google Drive. A partir de là, nous comprenons que chaque document contient une partie du lien.

1.8.2 Analyse de l'image

L'image dans [Aperisolve](#) nous donne un résultat intéressant avec `zsteg` :

```
zsteg kremlin.png
imagedata          .. text: "x@T\ \fV8^"
b1,g,lsb,xy       .. file: OpenPGP Public Key
b1,rgb,lsb,xy    .. text: "folders/1eXT8Wxae6qgH52AkYmUvT"
```

On obtient ainsi une deuxième partie du lien avec les paramètres `b1,rgb,lsb,xy`.

1.8.3 Analyse de la vidéo



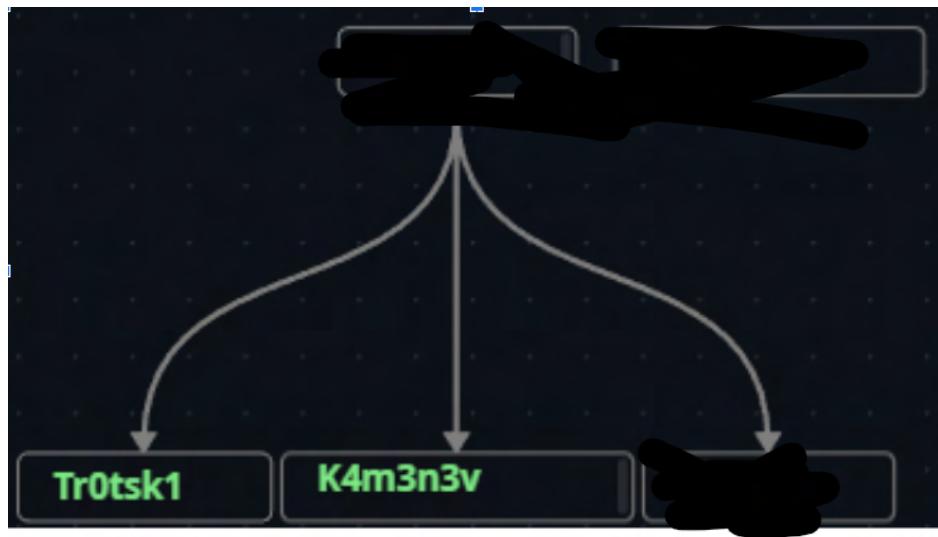
A 41.21 secondes, on a la dernière partie du lien : Mn6nDpQYbb6?usp=sharing. OpenShot Video Editor est un éditeur vidéo assez simple à utiliser et sans installation (tout du moins sous Linux).

1.8.4 Analyse du Google Doc

Une suite de caractères hexadécimaux : aHR0cHM6Ly9iaXQubHkvM0pEWkdtUw. On peut toujours essayer de décoder avec [Basecrack](#) (excellent outil au passage !) pour un [résultat sans intérêt](#). On met cet élément de côté.

1.8.5 Conclusion

Reste donc à concaténer tout ça (sans le Rick Roll) : <https://drive.google.com/drive/folders/1eXT8Wxae6qgH52AkYmUvTMn6nDpQYbb6?usp=sharing>. Le nouveau Drive donne une nouvelle adresse mail (zveplay@gmail.com) et surtout une image qui contient ce qui semble être un organigramme partiellement effacé.



On y retrouve Tr0tsk1/Andrejew ainsi qu'un nouveau pseudonyme.

Flag - Petite baie

1.9 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 ?

Un problème assez similaire à ce qu'on avait pu avoir dans le CTF Disparues de Oscar Zulu et le seul hint qu'on a payé, bêtement. Le hint nous disait en substance de trouver "là où les gens expriment leurs émotions publiquement". Après des recherches avec le mot clé K4m3n3v sur les différents réseaux sociaux usuels, on est enfin tombé sur la réponse en n'oubliant pas de cocher "Publications récentes" dans Facebook. Et si possible, on ne crame pas un essai en faisant "Prénom Nom" au lieu de "Nom Prénom"...

Résultats de la recherche

Filtres Réinitialiser

- Tous
- Publications**
- Publications récentes
- Publications que vous avez vues
- Date de publication
- Publications de
- Lieu identifié
- Personnes

Julien Prevot se sent en colère.
4 avril ·

Pourquoi ça n'arrive qu'à moi ce genre de choses ?????? Je pensais avoir tout vérifié concernant la sécurité de mon site !!!!!!!

J'ai regardé un peu le code et il y fait mention d'un certain K4m3n3v ! ça parle à quelqu'un ???

#DEFACED

YOUR SYSTEM HAS BEEN HACKED :-)! BAD SECURITY!
--Kolybyte

J'aime Partager

Flag - Here comes a new challenger

1.10 You have been h4ck3d !

Connaissez-vous le défactement ? 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 ?

On tombe donc sur le profil de [Julien Prevot](#), CTO de SeaCipher, une entreprise qui travaille dans les cryptomonnaies. Il suffit d'aller sur le site de [SeaCipher](#) pour identifier le groupe qui a défacé le site.

Flag - You have been h4ck3d !

1.11 Infiltration Virtuelle

Un défactement 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 défactement du site ?

Le site de SeaCipher a été défacé, mais son [robots.txt](#) est toujours accessible. Selon [robots-txt.com](#):

Le protocole d'exclusion des robots, plus connu sous le nom de robots.txt, est une convention visant à empêcher les robots d'exploration (web crawlers) d'accéder à tout ou une partie d'un site web.

```
User-agent: *
Disallow: /secret/
Disallow: /hidden/
Disallow: /confidential/
Disallow: /private-area/
Disallow: /admin-section/
Disallow: /restricted/
Disallow: /exclusive-content/
Disallow: /backups/
Disallow: /backd00r/
Disallow: /temp/
Disallow: /old-files/
Disallow: /development-env/
Disallow: /staging-area/
Disallow: /archive-files/
Disallow: /not-for-public-view/
Disallow: /vip-members/
```

On teste les différents chemins, un seul, sobrement nommé [backd00r](#) est accessible. Le nom de l'outil est directement affiché.

The screenshot shows a web-based file upload interface. At the top, it displays the current path as `/var/www/html/seacipher` and the PHP version as 4.3.2. Below this is a file upload form with a "Choose File" input set to "No file chosen" and a "upload" button. A table lists the files in the directory:

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

Flag - Infiltration Virtuelle

1.12 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 ?

En regardant le screenshot juste au-dessus, on identifie directement la version de PHP utilisée.

Flag - Update your system !

1.13 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 ?

Le site ayant été défacé, on se tourne vers la Wayback Machine qui contient fort heureusement une copie du site qui date de Mars 2024. Le cours du SeaCipher est indiqué en haut de la page.

The screenshot shows a Wayback Machine capture of the SeaCipher website from March 25, 2024. The page features a large, stylized blue letter 'C' logo followed by the word "SeaCipher" in green. Above the logo, a green upward arrow indicates the current price: "SeaCipher 0.00000000355 +45.63%". The page also includes the words "REVOLUTIONNAIRE" and "INNOVANT". Navigation links for "ACCUEIL" and "A PROPOS DE NOUS" are visible at the bottom.

Flag - Crypto

1.14 Signature

Les hackers aiment laisser leur signature sur leurs « œuvres ».
Sous quel autre pseudonyme le hacker est-il également connu ?

Toujours en étant sur la page [backd00r](#), on a étudié le code source de la page. L'en-tête contient un nouveau pseudo qui peut faire penser à celui déjà trouvé.

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

Flag - Signature

1.15 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)

Une recherche avec [Sherlock](#) nous renvoie un seul et unique résultat : un profil Mastodon !

```
$ python sherlock _v3n3m4K_
[*] Checking username _v3n3m4K_ on:
[+] mastodon.social: https://mastodon.social/@_v3n3m4K_
[*] Search completed with 1 results
```

On y trouve un lien vers un profil Github :

github.com/k4menev/'. At the bottom, it shows statistics: '11 Posts', '3 Following', and '0 Followers'. A small box at the bottom left says 'JOINED Mar 13, 2024'."/>

v3n3m4K
@_v3n3m4K_ mastodon.social

Follow

Follow me [github.com/k4menev/](#)

JOINED
Mar 13, 2024

11 Posts 3 Following 0 Followers

Le Github contient essentiellement des forks de projets existants mais un seul dépôt personnel nommé `first-try`. En étudiant le [dernier commit](#), on identifie l'entreprise visée par le hacker qu'il a voulu effacer du dépôt :

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

NB : On ne s'est pas essayé à comprendre ce code assembleur...

Flag - L'entreprise sous attaque

1.16 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)

Sur le site de Stella Launch Solutions, il suffit d'aller voir la page [Team](#) :

The screenshot shows a web browser window with the following details:

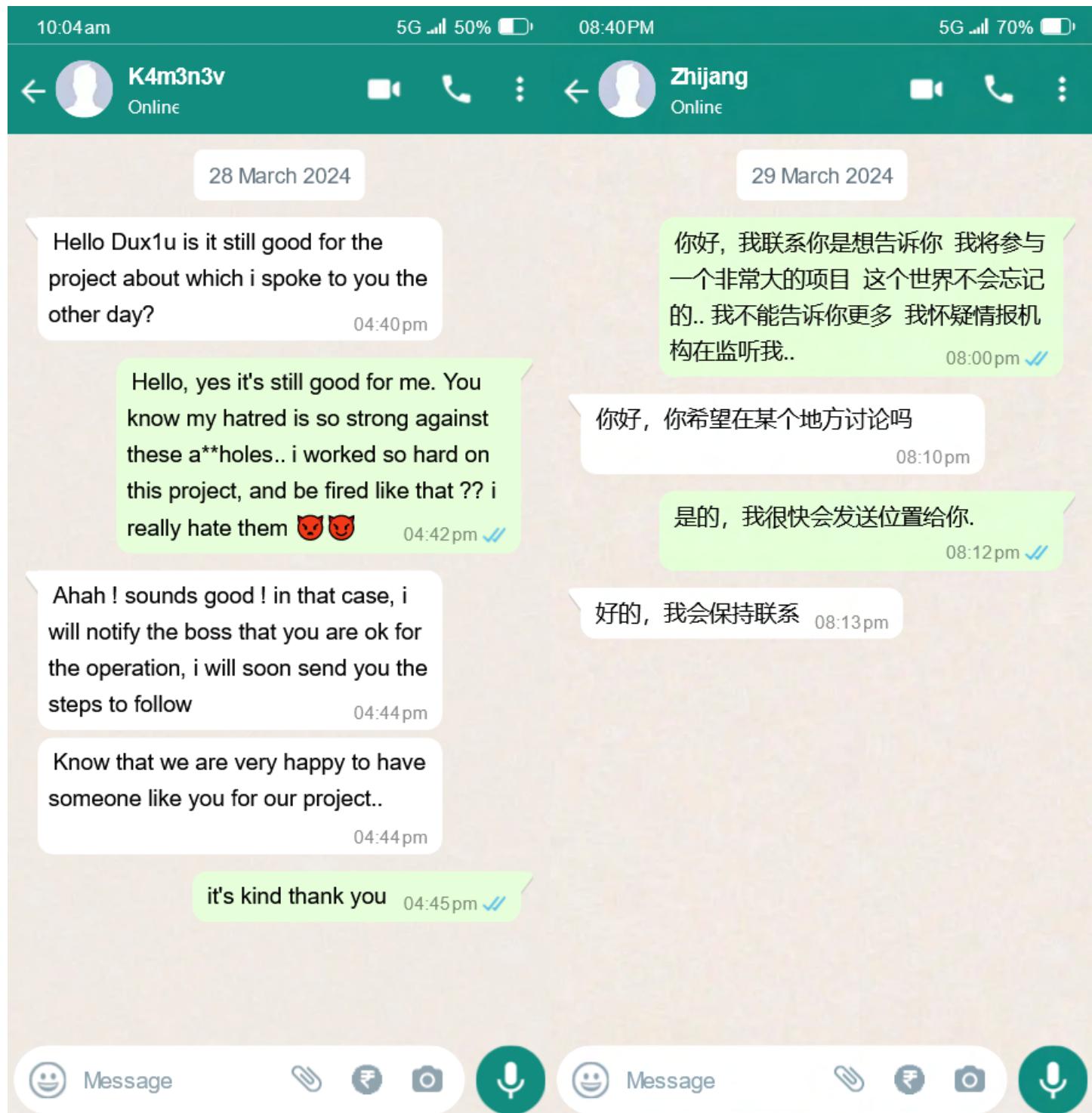
- Address Bar:** Shows the URL `stella-launch-solutions.com/#team-section`.
- Page Content:**
 - Logo:** The Stella Launch Solutions logo, which is a stylized purple and white graphic followed by the text "STELLA LAUNCH".
 - Tagline:** "They do their best for you" in a pink font.
 - Key Employees:** A section titled "KEY EMPLOYEES" featuring two profiles:
 - Matilda Beck:** R&D Division Manager. She is a woman with blonde hair, wearing glasses and a white lab coat, smiling at the camera.
 - Kyron O'Gallagher:** Engineer. He is a man with a beard, wearing a blue protective cap and safety goggles, looking directly at the camera.

Flag - Mise en orbite

1.17 Énigmes 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 ?



On identifie directement le pseudonyme dans le premier screenshot.

Flag - Énigmes des ondes

1.18 Un bon ami

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

Quel est le prénom de l'ami de Dux1u ?

Une traduction du deuxième screenshot Whatsapp :

Bonjour, je tiens à vous dire que je participerai à un très grand projet que le monde n'oubliera pas... Je ne peux pas vous en dire plus. Je doute des services de renseignement. Je suis en prison...

Bonjour, souhaiteriez-vous discuter quelque part

Oui, je vous enverrai bientôt l'emplacement.

D'accord, je resterai connecté

Il s'agit du prénom visible dans le deuxième screenshot Whatsapp puisqu'on comprend que Dux1u reparle du projet secret.

Flag - Un bon ami

1.19 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)



On comprend que Dux1u a été licencié de Stella Launch Solutions et qu'il cherche un moyen de se venger. La recherche par pseudonyme ne donne. Dans un challenge précédent, on a visité la page qui liste les [employés de Stella Launch Solutions](#). Et si Dux1u était dans une version précédente de cette même page (avant le 28 mars) ?

Une [sauvegarde du 13 mars](#) nous donne la réponse : on trouve un employé qui n'est pas dans la version actuelle du site de Stella.

They do their best for you



Fleur Harmon
Engineer



Wen Ch'ien
Aerospace engineer

Flag - L'Identité Révélée

1.20 Entrée secrète

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.

A priori, on cherche une autre page sur le site de Stella où il y aurait une backdoor. Contrairement au site de Seacipher, il n'y a rien dans le [robots.txt](#). On lance alors un [urlscan.io](#) qui nous donne les différentes URLs accessibles dans ce domaine et surtout une qui nous donne accès à [la page avec backdoor](#).

A screenshot of a web browser window. The address bar shows the URL "stella-launch-solutions.com/af0512e16553f/". The main content area displays a terminal-like interface with the title "ReverseShellWebV1.1". Inside the terminal, there is a single line of text: "bc29156d400a18991f6087c@debian:~\$". The browser interface includes standard navigation buttons (back, forward, search) and a star icon for bookmarks.

Flag - Entrée secrète

1.21 Command and Control

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 ?

On teste les différentes commandes disponibles dans le reverse shell :

```
bc29156d400a18991f6087c@debian:~$ help
Available commands: help, startc2server, id, pwd, extractpasswd
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
```

Flag - Command and Control

1.22 Une politique non respectée

En parcourant le terminal, vous trouvez une commande intriguante.

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

```
bc29156d400a18991f6087c@debian:~$ extractpasswd
[i] Try to find /etc/shadow
[+] Credentials found !
[i] Gaining access...
.
.
.
.
[i] root : 240be518fabd2724ddb6f04eeb1da5967448d7e831c08c8fa822809f74c720a9
[i] stellalaunchsolutions : 008c70392e3abfb0fa47bbc2ed96aa99bd49e159727fcba0f2e6abeb
3a9d601
```

On voit que ce sont des hashs SHA2-256 avec un [outil en ligne](#). On utilise ensuite un autre [outil pour déchiffrer](#).

Flag - Une politique non respectée

1.23 Trafic dissimulé

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 ?

```
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
```

On comprend qu'on cherche à déchiffrer ce qui est dans `Host`. Ca ne ressemble pas à un hash classique qu'on connaît. A tout hasard, on teste cette chaîne de caractères dans [Basecrack](#) qui a le bon goût de tester le Base64, toutes ses variantes ainsi que les cas où on enchaînerait plusieurs passes :

```
$ python basecrack.py --magic
[>] Enter Encoded Base: Dzt(X*bSyiGHq+43GHv*kG4Rygp^+kjVE^=RrF+f@Rt0C0^=DYk+kA6}JNF#jw^8HgkpTt5Wt)qCB
[-] Iteration: 1
[-] Heuristic Found Encoding To Be: Base92
[-] Decoding as Base92: co4fuiol57xfwjobszioknloyqejr7emsey5obnhsnwg23725jn6yd.onion
{{<<=====>>}}
[-] Total Iterations: 1
[-] Encoding Pattern: Base92
[-] Magic Decode Finished With Result:
co4fuiol57xfwjobszioknloyqejr7emsey5obnhsnwg23725jn6yd.onion
```

Un lien vers un site sur TOR !

Flag - Trafic dissimulé

1.24 Revente

Cela ne vous étonne pas de trouver un site sur le réseau Tor ; la plupart des cybercriminels utilisent ce réseau pour revendre des données.

Quel est le prix de vente de “La Pomme Fraîche” en ETH ? (le chiffre uniquement, sans la devise)

The screenshot shows a dark-themed Tor browser window for 'The KolymaByte Market'. At the top, it displays the URL 'co4fuiol57xfwjobszioknloyqejrx7emsey5obnhsnwg23725jn6yd.onion' and language settings 'Russian → English Automatic Translation enabled. Elements pending to translate: 0'. The main page features a large circular logo with a silhouette of a person wearing a fedora hat against a red background, with the text 'Demand only the quality' below it. To the right, there is a grid of eight data leak listings:

"SeaCipher"	"Les Enfants d'Hades"	"StellaLaunch"	"Tech Consulting"
All databases with private wallet login 97,589 ETH	Last name, Name, Address, Social insurance, Phone number, Credit card 0,836 ETH	Database, surname, name, address, phone number, password 41,824 ETH	Database, surname, name, address, phone number, password 39,035 ETH
"Innovative Designs"	"Gourmet Brasserie"	"Ancien Salon de th"	"La Pomme Fraîche"
Database, surname, name, address, phone number, password 55,7654 ETH	Database, surname, name, address, phone number, password 1,337 ETH <i>Sold out</i>	Database, surname, name, address, phone number, password 4,12345 ETH <i>Sold out</i>	Database, surname, name, address, phone number, password 6,997 ETH <i>Sold out</i>

Copyright - KolymaByte Market

Ce site est tout simplement la marketplace de KolymaByte qui vend des leaks de bases de données de différentes entités dont Stella Launch Solutions, Les enfants d’Hades (si vous avez fait le CTF Disparues de Oscar Zulu, [ça vous parle](#)) et la Pomme Fraîche.

Flag - Revente

1.25 Monnaie virtuelle

La cryptomonnaie est la monnaie de prédilection sur le darknet.

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

Il suffit d'aller sur la page [Как купить](#) de la marketplace.

The screenshot shows a dark-themed Tor browser window for 'The KolymaByte Market'. At the top, it displays the URL 'co4fuiol57xfwjobszioknloyqejrx7emsey5obnhsnwg23725jn6yd.onion/how-to-buy.html' and language settings 'Russian → English Automatic Translation enabled. Elements pending to translate: 0'. To the right, there is a 'Translate this tab automatically' button. Below the header, there is a large black rectangular redaction area. Underneath it, a white box contains the heading 'How to buy' and the following text:

To buy just send the exact amount to ETH to this cryptocurrency wallet 0xCec4748becc7eC74214cA0BDb3bC8DDAf68D4108. Then you will be sent confirming the message, and you can download the data within 5 days.

Thank you for your trust!

Flag - Monnaie virtuelle

1.26 Achat

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

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

Après avoir cherché sur les différents blockchain explorers qui peuvent exister, on s'est souvent que nous étions dans un CTF. Pour ce qui concerne les cryptomonnaies, on essaye alors d'aller sur le [Testnet Sepolia](#). L'adresse du portefeuille pour acheter les données a été utilisée pour différentes transactions, notamment 3 pour 0 ETH.

Latest 8 from a total of 8 transactions							
①	Transaction Hash	Method ②	Block	Age	From	To	Value Txn Fee
②	0xd7634b1c3...	Transfer	5626415	34 days ago	0xff374A42...A318aa200	IN 0xCec4748b...Af68D4108	1.4240613 ETH 0.0000315
②	0xc98d285672...	Transfer	5626210	34 days ago	0xCec4748b...Af68D4108	OUT 0xD1C7d77...43faC36C4	2.42354676 ETH 0.0000315
②	0x4f57753eb4e...	Safe Mint	5622674	34 days ago	0xCec4748b...Af68D4108	OUT 0x9F64932B...921f372B6	0 ETH 0.00043491
②	0x6675c8c349...	Safe Mint	5622662	34 days ago	0xCec4748b...Af68D4108	OUT 0x9F64932B...921f372B6	0 ETH 0.00043931
②	0xf0dc112e846...	Safe Mint	5622633	34 days ago	0xCec4748b...Af68D4108	OUT 0x9F64932B...921f372B6	0 ETH 0.00044013
②	0x067b85c029...	Transfer	5578939	40 days ago	0xee70bdE4...A73D3eF52	IN 0xCec4748b...Af68D4108	1.337 ETH 0.00003773
②	0xbe4b96914d...	Transfer	5578937	40 days ago	0xaFB4F595...681496F85	IN 0xCec4748b...Af68D4108	4.12345 ETH 0.00003749
②	0x17274242d2...	Transfer	5578934	40 days ago	0xD5e107b...54f60d6ff	IN 0xCec4748b...Af68D4108	6.997 ETH 0.00003906

Première transaction : dans la section “More details”, on identifie [un lien vers un fichier JSON](#).

① Other Attributes:	Txn Type: 2 (EIP-1559)	Nonce: 2	Position In Block: 31								
② Input Data:	# Name Type Data	<table border="1"> <tr> <td>0</td> <td>to</td> <td>address</td> <td>0xee70bdE4Bc29F2491b8aeF671298E0bA73D3eF52</td> </tr> <tr> <td>1</td> <td>uri</td> <td>string</td> <td>https://nftstorage.link/ipfs/bafybeiagcwda4u32yofiyguzud1mydxuwlmuryvbbecjaugrlfj44ssaa/696a9f4b-da39-44e0-bc21-5b6c537ad7c1.json</td> </tr> </table>		0	to	address	0xee70bdE4Bc29F2491b8aeF671298E0bA73D3eF52	1	uri	string	https://nftstorage.link/ipfs/bafybeiagcwda4u32yofiyguzud1mydxuwlmuryvbbecjaugrlfj44ssaa/696a9f4b-da39-44e0-bc21-5b6c537ad7c1.json
0	to	address	0xee70bdE4Bc29F2491b8aeF671298E0bA73D3eF52								
1	uri	string	https://nftstorage.link/ipfs/bafybeiagcwda4u32yofiyguzud1mydxuwlmuryvbbecjaugrlfj44ssaa/696a9f4b-da39-44e0-bc21-5b6c537ad7c1.json								
	Switch Back										
More Details:	— Click to show less										

JSON qui contient [un lien vers un PDF](#) qui n'est rien d'autre que la facture pour le leak de Gourmet Brasserie ! On effectue la même recherche avec les deux autres transactions pour obtenir 3 factures :

INVOICE SUMMARY	INVOICE SUMMARY	INVOICE SUMMARY
To: 0xD5e107b4A3884dA16db5ef4f73d48954f60d6ff	To: 0xCec4748becc7eC74214cA0BDb3bC8DDAf68D4108	To: 0xCec4748becc7eC74214cA0BDb3bC8DDAf68D4108
From: 0xCec4748becc7eC74214cA0BDb3bC8DDAf68D4108	From: 0xaFB4F59507C1E055A61c360Bd29F90c681496F85	From: 0xee70bdE4Bc29F2491b8aeF671298E0bA73D3eF52
Description of Item: La Pomme Fraîche	Description of Item: Ancien Salon de thé	Description of Item: Gourmet Brasserie
Content: База данных, фамилия, имя, адрес, номер телефона, пароль	Content: База данных, фамилия, имя, адрес, номер телефона, пароль	Content: База данных, фамилия, имя, адрес, номер телефона, пароль
Price: 6.997 ETH	Price: 4.12345 ETH	Price: 1.337 ETH
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	Note: "Chaque cœur possède une mélodie secrète, attendant qu'une âme sœur vienne l'orchestrer." #AU

Chaque facture est accompagnée d'une citation avec le mot-dièse #AU. C'est un détail qui est important pour la suite.

Flag - Achat

1.27 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 ?

Le #AU n'a rien donné sur les réseaux sociaux classiques (notamment Twitter) jusqu'à ce qu'on aille sur Mastodon :

The screenshot shows the Mastodon interface. On the left, there's a sidebar with the Mastodon logo and some server statistics: "mastodon.social is part of the decentralized social network powered by Mastodon.", "ADMINISTERED BY: Mastodon @Mastodon", and "235K active users". Below that is a "Learn more" button. The main area shows a search bar with "#AU" and a feed of tweets. Two tweets are visible:

- AU** (@Arina_Urvr, Apr 16)
"Chaque épreuve est un fil sur le métier à tisser de notre caractère."
#citational #AU
- AU** (@Arina_Urvr, Apr 16)
"Les étoiles brillent pour tous, mais c'est à chacun de choisir son étoile à suivre."
AU

On the right side of the interface, there are links for "Explore", "Live feeds", and a "Create account" button.

On tombe alors sur le [profil d'une personne](#) qui se déclare "Adepte de la langue française et de la poésie" et qui fait des toots sous forme de citation avec la signature AU conformément aux factures trouvées sur TOR.

Flag - La clé financière

1.28 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 ?

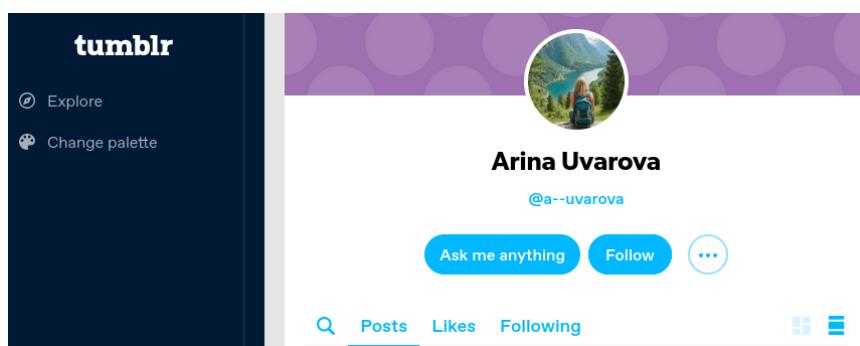
Sur Mastodon, contrairement à Twitter/X, on peut éditer ses toots. Cela se voit avec un symbole *.

The screenshot shows the Mastodon interface. The top tweet has been edited, indicated by a small asterisk (*) next to the timestamp "Apr 7". The text of the tweet has been truncated: "Dommage que l'on ne puisse pas poster de long textes ..". The bottom tweet is in its original state: "Dans le jardin de l'âme, la patience est la fleur la plus rare et la plus belle." #AU

Dans ce toot, la personne se plaint de ne pas pouvoir poster des textes plus longs. En regardant les différentes versions du toot, on trouve son pseudonyme sur Tumblr, une plateforme où la limite de longueur est [beaucoup plus importante](#).

The image shows two side-by-side posts. On the left is a Mastodon post by user AU (@Arina_Urvv@mastodon.social) dated April 7, 2024, at 07:04 PM. The content is "Dommage que l'on ne puisse pas poster de long textes ..". Below it is a note: "Last edited Apr 07, 07:04 PM" and "0 bo Edited 1 time". On the right is a Tumblr post by user Arina_Urvv (@a--uvarova) dated April 7, 2024. The content is identical: "Dommage que l'on ne puisse pas poster de long textes .. RDV sur Tumblr !". Below it is a note: "Arina_Urvv created Apr 7". Both posts have a small profile picture of a person with blonde hair and a blue backpack.

On obtient alors l'identité réelle sur son [Tumblr](#) :



Flag - La Traque Financière

1.29 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 ?

Selon [ce post](#), on comprend qu'Arina Uvarova a dû quitter la Russie, on suppose à partir d'un aéroport russe.





En regardant un peu plus en détails la photo, on est a priori sur un petit aéroport. Nous cherchons alors à déchiffrer le nom marqué en cyrillique. Deux outils pour cela :

- Un [clavier russe cyrillique](#).
- Une liste des [aéroports russes, en cyrillique](#) (passez la page Wikipedia en langue russe).

Même si le mot est très pixelisé, on devine qu'il commence par un **C** et finit par un **T** et que le nom doit faire au plus 5-6 caractères. D'après le clavier Lexilogos, le **C** correspond à un **S** en alphabet latin.

A partir de la liste, on vérifie les différents noms jusqu'à tomber sur l'aéroport de Sourgout (Сургут en russe) qui a l'air de correspondre au texte zoomé. Nous souhaitons malgré tout confirmer en trouvant d'autres images de l'aéroport en question.

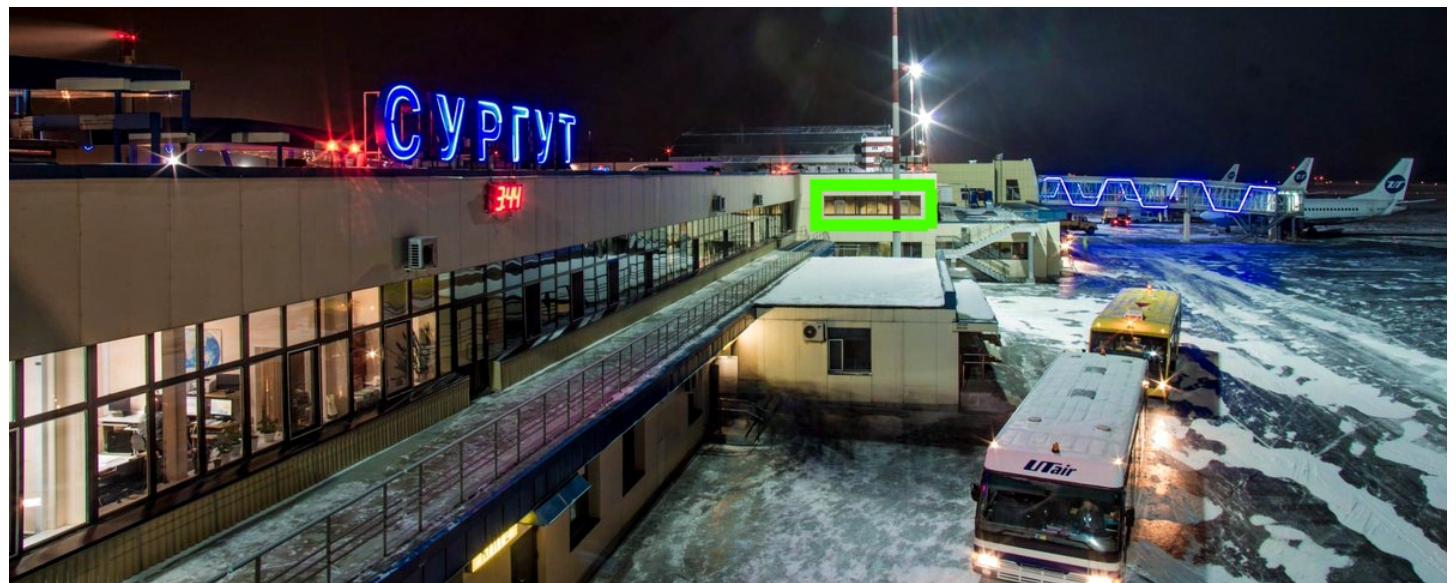
Une [première photo](#) où on voit le texte clairement, l'horloge 7 segments et le bâtiment qui a l'air de ressembler.



Une deuxième image nous permet de voir que les différents éléments correspondent :



La photo a été prise depuis la fenêtre encadrée en vert sur la photo ci-dessous :



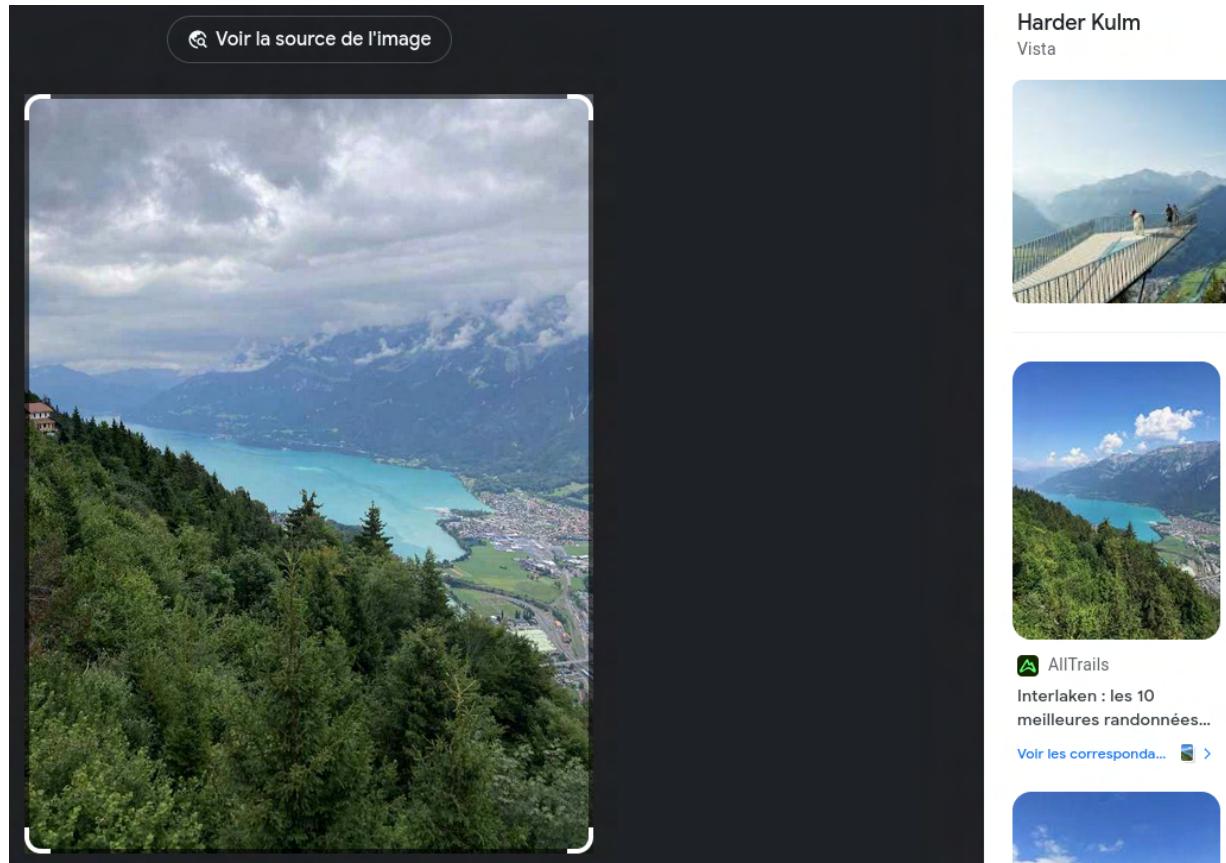
On a donc bien retrouvé l'aéroport !

Flag - Sous le ciel d'adieu

1.30 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 ?

Retour sur le profil Mastodon d'Arina et [sa photo du 4 avril 2024](#). On identifie rapidement le lac de Brienz au-dessus de Interlaken/Unterseen et plus précisément le Harder Kulm où se trouve un belvédère au-dessus du lac.



Etant donné que le point de vue a l'air à la frontière des deux villes, on a d'abord essayé Interlaken. Mais en vérifiant avec Google Map, le point est bien sur la commune d'Unterseen :



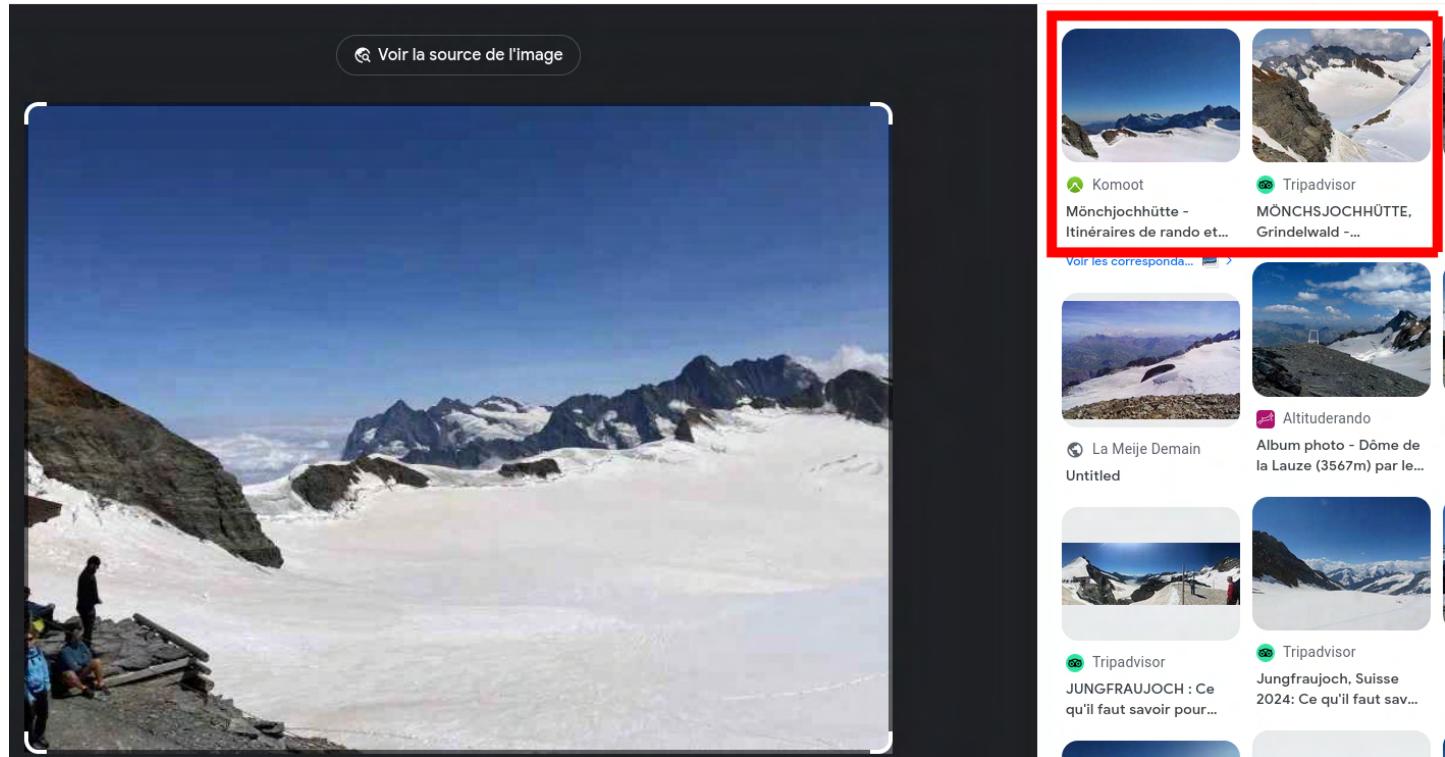
Flag - Un bon bol d'air

1.31 Altitude

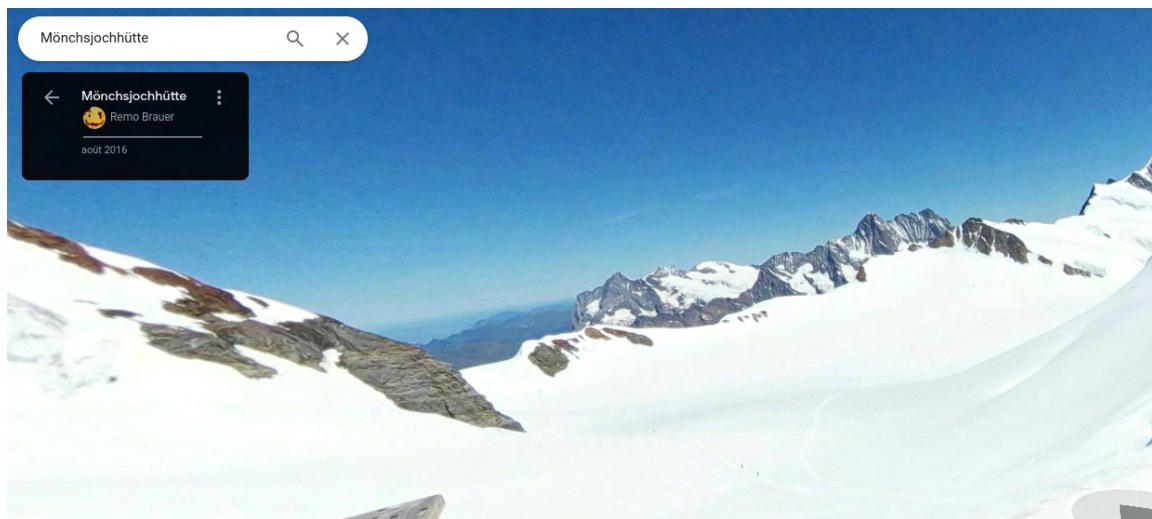
En examinant ses photos, vous trouvez une publication qui semble avoir été capturée depuis une altitude très élevée.

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

On cherche donc les coordonnées de la photo de montagne visible dans [ce toot](#). Après une simple recherche, la photo sur Komoot paraît correspondre :



On peut confirmer avec StreetView, le refuge Mönchsjochhütte est le point recherché !



Flag - Altitude

1.32 Un abri temporaire

Vous savez à présent où se trouve la trésorière, cependant une photo vous donne une grande indication quant à sa possible localisation.

Quelle année pouvez-vous distinguer sur la façade de sa résidence?

Ensuite, on retourne sur le [profil Tumblr d'Arina](#) :

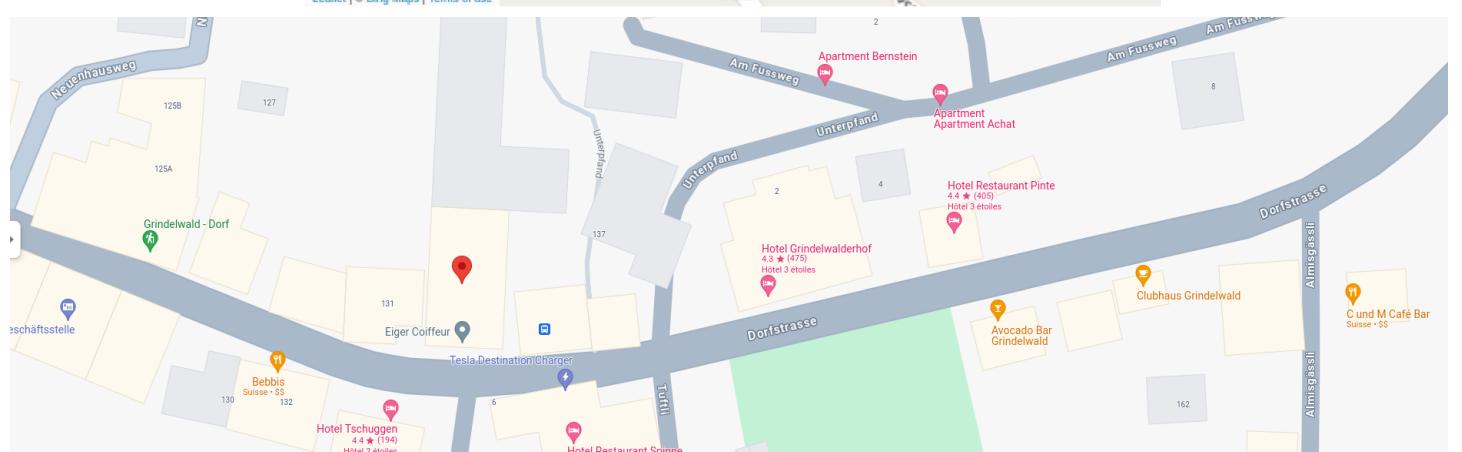
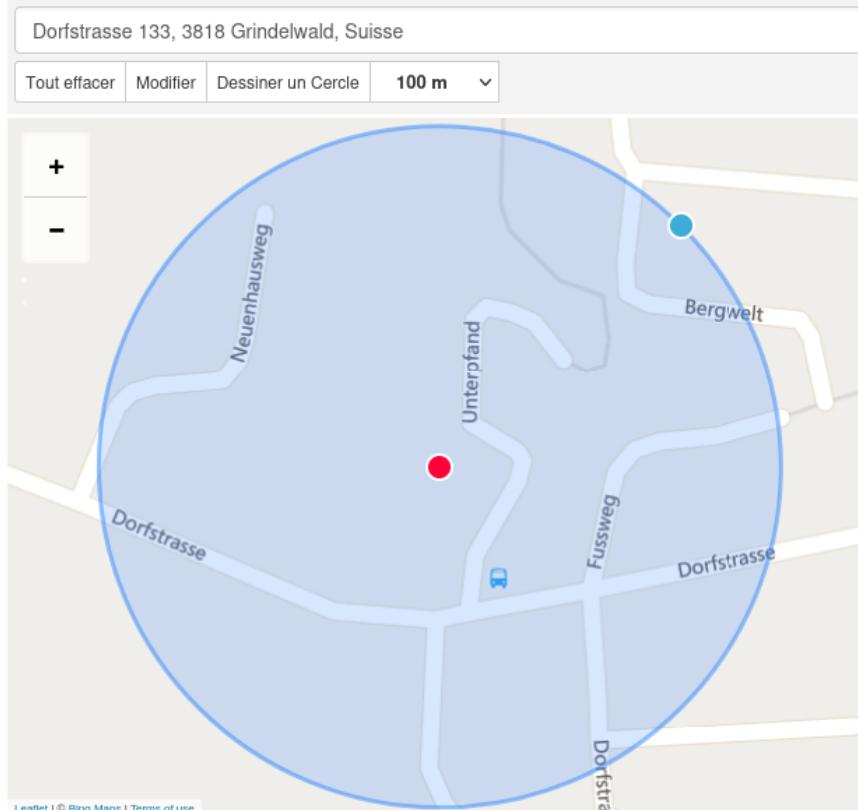


Ce pays m'avait manqué ! Ma bonne action du jour: aider Barry, un gentil papy, à changer son pneu après avoir crevé sur la route ! Mais il m'a dit que pour me remercier il allait m'offrir sa spécialité, le BARRYS NAPF à son restaurant ce soir ! Hâte d'y gouter.

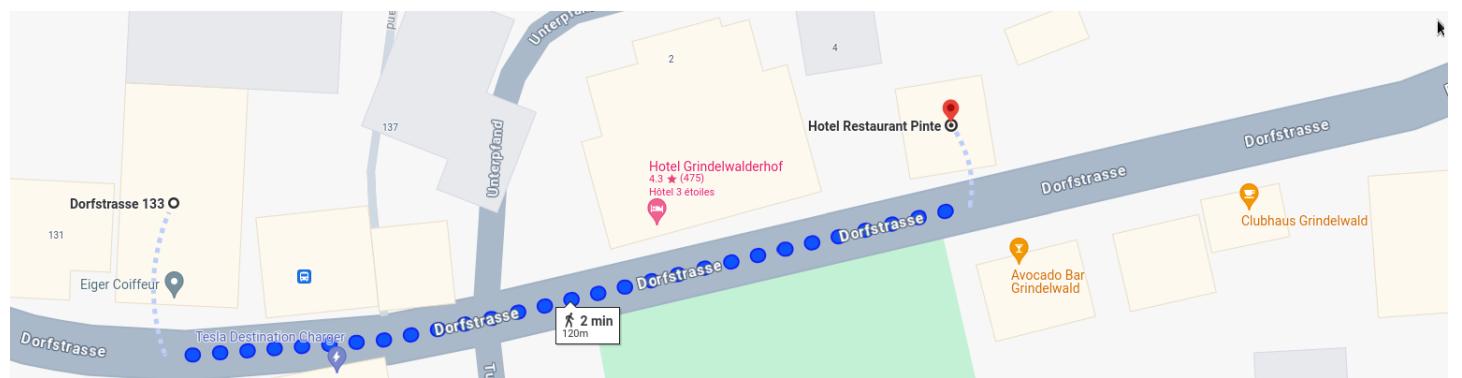
Et un message plus récent :

Heureusement que j'ai une belle vue depuis ma chambre (et seulement à 100m du restaurant de Barry !) en dépit du bruit du bar d'en face ! Ca fait plusieurs jours que j'arrive pas à dormir ! Les murs sont si fins, j'arrive même à entendre le serveur qui m'a servi mon repas ranger ses tables. Je vais devoir investir dans des boules quies si je veux bien dormir pendant mon séjour..

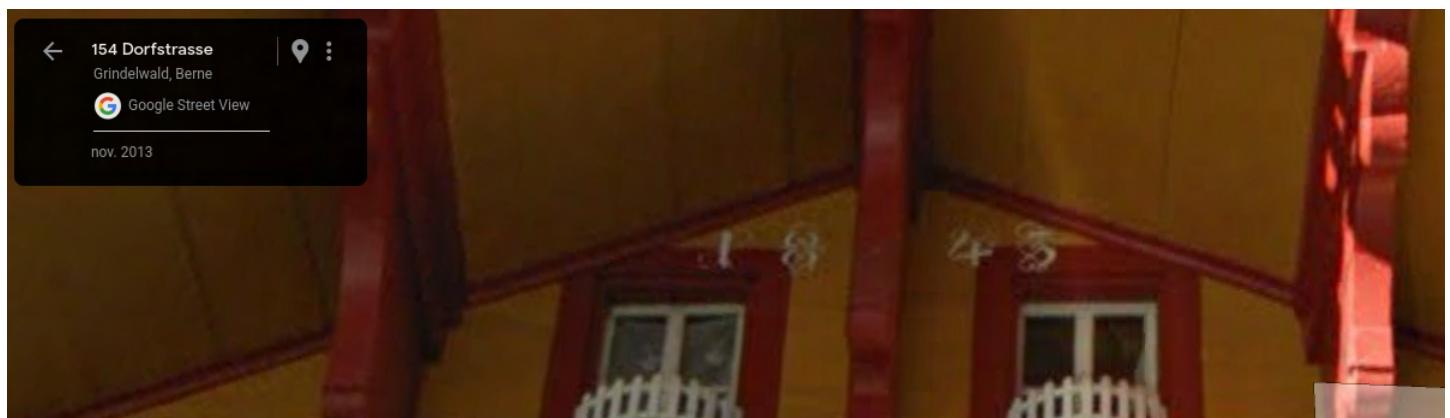
En recherchant “BARRYS NAPF”, on arrive assez vite au restaurant [Barrys au Dorfstrasse 133, 3818 Grindelwald, Suisse](#). On sait ensuite que l'hébergement d'Arina est à 100m du restaurant Barrys et qu'il y a un bar en face. On définit un rayon de 100m sur [CalcMaps](#).



L'hôtel-restaurant Pinte est dans ce périmètre :



Et il y a bien une date sur la façade de l'hôtel :



Flag - Un abri temporaire

1.33 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 Andrejew Vladlen ?

Andrejew Vladlen • 3rd+
Software Engineer
France
Experience: Rubius, BI.ZONE, and 1 more

Posts by Andrejew

Andrejew Vladlen • 3rd+
Software Engineer
1mo

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

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

D'après un de ses tweets, on sait qu'il souhaite travailler en Europe et donc en France d'après son Linkedin. Une "cyber-security city" en France où il y aurait des crêperies ? On pense à Rennes en premier lieu. Soit la requête Overpass Turbo suivante :

```
(  
    /* Fleuristes */  
    node[shop=florist]({{bbox}});  
    /* Eglises */  
    way[building=church]({{bbox}});  
    /* On n'oublie pas la crêpe, ça écarte les restaurants classiques */  
    node[cuisine=crepe]({{bbox}});  
    /* Affiche les rues piétonnes */  
    way[highway=pedestrian]({{bbox}});  
);  
out body;  
>;  
out skel qt;
```

Andrejew habite juste au-dessus du fleuriste "Maison Tulipe" (et à côté de la crêperie Saint-Georges) !

The screenshot shows the Overpass Turbo web application. At the top, there are buttons for Run, Share, Export, Wizard, Save, Load, Settings, Help, and a search bar labeled "overpass turbo". Below the interface is a map of Rennes, France, with various streets and landmarks labeled. A blue line highlights a route or path through the city center. To the left of the map, the query code is displayed:

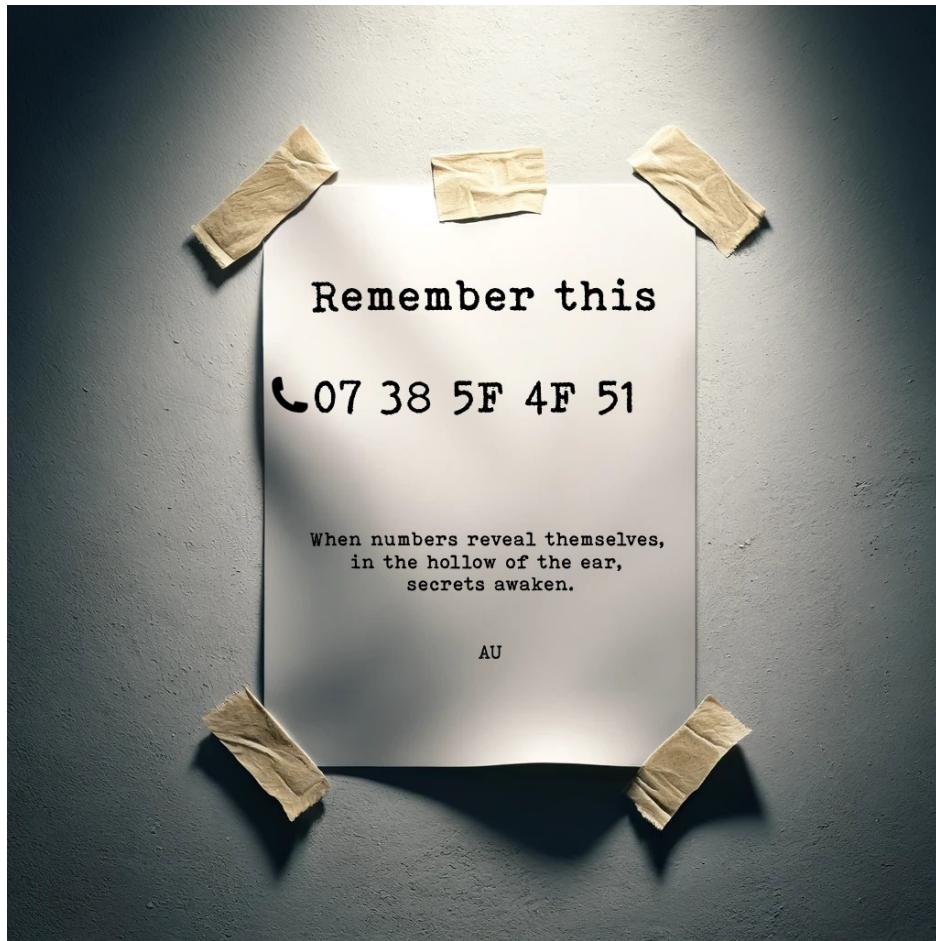
```
1  /* Fleuristes */  
2  node[shop=florist]({{bbox}});  
3  /* Eglises */  
4  way[building=church]({{bbox}});  
5  /* On n'oublie pas la crêpe, ça écarte les restaurants classiques */  
6  node[cuisine=crepe]({{bbox}});  
7  /* Affiche les rues piétonnes */  
8  way[highway=pedestrian]({{bbox}});  
9  
10 );  
11 out body;  
12 >;  
13 out skel qt;
```

A noter qu'un point rue Jules Simon au-dessus du fleuriste "Aquarelle" concorde presque avec ce script Overpass sauf qu'il est dans une rue ouverte à la circulation alors qu'Andrejew apprécie le calme.

Flag - Mise au point

1.34 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 ?



07 38 5F 4F 51 avec une citation comme en a pu en trouver chez Arina.

En plus vu le symbole, on recherche un numéro de téléphone. Un challenge où on a perdu du temps inutilement et qui aurait pu être résolu plus rapidement. Les 3 derniers nombres sont clairement en héxadécimal : convertis en décimal, cela donne un numéro non attribué. Nous avons ensuite essayé des combinaisons $5+0xF$ $4+0xF$ $5+1$ et d'autres choses : des numéros non attribués également.

Jusqu'au moment où on s'est dit "est-ce que la *totalité* du numéro n'est pas aussi en héxadécimal ?" : 07 56 95 79 81, ce n'était pas plus compliqué que ça. On tombe sur une boîte vocale qui nous donne le message suivant en [alphabet phonétique de l'OTAN](#) : BITLY/APJDROZ. On a donc un lien bit.ly/APJDROZ

Flag - 6h00

1.35 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 ?

Le lien trouvé au challenge précédent redirige vers un Proton Drive nommé **Специальная операция** ("Opération spéciale" en russe) qui contient 4 fichiers à analyser.



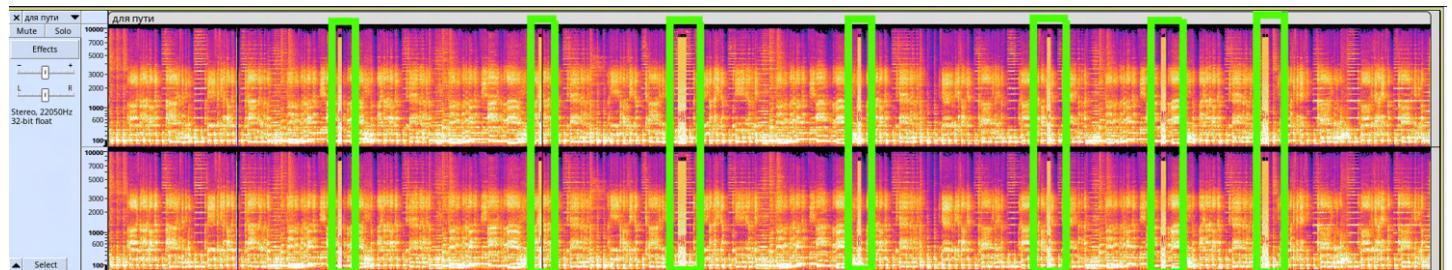
Специальная операция

End-to-end encrypted • 4 MB

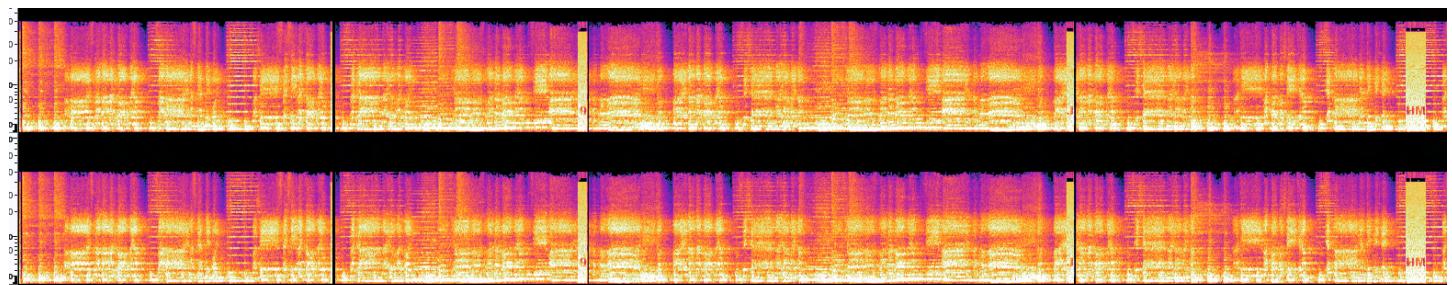
	Name ↑	Size
	для пути.mp3	2 MB
	позволяет получить доступ к месту.txt	1 KB
	Статья в прессе.png	914 KB
	Фото на память 📸.pdf	897 KB

1.35.1 для пути - Pour le chemin

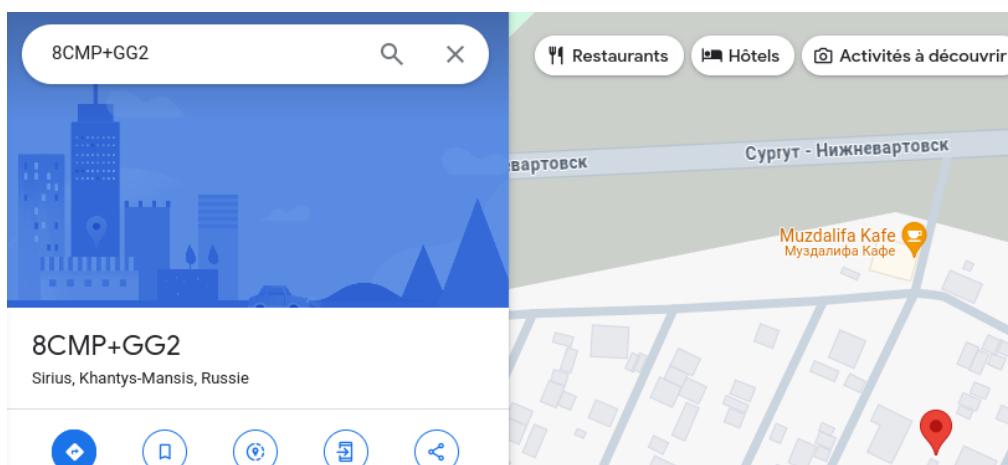
A première vue, rien dans le fichier MP3. Ceci dit, en passant dans la vue spectrogramme de Audacity, on observe quelques zones avec des motifs particuliers :



En diminuant la vitesse par 2, on observe des caractères lisibles qui nous fait penser à un Google Code : 9JHM8CMP+.



Ca nous donne un point [proche de l'aéroport trouvé plus tôt](#).



1.35.2 позволяет получить доступ к месту - Vous permet d'accéder au lieu

Traduit, on obtient des directions :

A la sortie du café, le voyage vers l'est commence, Prends la voiture qui t'attend, Passage par la réserve naturelle de la Fourmilière, un voyage sans fin. Sans s'arrêter ni reculer, pendant trente-sept kilomètres exactement, il continue, Jusqu'à ce qu'un nouveau chemin s'ouvre sur la droite.

Là, un pont apparaît au-dessus d'une rivière vivante, Reconnaissable à sa clôture rouge et brillante. Il continue, emporté par le courant, Tourne toujours à gauche puis tout droit jusqu'à ce que vous alliez là où les gens se reposent.

A proximité, une église, vous y trouverez Coin, appelle-moi quand tu y seras Nous vous attendrons au deuxième étage, Dans un immeuble où les balcons rouges scintillent.

1.35.3 Статья в прессе - Article dans la presse

Une image d'un article de journal russe qu'on a passé dans un [outil d'OCR](#) puis Google Translate dont voici quelques morceaux choisis :

Un pirate informatique soupçonné d'être impliqué dans activités terroristes contre France, retrouvé mort

il y a eu une tournure des événements a confirmé que corps sans vie découvert au loin appartenait à la forêt. le fameux cybercriminel connu : dans les profondeurs du numérique le monde souterrain comme KattZiZu, nommé Tigran Zirov.

Compte tenu de l'attendu connexions avec un groupe de hackers, impliqué dans la récente terroriste activités en France, La mort de Tigran soulève questions troublantes.

les organismes d'application de la loi actuellement enquêtent sur les circonstances mort de Tigran, mais détaillée information publique non fourni. Dans la déclaration Service de police le sérieux est souligné situation et contenu appelle à la minutie. enquête sur les événements menant à la mort de Tigran.

On comprend qu'un certain Tigran Zirov a été impliqué dans les affaires terroristes qui nous intéressent dans cette enquête et que celui-ci est décédé.

1.35.4 Фото на память - Photo pour mémoire

KOLYMBABYTE DESTRUCTIVE MALWARE AND INTERNATIONAL CYBER ATTACKS

Computer intrusion, conspiracy, intentional damage to a protected computer, satellite system intrusion.



GOLUBOV Sviatoslav



VALDEN Andrejew



TIGRAN Zhirov (†)



UVAROVA Arina



WEN Ch'ien

L'avis de recherche du FBI où on retrouve Andrejew, Arina, Wen (l'ex-employé de Stella) et Tigran. Un nouveau venu : Sviatoslav Golubov qu'on suppose être le chef.

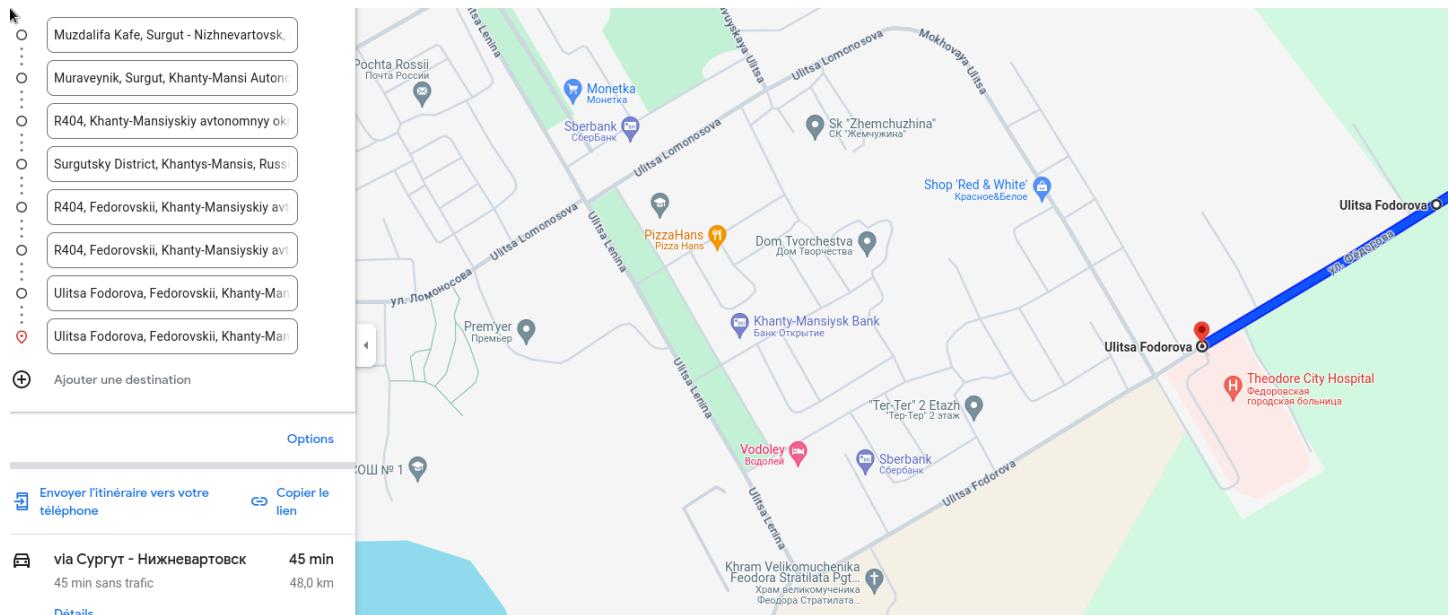
Flag - La dernière pièce du puzzle

1.36 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 ?

On utilise le Google Code et les instructions trouvées dans le challenge [La dernière pièce du puzzle](#). On suit les différentes instructions pour arriver dans la ville de [Fedorovskii](#) :



A partir de là, on a dû relire ligne par ligne les instructions et on a également eu une aide des admins alors qu'il ne nous restait plus qu'un essai :

jusqu'à ce que vous alliez là où les gens se reposent.

Nous avons cru pendant longtemps qu'il s'agissait de l'hôtel [Vodoley](#), les gens s'y reposent. Alors qu'en fait, il s'agit de l'hôpital à l'[entrée de la ville](#).

A proximité, une église, vous y trouverez

Une [église orthodoxe](#) est bien là.

Nous vous attendrons au deuxième étage, Dans un immeuble où les balcons rouges scintillent.

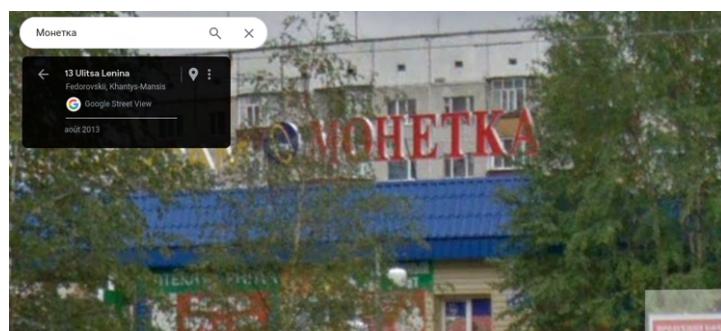
Un immeuble aux balcons rouges est dans le quartier, on y reviendra plus tard.

Coin, appelle-moi quand tu y seras

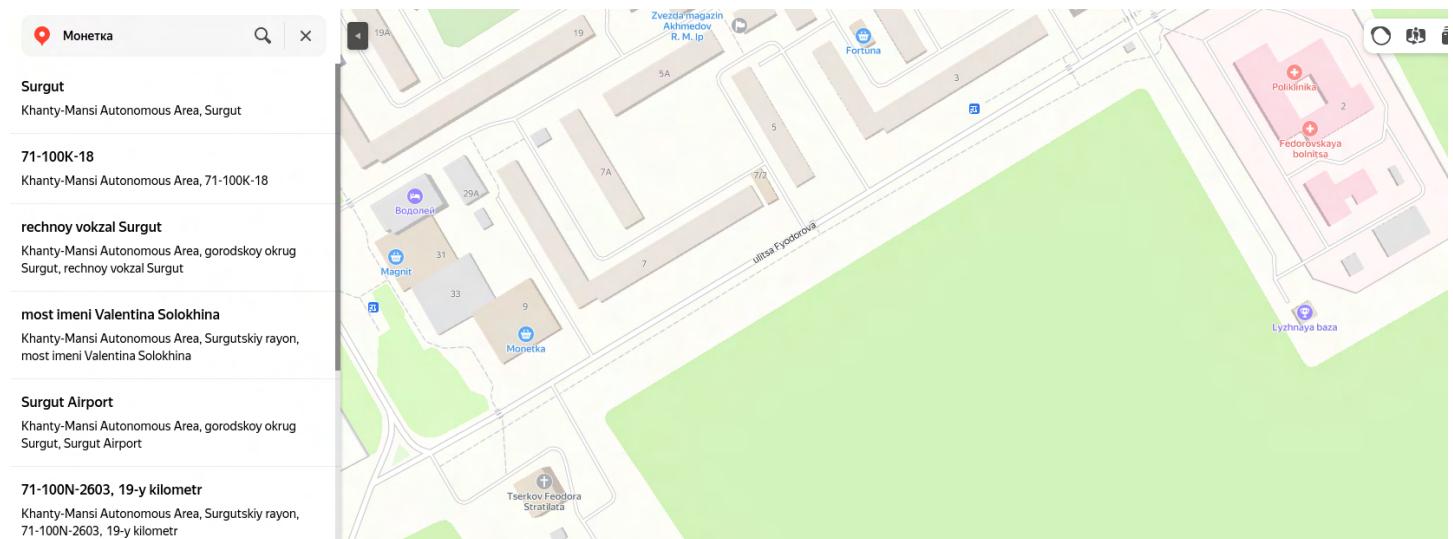
On a longtemps ignoré cette phrase. "Coin" ne veut rien dire en l'état, le mot original dans le texte russe est **Монетка** qui peut être traduit par "Pièce de monnaie" :



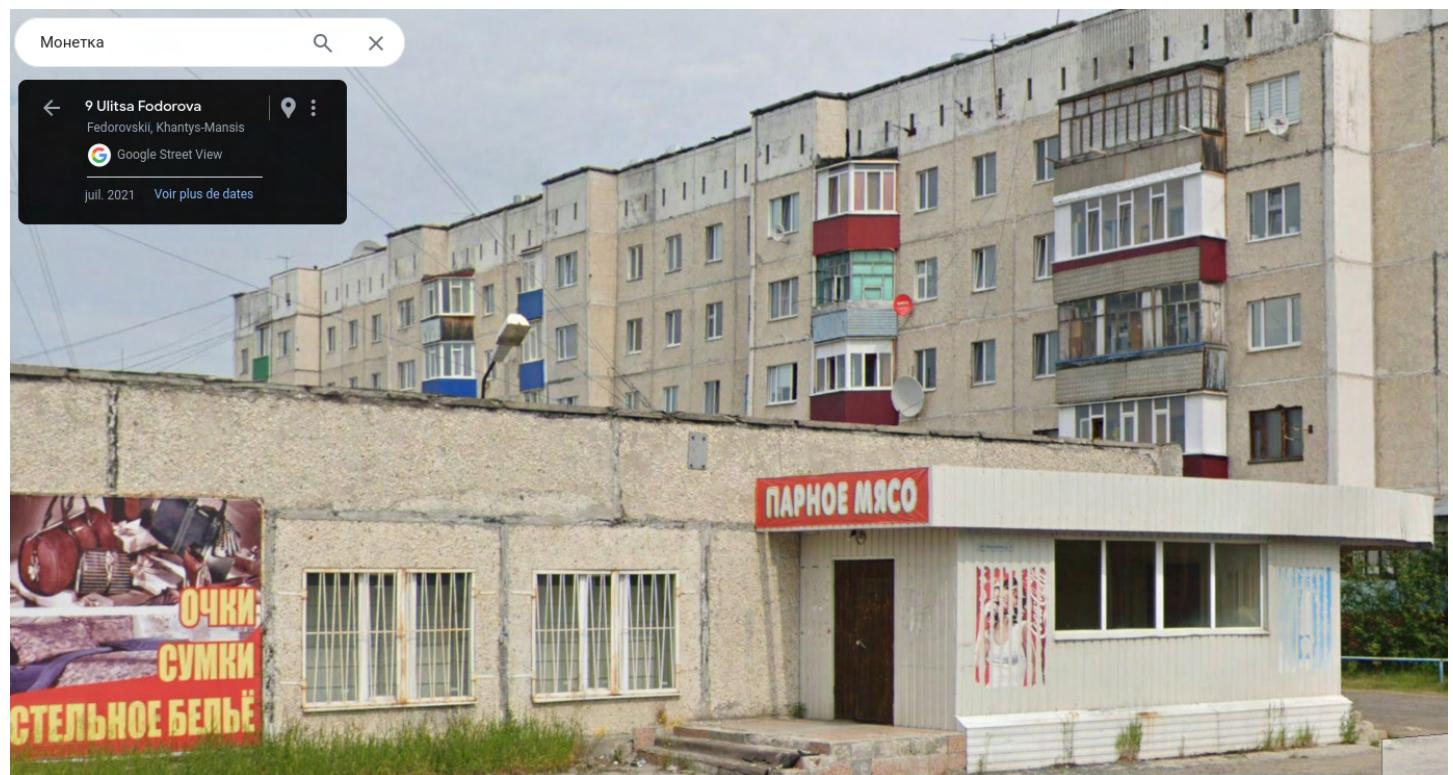
Il y a bien une banque Sperbank dans le quartier mais rien de particulier. Par contre, en cherchant directement le mot russe dans Google Maps, on trouve un résultat plus intéressant :



Монетка est en fait un supermarché/épicerie mais qui nous éloigne encore plus de l'église et de l'hôpital. La recherche sur OpenStreetMap ne nous donne rien de plus... Jusqu'au moment où on s'est aperçu d'un truc : la photo Street View date de 2013. Et si il y avait un autre **Монетка** ailleurs depuis ?



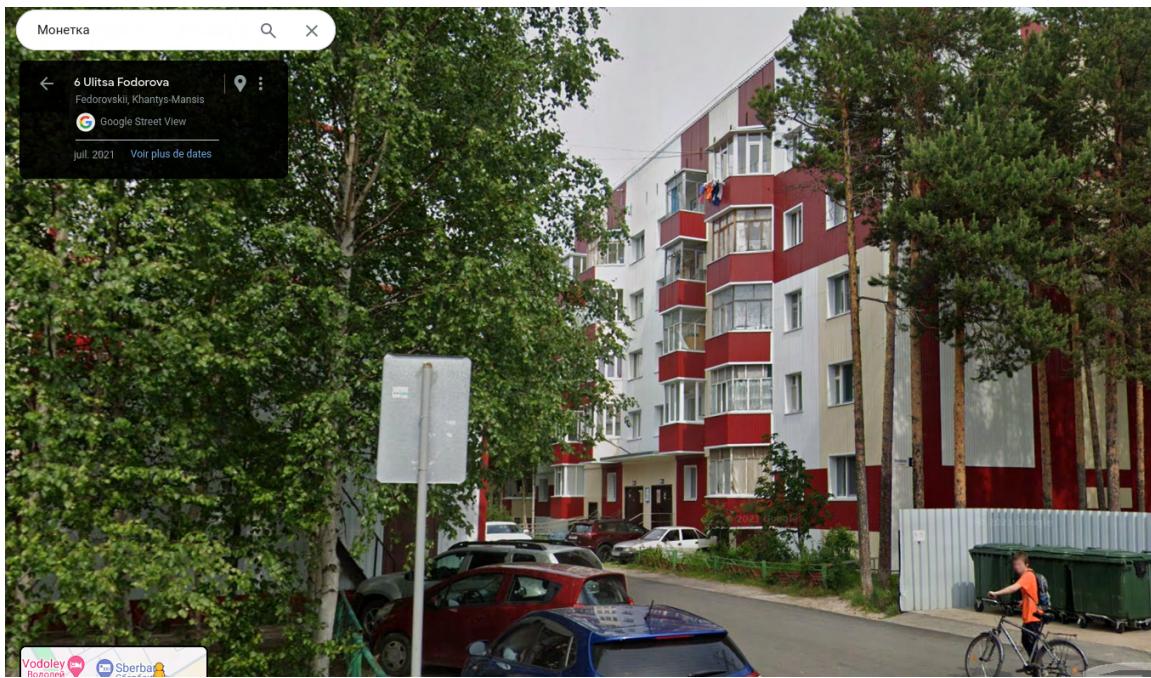
La réponse est en fait oui, juste en face de l'église... “Etrangement”, Yandex Maps (moteur de recherche russe) est plus facilement à jour que Google ou OpenStreetMap.



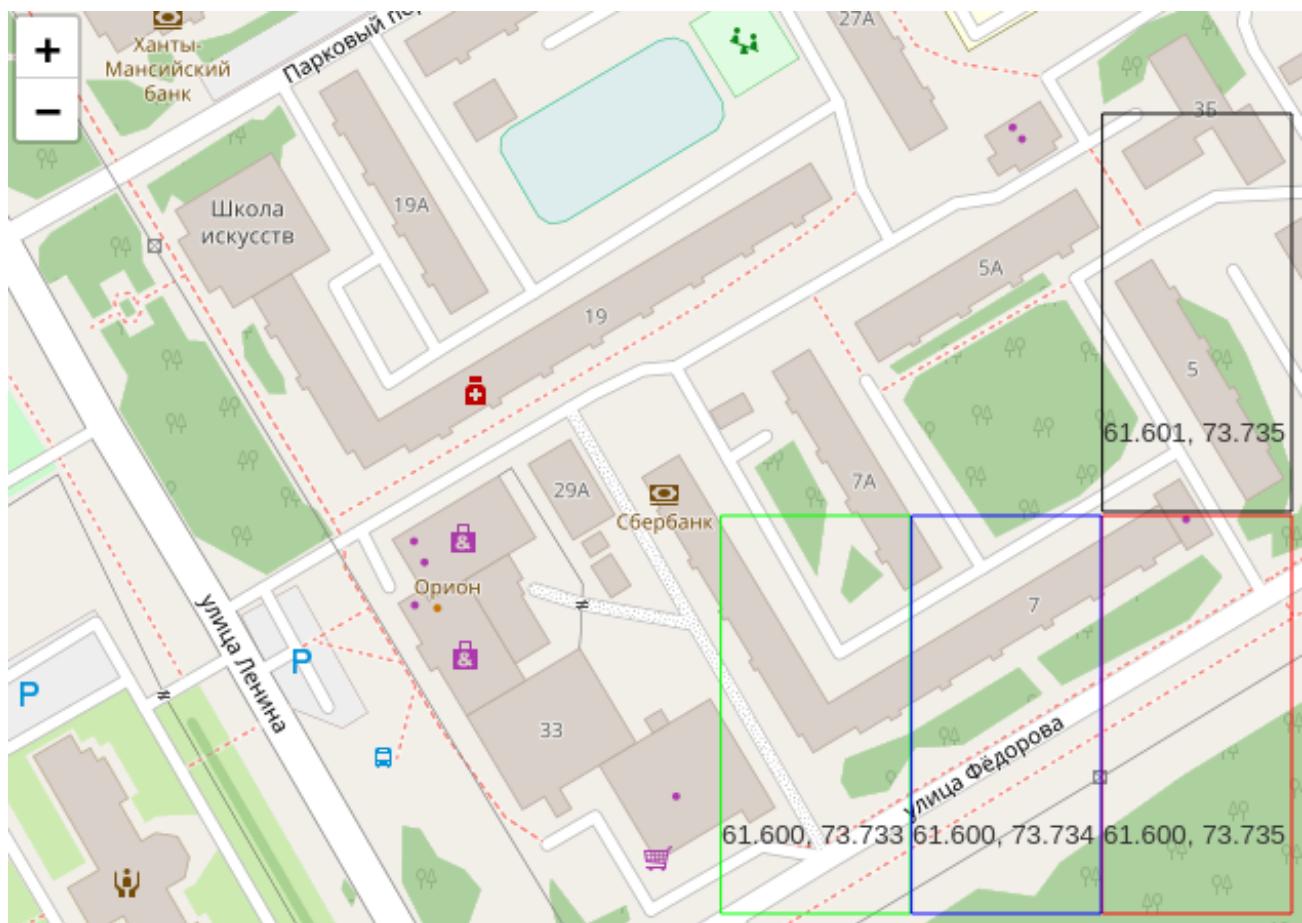
Il y a bien un immeuble avec des balcons rouges juste en face du bloc où est l'épicerie tant recherchée. On suppose donc qu'une personne est capable de surveiller depuis le balcon qui arrive à l'épicerie. Pratique pour récupérer un rendez-vous.

1.36.1 Micro-remarque

A peine plus loin, il y avait un immeuble avec des vrais balcons rouges qui “scintillent”.



Avec Folium, on a refait un quadrillage avec les coordonnées des différentes zones :



- L'immeuble avec les balcons rouge plus ternes est en 61.600, 73.333.
- L'immeuble plus récent est en 61.601, 73.735.

L'immeuble récent nous semblait convenir aux instructions données. Mais ce n'est qu'ensuite que nous avons retrouvé la position réelle et actuelle de l'épicerie **Монетка** qui rendait le choix plus logique.

Flag - Lieu secret

1.37 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 ?

Mes chers amis,

Le jour où ce satellite entrera en collision avec notre ennemi commun restera gravé dans l'histoire et nos noms resteront gravés à jamais dans la mémoire collective. Merci à chacun d'entre vous pour votre participation dévouée à ce projet. Je vais me rendre pendant un moment dans un endroit secret que je préfère garder secret. J'espère que vous utiliserez également ce temps pour vous-même.

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 à K4m3n3v, rappelez-vous, si le satellite s'écarte de la trajectoire prévue et menace notre patrie, utilisez la touche stop pour tout abandonner, corrigez l'orbite et redémarrez le programme.

Si vous avez oublié la clé : Au nom de celui qui a construit le mausolée du chef réside le pouvoir d'arrêter la tempête.

n'oubliez pas : bow/4ec0ce6db63dd91893187c4c2348dc2c1008d6443014da4dab569e3e4d724ceb/

Le pseudonyme est directement indiqué dans la lettre traduite.

Flag - Opération spéciale

1.38 La tête dans les étoiles

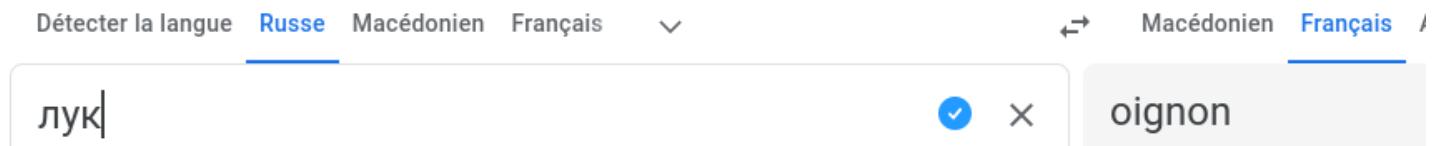
Après avoir analysé la lettre, vous obtenez des informations précieuses.

Quel est le nom du satellite infecté ?

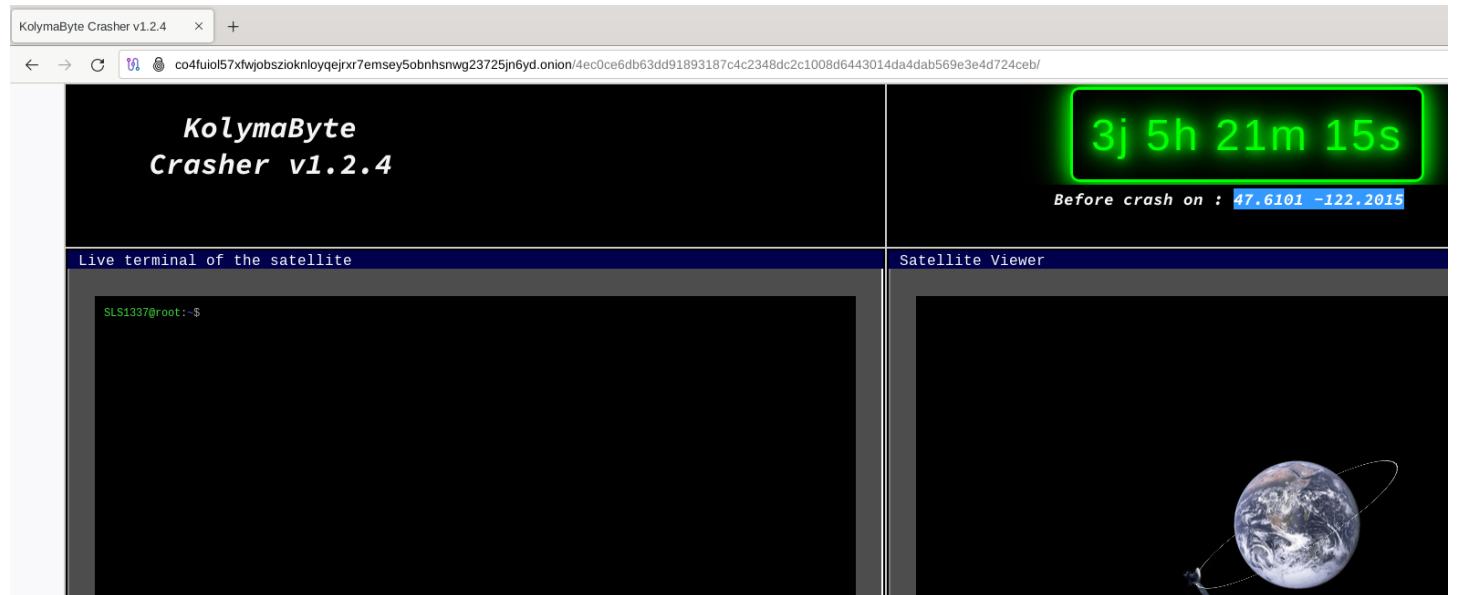
On touche au but ! La lettre ne contient pas d'informations qui nous sautent aux yeux, sauf la dernière ligne :

n'oubliez pas : bow/4ec0ce6db63dd91893187c4c2348dc2c1008d6443014da4dab569e3e4d724ceb/

Une suite de caractères en hexadécimal et un mot **bow** qui n'a a priori pas de sens. Ayant été embêté un certain temps avec le problème de traduction sur le nom de l'épicerie, on essaye de traduire uniquement le mot russe.



Oignon ? Comme TOR ? La chaîne de caractères est en fait juste le chemin d'une page sur le site TOR de KolymaByte.



Flag - La tête dans les étoiles

1.39 Arrêt net

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 ?

D'après le screenshot du KolymaByte Crasher, le satellite s'écrasera sur un point près de Seattle, il faut arrêter ça ! Rappel de **Opération spéciale** :

Si vous avez oublié la clé : Au nom de celui qui a construit le mausolée du chef réside le pouvoir d'arrêter la tempête.

Le chef étant Lénine, on cherche alors celui qui a construit son mausolée. En essayant cette clé dans le terminal du KolymaByte Crasher :

```
SLS1337@root:~$ help
Available commands: help, cd, ls, resume-crash, stop-crash
SLS1337@root:~$ stop-crash
Please use : stop-crash key
SLS1337@root:~$ stop-crash Chtchoussev
[i] Decipher the key
[i] Search the key on remote satellite
[i] Compare key
.
.
.
.
.
.
.
[+] keys matchs !
[i] Malware is still active but inofensif
[i] If you want to resume, please run : resume-crash
[-] Exit code : 0x95BF4A
```

Flag - Arrêt net

1.40 Echec et mat

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.

[...]

Flag : **finish.**

RAS.

Flag - Echec et mat

1.41 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 ?

Le challenge qu'on a gardé pour la fin car il était en bonus. On doit se rappeler du challenge **Un bon bol d'air** : on cherche a priori un élément emblématique de la Suisse. Il se trouve qu'il y a une vache au niveau du belvédère.



Autres points de vue : [1](#), [2](#) et [3](#).

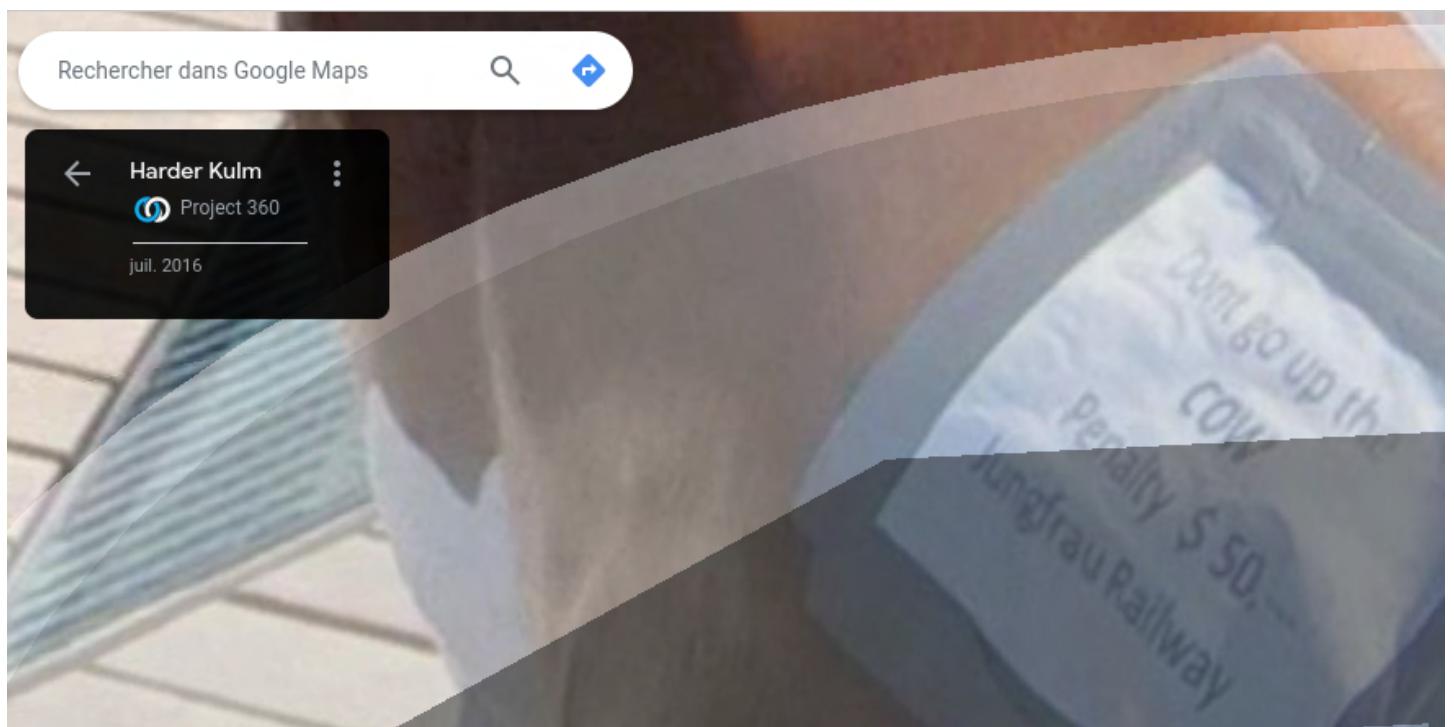
Après avoir parcouru les différents faits divers liés à des vaches et des cloches en Suisse (et il y en a), on a regardé d'un œil plus attentif les photos sur StreetView :



Il est écrit "Don't sit on the cow". L'amende correspondrait donc à ce qu'on doit payer si on monte sur la sculpture. Malheureusement, pas de prix ici... Sur une autre photo, on s'aperçoit que l'étiquette est différente.



On s'est alors mis en tête de fouiller toutes les photos visibles sur Google Maps autour de la vache pour en trouver une de juillet 2016.



Flag - Sur les traces de l'amende helvétique

2 Conclusion

Команда благодарит организаторов за этот великолепный CTF !

3 Flags

3.1 Flag - Introduction

lu et accepté

3.2 Flag - Une communication inquiétante

compris

3.3 Flag - La lettre

_Tr0tsk1

3.4 Flag - Une inattention ?

Andrejew Vladlen

3.5 Flag - La piste de l'emploi

Rubius

3.6 Flag - Coding

pastebin

3.7 Flag - Python

russian_roulette

3.8 Flag - Petite baie

K4m3n3v

3.9 Flag - Here comes a new challenger

Prevot Julien

3.10 Flag - You have been h4ck3d !

KolymaByte

3.11 Flag - Infiltration Virtuelle

WebShellUploadV3

3.12 Flag - Update your system !

4.3.2

3.13 Flag - Crypto

0.0000000035

3.14 Flag - Signature

v3n3m4K

3.15 Flag - L'entreprise sous attaque

Stella Launch Solutions

3.16 Flag - Mise en orbite

Matilda Beck

3.17 Flag - Énigmes des ondes

Dux1u

3.18 Flag - Un bon ami

Zhijang

3.19 Flag - L'Identité Révélée

Ch'ien Wen

3.20 Flag - Entrée secrète

ReverseShellWebV1.1

3.21 Flag - Command and Control

1.1.3

3.22 Flag - Une politique non respectée

admin123

3.23 Flag - Trafic dissimulé

co4fuiol57xfwjobszioknloyqejxr7emsey5obnhsnwg23725jn6yd.onion

3.24 Flag - Revente

6.997

3.25 Flag - Monnaie virtuelle

0xCec4748becc7eC74214cA0BD**b3bC8DDAf68D4108**

3.26 Flag - Achat

0xee70bdE4Bc29F2491b8aeF671298E0bA73D3eF52

3.27 Flag - La clé financière

Arina_Uvrv

3.28 Flag - La Traque Financière

Arina Uvarova

3.29 Flag - Sous le ciel d'adieu

USRR

3.30 Flag - Un bon bol d'air

Unterseen

3.31 Flag - Altitude

46.554, 8.005

3.32 Flag - Un abri temporaire

1843

3.33 Flag - Mise au point

9 Rue du Chapitre, 35000 Rennes

3.34 Flag - 6h00

bit.ly/APJDROZ

3.35 Flag - La dernière pièce du puzzle

Golubov Sviatoslav

3.36 Flag - Lieu secret

61.600, 73.333

3.37 Flag - Opération spéciale

L3n1n3

3.38 Flag - La tête dans les étoiles

SLS1337

3.39 Flag - Arrêt net

0x95BF4A

3.40 Flag - Echec et mat

finish

3.41 Flag - Sur les traces de l'amende helvétique

50