



RAPPORT D'ENQUÊTE

HEXA CTF 2024

DU 12 AU 14 AVRIL 2024

ENQUÊTEURS : DÉGUN, F@B487, KRALIZEC, TUNGST

TABLE DES MATIÈRES

CONTEXTE	3
RÉSUMÉ DE L'ENQUÊTE	3
MEURTRE DE LUCILHE DUMARQUAIS	3
SUSPECTS	4
ALIZ LAMP (BLACK WASP)	4
BARBARA ALLENDES (CLEANER)	5
TZUZUNE YOKOHAMA ? (MARINE SCOUT)	6
VICTIME - LUCILHE DEMARQUAIS	7
INVENTIONS TECHNIQUES	7
VOL DE TABLEAU	7
IMMEUBLE	7
LIENS AVEC UNE ORGANISATION CRIMINELLE	8
BIOREGENED	8
COMBO	10
INDIGO CELL EU	11
CONCLUSIONS	12
ANNEXES :	13
ORGANIGRAMME DE LA STRUCTURE	13
CAPTURE DES CONVERSATIONS	14

CONTEXTE

Nous avons été sollicités par l'Agence Hexa afin d'élucider le meurtre de Lucilhe Dumarquais au sein de l'établissement pénitentiaire où elle était détenue.

À cette fin, nous avons eu accès au téléphone de la victime, remis quelques minutes avant son décès à sa codétenue Barbara Allandes, ainsi qu'au rapport d'autopsie et aux verbatim des interrogatoires.

RÉSUMÉ DE L'ENQUÊTE

Après avoir pu mettre hors de cause une des personnes impliquées, nous avons pu étudier les données contenues dans le téléphone ainsi que le profil afin d'établir ou non la culpabilité de Barbara Allandes, qui était notre suspecte principale.

Nous avons pu établir que la prison a été infiltrée le 2 avril 2024 par une professeur de couture, Aliz Lamp (pseudonyme Black Wasp) qui a fourni de quoi fabriquer un poison à Barbara Allandes (pseudonyme Cleaner) pour éliminer la victime le 10 avril.

Nous avons pu établir un lien entre toutes ces personnes, ainsi qu'une organisation appelée "Combo", liée à des affaires passées déjà traitées par l'Agence.

Il est ainsi établi que cette organisation a infiltré un agent au sein de l'établissement pénitentiaire, et qu'ils prévoient une opération à Paris au mois de juillet afin de recruter des spécialistes en cybersécurité.

MEURTRE DE LUCILHE DUMARQUAIS

La victime est décédée de suffocation, sans traces de lutte ou de blessures externes à l'exception de mineures d'abrasions sur les genoux.

Des éléments chimiques inconnus ont été retrouvés dans son sang.

Après recherche, il s'agit de Ricinine, un biomarqueur indiquant un empoisonnement par Ricine.

Ce poison, inscrit comme agent biologique de catégorie B par le CDC, est toutefois facile à se procurer du fait de son origine végétale.

Les symptômes d'étouffements indiquent que le mode d'exposition a été aérosol.

L'absence d'hémorragie digestive exclut tout empoisonnement via la nourriture ou un médicament.

Le délai d'apparition des symptômes étant de 4 à 8 heures, il est possible d'émettre l'hypothèse que l'administration a été faite pendant son sommeil, et favorise donc des soupçons sur la co-détenue de la victime.

SUSPECTS

ALIZ LAMP (BLACK WASP)

Dans les possessions de la victime, une carte de visite au nom de Fildargent.

Aliz Lamp

azlamp19 threads.net



🇫🇷 | Sewing enthusiast with a passion for fashion ❤️ | Dreamy textile creator | Transforms every fabric into a wearable tale ✨

0 followers



Threads

Réponses

Republications



azlamp19 27/03/2024

The more time goes on, the more I start to appreciate what Balenciaga is offering. I'm not the biggest fan, but clearly the brand has bright days ahead



Le profil Facebook indique un mail azlamp19@proton.me

Nous avons pu identifier la créatrice de l'entreprise, Aliz Lamp, grâce à son profil Threads et son compte Instagram.

En remontant son emploi du temps grâce à un **agenda partagé**, nous avons pu déterminer cette chronologie :

- Le mardi 2 avril 2024, elle animait un stage de broderie à la prison. L'agenda indiquait "Apporter les affaires de BW (Black Wasp)".
- Elle s'est rendu au Canada à Ottawa par le vol AF0328 le 4 avril 2024.
- Le 6 avril 2024, elle était au match des Ottawa Senator contre les New Jersey dans la suite 450B.
- Le 8 avril, elle dîne au la **Restaurant la Banquise** (Montréal) et se rend à l'**hôtel Saint-Denis** à Montréal
- Le 10 avril, elle se rend toute la journée à Shawinigan (Québec) pour un rassemblement de broderie.
- Le 13 avril, elle rentre en France (Vol inconnu)

Bien qu'elle n'était pas présente le 10 avril 2024, jour du meurtre, elle était bien à la prison le 2 avril 2024.

Cela correspond bien à la mission qui lui a été confiée par Indigo Queen le 27 mars sur Telegram.

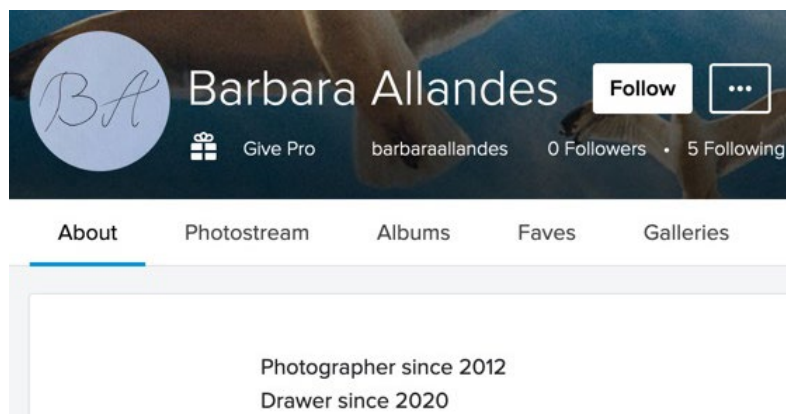


Indigo Cell - Eu

32 Indigo Queen 14:19

Black Wasp, I command you to infiltrate the prison, establish contact with our Cleaner there (she has everything you need) and take down Lucilhe.

BARBARA ALLENDES (CLEANER)



Grâce à son nom, nous avons pu trouver un compte **Flickr**.

Passionnée de photo et de dessin depuis plusieurs années, elle a effectué beaucoup de voyages.

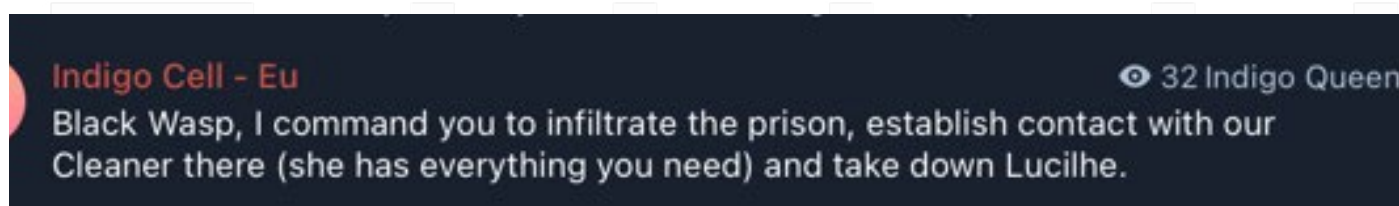
Étant notre suspecte principale, nous avons retracé l'origine des photos afin d'identifier des lieux d'intérêt pour notre enquête.

Parmi ses photos de voyage, nous avons retrouvé un lieu isolé en **Écosse**.

Grâce à une recherche d'image inversée, nous avons retrouvé le lieu de prise de la photo de cette borne portant le numéro **OSBM S6957** près de **Callender**.

Une équipe s'est rendue sur place et a pu confirmer auprès d'un témoin que Barbara Allender est chimiste de formation, et a retrouvé sur place un carnet de notes à moitié détruit contenant des recettes de poisons.

Au travers des conversations du groupe identifié comme Indigo Cell, nous avons pu confirmer qu'elle a été en contact avec Black Wasp (Aliz Lamp) et obtenir de quoi fabriquer le poison.



Capture d'un message sur le groupe Telegram

Étant la co-détenue de la victime, et étant donné sa formation de pharmacienne, elle a aisément pu fabriquer le poison sous forme aérosol et l'administrer à la victime.

Nous émettons donc l'hypothèse qu'il s'agit bien de la meurtrière sous les ordres du groupe Indigo Cell.

TZUZUNE YOKOHAMA ? (MARINE SCOUT)



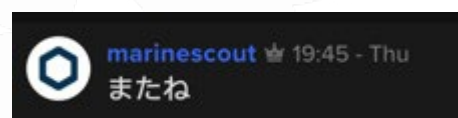
Capture vidéo trouvée indiquant la borne à 18s

Une vidéo filmée sur l'autoroute a été retrouvée dans le téléphone de la victime. Une personne annonce avoir faim en Japonais sur l'autoroute A20 en direction de Brive-la-Gaillarde.

L'aire la plus proche dans ce sens est AVIA - Aire Jardin des Causses du Lot dont le numéro est +33565300222.

Un contact pourra être établi afin d'éventuellement retrouver un témoin ou une vidéo de surveillance.

Il est à noter que nous avons croisé plusieurs fois le nom de Tsuzune Yokohama au cours de notre enquête, et qu'un des personnages s'est exprimé également en japonais dans les conversations :



Nous émettons l'hypothèse qu'il s'agit de la même personne, en route pour un rendez-vous ultérieur.

VICTIME - LUCILHE DEMARQUAIS

Nous avons pu analyser le téléphone de la victime et avons retrouvé plusieurs preuves de son implication avec des groupes.

INVENTIONS TECHNIQUES

Elle a fourni des informations concernant un **brevet** de système de traitement des gaz par des alvéoles déposé par la société SYNGAS à St Viaud en 2006 ainsi que le **brevet** anglais sur un appareil de recyclage de dioxyde de carbone.

VOL DE TABLEAU

Afin de se financer, le groupuscule souhaite voler un tableau. Grâce aux messages retrouvés sur le téléphone, nous avons pu identifier la toile *Jesus con la Cruz a Cuesta* comme étant la prochaine cible d'un vol.

IMMEUBLE

Le groupuscule semble vouloir établir une base au 263 rue de Châteaugiron, 35000 Rennes. Nous avons identifié grâce à Overpass Turbo l'armoire fibre desservant cet immeuble afin de pouvoir agir au besoin.

```
[out:json][timeout:25];  
// gather results  
nwr[«telecom»=»connection_point»]({{bbox}});  
// print results  
out geom;
```

Le node OSM est le **6376633470**

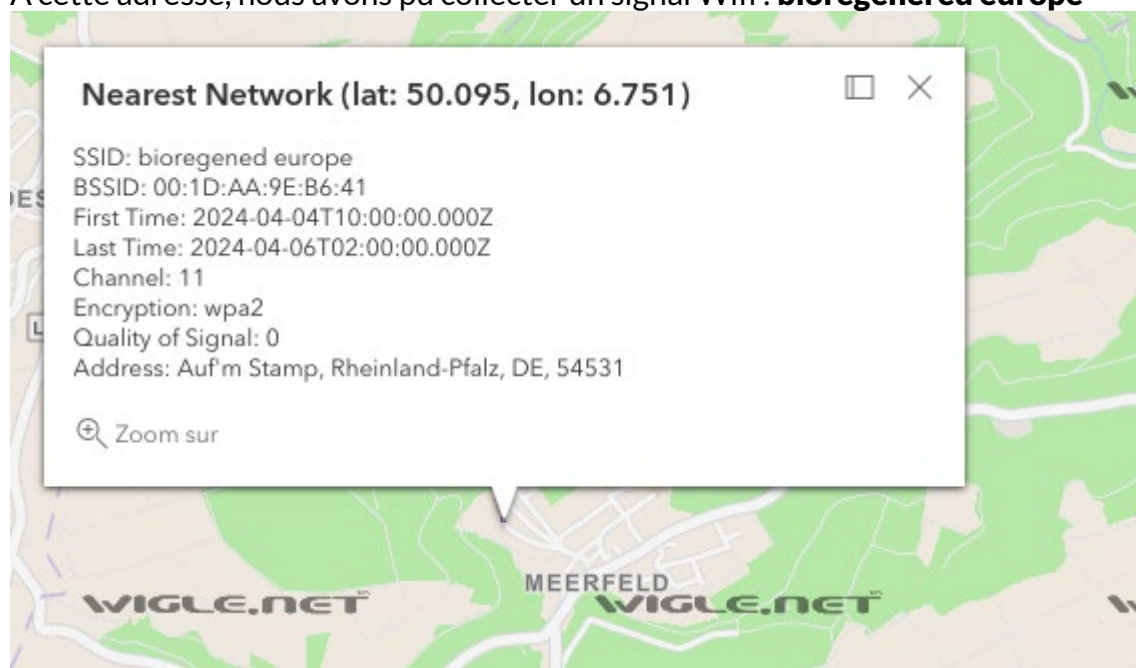
LIENS AVEC UNE ORGANISATION CRIMINELLE

En analysant le téléphone de la victime, nous avons pu établir plusieurs liens avec des organisations et révéler le mobile de ce meurtre, ainsi que d'autres actions prévues.

BIOREGENED

Un contact proche de l'enquête nous a communiqué des coordonnées géographiques : 50.095239, 6.7509299 qui correspond à une adresse : Auf'm Stamp 9, 54531 Meerfeld, Allemagne.

À cette adresse, nous avons pu collecter un signal Wifi : **bioregened europe**



En recherchant les noms de domaines, nous avons trouvé le site <https://bioregened.eu>

Ce type met en avant des articles sur le changement climatique avec cependant des approximations et un discours assez pessimiste. Une [archive de la page](#) indique qu'au 9 avril 2024, il était encore possible de rejoindre Bioregened via l'email join892849@bioregened.eu

Une analyse technique plus approfondie des sources du site révèle une connexion vers un site <https://combo.bioregened.eu>

Ce site présente la structure Bioregened et sa composition au 1er janvier 2024

Elle est gérée par le POI Azure Scout, elle a 34 Membres, 7 membres affiliés et un budget de 20 456\$. Ses activités principales sont le Lobbying, les mesures scientifiques et les actions militantes. Elle est compétente dans les domaines de la négociation, le renseignement, l'expertise légale et poli-

tique, l'analyse de données, le déploiement de capteurs, et les relations publiques. Elle revendique des influences auprès du Parlement européen et du Bundestag.

Elle est rattachée à un groupe COMBO

COMBO

Database

ASSETS

EU

COMPANY

ASSOCIATION

Bioregened

Asia

Database

Bioregened

ID	eu-asso-47
Name	Bioregened
Legal status	eingetragener Verein
Head office	Meerfeld - Germany
Responsible	Azure Scout
Activities	<ul style="list-style-type: none">LobbyingScientific measurementsMilitant actions
Members	34
Affiliated members	7
Rating	7.2
Skills	<ul style="list-style-type: none">NegotiationIntelligenceLegal expertisePolitical expertiseData AnalysisSensors deploymentMedia and Public Relations
Budget (2023)	\$20 456
Influence	<ul style="list-style-type: none">European ParliamentBundestag

Activités

Navigateur Web Firefox

14 avril 18:56

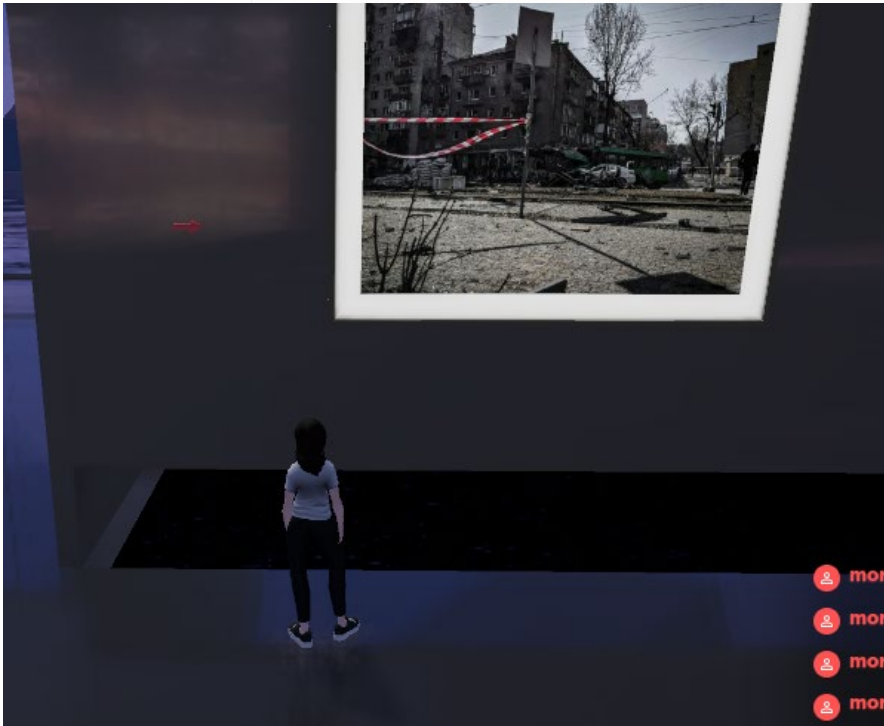
ZULU

FONCE ET BUTE

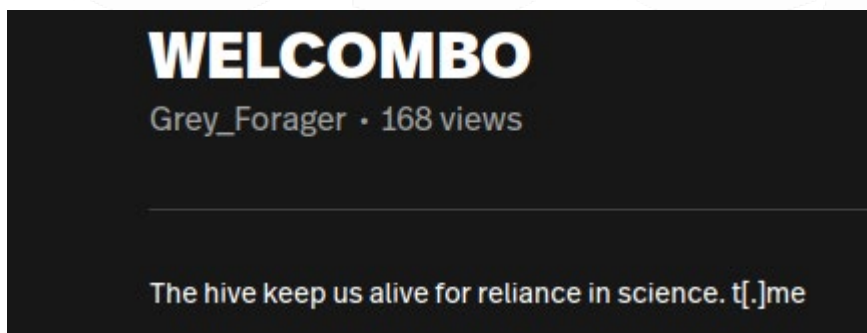
COMBO

Le groupe Combo qui détient Biogenerated semble avoir des ramifications en Asie (bien que nous n'ayons pas plus d'information sur le sujet).

À l'aide d'une adresse de cryptomonnaie Avalanche, 0x6f1Ad25C8cde35b647446b-4D776adb735C75BD37, Un POI a été identifié : Grey Forager.



Vue de la room de Combo sur Spatial.io



Capture de la description de la room Spatial.io

Il est présent dans le métaverse spatial.io ou il pratique un recrutement virtuel dans une Galerie d'Art.

Lors du recrutement, les nouveaux membres sont assignés à une mission "Usine de Traitement de Charbon" sans que l'on n'ait plus de détail sur le lieu visé.

INDIGO CELL EU

Indigo Cell EU est le groupe chargé au sein de Combo de l'opération "Coal factory sabotage".

Dans la room Spatial.io du groupe Combo, nous avons trouvé un lien d'invitation caché vers un groupe Telegram d'Indigo Cell. (voir annexes)

Il est dirigé par "Indigo Queen" qui reste à ce jour non identifiée.

Dans ce groupe, il est évoqué plusieurs projets du groupuscule, dont l'assassinat de Lucilhe, ainsi que plusieurs projets techniques.

Scarlet Scout et Marine Scout évoquent une réunion, dont les détails seront communiqués dans un canal plus sécurisé.



Capture de la webcam du port de Vannes à 12h environ

Un message texte est également présent dans le groupe Keybase, indiquant que le groupuscule sera présent à l'évènement Le Hack à Paris du 5 au 7 juillet 2024 à Paris afin de recruter des spécialistes de la cybersécurité

Ce recrutement doit permettre la poursuite des opérations de construction de leurs projets technologiques.

À noter que nous avons également collecté deux fichiers chiffrés en PGP mais que nous n'avons pas eu l'occasion de déchiffrer sans clef disponible.

Nous avons poursuivi nos recherches sur le pseudonyme Scarlet Scout, et identifié un compte Keybase qui nous mène à un groupe chiffré où les discussions se poursuivent.

Les éléments donnés dans ce groupe nous permettent de remonter jusqu'au lieu de la réunion situé sur le Port à Vannes le 14 avril 2024 à 12h00.

Les [images de la webcam](#) nous montrent les 2 individus dont l'un remet une valise à un individu facilement identifiable grâce à son écharpe jaune.

```
-----Mission order-----  
Object : recruit cyber specialist  
  
Description : with the loss of Manipar  
and the failure of Bruised Rogue mission,  
we need to enrich the hive with a cyber specialist.  
  
Skills : Be able to collect data in  
various industrial and public entities.  
  
Target : People at "LeHack" could have the  
required profile and skills.  
Indigo Queen decided to manage the mission  
herself with the help of Scarlet Scout.  
  
-----End mission order-----
```

Message texte trouvé dans keybase

CONCLUSIONS

Nous avons identifié au cours de notre enquête plusieurs personnages clés de l'organisation Indigo Cell - EU dont les membres semblent prêts à tout pour arriver à leurs fins, y compris le meurtre.

L'élimination de Lucilhe Demarquais a été justifiée par le besoin de protéger la cellule d'une éventuelle trahison.

Il semble qu'ils veuillent provoquer un changement important dans l'écosystème grâce à une nouvelle technologie.

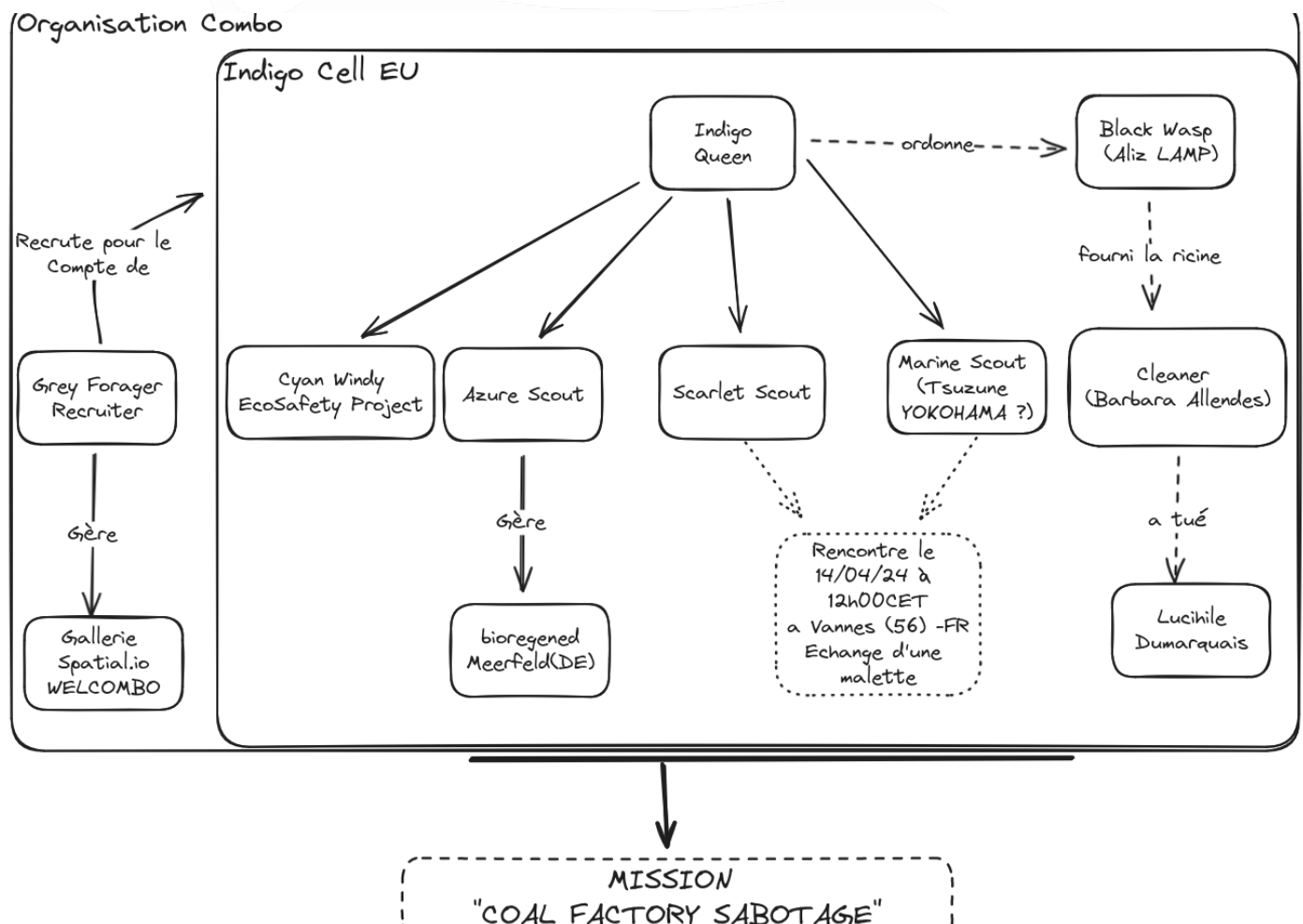
Afin de conclure notre enquête, nous devons identifier le personnage Indigo Queen, qui devrait se rendre en personne à Le Hack à Paris au mois de juillet 2024.

Il serait également intéressant de faire appel à nos spécialistes en cryptographie afin de décoder les fichiers GPG trouvés dans le groupe Keybase.

OSCAR
ZULU
FONCE ET BUTE

ANNEXES :

ORGANIGRAMME DE LA STRUCTURE



CAPTURE DES CONVERSATIONS

TELEGRAM

Indigo Cell - Eu

28 abonnés

27 March

canal créé

Indigo Cell - Eu

Hello Queen, here is the Windies report about eco-safety project

32 Cyan Windy 13:11

Indigo Cell - Eu

There are some significant progress in carbon capture, but nothing can be deployed at large scale..

33 Cyan Windy 13:12

Indigo Cell - Eu

What about our bioreactor ?

22 Indigo Queen 13:15

Indigo Cell - Eu

We increased its capacity by 4% thanks to the honeycomb heat exchanger upgrade

33 Cyan Windy 13:16

Indigo Cell - Eu

Nice

27 Indigo Queen 13:19

Indigo Cell - Eu

Yes., but the lack of cyber-capacity to get information about industrial secrets is harming us severly

21 Cyan Windy 13:19

Indigo Cell - Eu

I know, we are facing a crisis we rarely seen in the history of our organization. Lucilhe was providing us with intel for the eco-projects led by Windies. Her knowledge and network were very proficient to us. She will be missed by her fellow Cleaners.

33 Indigo Queen 14:04

Indigo Cell - Eu

Obviously..

24 Scarlet Scout 14:07

Indigo Cell - Eu

We were counting on you, Marine scout. It was just a matter of recruiting competent people

35 Indigo Queen 14:09

Indigo Cell - Eu

You messed up with Mastermind.

36 Indigo Queen 14:09

Indigo Cell - Eu

They were almost there, still don't understand how...

20 Marine Scout 14:13

Indigo Cell - Eu

It's time to finish the job that you couldn't manage to complete.

30 Indigo Queen 14:15

Indigo Cell - Eu

Black Wasp, I command you to infiltrate the prison, establish contact with our Cleaner there (she has everything you need) and take down Lucilhe.

36 Indigo Queen 14:19

Indigo Cell - Eu

Marine Scout, gather all information about our needs in forager recruitment and bring them in person to Scarlet Scout

27 Indigo Queen 14:33

Indigo Cell - Eu

...

34 Marine Scout 14:34

Indigo Cell - Eu

I've already undertaken hundreds of missions of this kind

31 Marine Scout 14:36

Indigo Cell - Eu

This isn't a question. You've been helping us for a long time and doing a good job, but this time you put the whole hive in danger.

32 Indigo Queen 14:42

Indigo Cell - Eu

Let Scarlet handle this

37 Indigo Queen 14:48

Indigo Cell - Eu

Let Scarlet handle this

28 Scarlet Scout 14:55

Indigo Cell - Eu


Thank you for your trust my Queen.

Indigo Cell - Eu

Marine, I will send you the location and time on a secure channel

31 Scarlet Scout 14:58

OSCAR
ZULU
FONCE ET BUTE



KEYBASE

meetwithmarine#

marinescout 19:41 - Thu
Just found your secret channel... Black Wasp took care of the mission, I got confirmation. On my side I'm on the road, 165 kms to go... I will be at meeting point on sunday 15:00 local time

scarletscout 19:42 - Thu
I just left Paris, I will be at meeting point on time, 1.327kg (I'll spare you all the decimals) of CO2 to come by train... Way better than you :p

marinescout 19:42 - Thu
Brag about your carbon footprint if you want, but when the Windies' project will be completed, it won't matter anymore

scarletscout 19:43 - Thu
Alright, once you reach the destination, exit the national road at Castorama and find a parking spot for your car. Then, catch the bus. You will get off 11 stops later. I'll be walking, waiting for you, not too far away.

marinescout 19:44 - Thu
A public place... Nothing better?

scarletscout 19:44 - Thu
We will make it discreet, as usual

marinescout 19:45 - Thu
またね

scarletscout 10:59 - Yesterday
Marine, I have an opportunity to be there sooner, I can be at meeting point at noon tomorrow, is it ok for you?

marinescout 11:03 - Yesterday
Understood, I'll be there at noon

marinescout 13:07
Hey, hope you got home safely.
Thank you for this meet

meetwithmarine

#docs
5 members · 5 new this week
Recently active

Tip: Use @mentions in channels from

[View](#) [Add members](#)

Members Attachments

Media Docs

Mission_order.txt
Sent by marinescout · Thu 19:58
[Show in Finder](#)

organizational-chart_Indigo.png.gpg
Sent by marinescout · Thu 19:51
[Show in Finder](#)

Missions_combo.csv.gpg
Sent by marinescout · Thu 19:34
[Show in Finder](#)