

Équipe : En Légende

STRANGER CASE 2023

Mission: ICARUS



Objectif : Retrouver Eric EDURT

Rappel des faits

Il y a quelques semaines, un client anonyme nous a transmis une demande d'enquête particulière.

D'après son signalement, une personne du nom d'**Eric EDURT** est portée disparue. Cet homme, éminent CEO d'une entreprise informatique liée au domaine médical, semblait, d'après notre client, très perturbé avant sa disparition.

L'objectif de notre mission est de découvrir la vérité et de comprendre ce qui est arrivé à notre cible.

Equipe

Notre équipe, En Légende, est composée de deux personnes, et de leurs sockpuppets relatifs :

- [REDACTED] aka **NozZy** - Capitaine

Le sockpuppet est [REDACTED], présent sur les réseaux sociaux sous les pseudonymes [REDACTED].

[REDACTED]

- [REDACTED] aka **Skiep**

Le sockpuppet est [REDACTED].

[REDACTED]

Constats globaux

L'entreprise Copprethia a fait preuve de censure pour cacher une activité douteuse : la revente de données médicales et personnelles. Le CEO Eric EDURT a détourné beaucoup d'argent avec cela, pour essayer de rembourser des dettes, en collaborant avec un certain Luc EFOK. Ce dernier cherchant à optimiser les profits de son entreprise Bankroot, en utilisant des informations médicales comme justificatifs de refus de prêts bancaires. Les employés ont commencé à remarquer que quelque chose se tramait, et cela à grandement joué sur le moral de l'équipe. Certains se plaignent du manque de respect, voire d'inhumanité, et certains pensent à quitter le navire.

Eric et sa société ont été victimes de représailles de la part d'un groupe radicaliste appelé Unplug. Monsieur EDURT s'est fait enlevé lundi 1er mai, alors qu'il se sentait suivi, par le groupe Unplug. Mathieu Asahara, gourou présumé de cette secte d'après une enquêtrice indépendante, sera présent sur Paris prochainement. Il y a de fortes chances que l'enquête puisse s'y poursuivre, et que Eric puisse être retrouvé.

Chronologie des éléments

Cette partie ressasse les éléments constatés et redoutés, dans les faits et les hypothèses, dans un ordre pseudo-chronologique. Les éléments de compréhension et de corrélation seront présentés par la suite.

Censure et manipulation

Copprethia est une entreprise de santé fondée en 2016, qui offre des consultations médicales à distance ou en personne.

Durant les années 2020 à 2023, des avis sont laissés sur le site de l'entreprise [Copprethia.fr](https://copprethia.fr). De nombreux avis sont positifs, mais certains dénotent un peu, et font chuter la note globale de l'entreprise. Des personnes se plaignent d'une utilisation douteuse de leurs données médicales et personnelles :

Je suis inquiet..

★☆☆☆☆ mars 19, 2020

Je suis préoccupé par le fait que mes informations d'assurance vie pourraient être utilisées à des fins non médicales

Jean

Demande douteuse...

★☆☆☆☆ janvier 30, 2023

Je ne suis pas à l'aise de partager mon numéro de sécurité sociale avec une entreprise tierce. Est-ce que c'est vraiment autorisé d'ailleurs ??

Paulette

Certains se plaignent aussi du manque de qualité du service, ou de frais excédentaires :

vol d'argent ???

★☆☆☆☆ août 1, 2022

J'ai été facturé à tort pour des services que je n'ai pas reçus

Bertrand

Manque de convivialité

★★☆☆☆ avril 27, 2022

Manque de convivialité.

Secretariat LOWCOST

Lucas

Un commentaire en particulier ressort du lot :

Contact

★★★★☆ avril 14, 2023

Bonjour,

Je suis Ange SANASORA, journaliste indépendant qui enquête sur les fraudes aux consommateurs.

Je vois beaucoup de personnes qui remontent des soucis liés aux données personnelles.

Si vous êtes concerné et/ou que vous avez des informations à ce propos, merci de me contacter sur mon adresse email : ange.sanasora@gmail.com

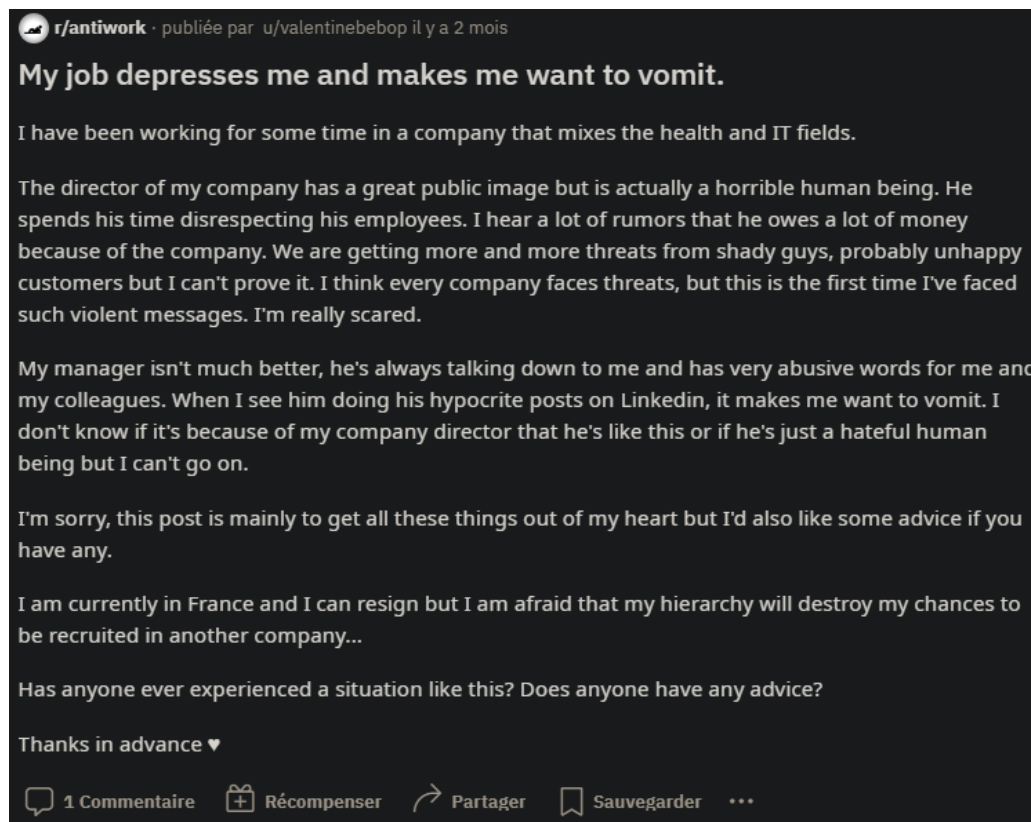
Ange SANASORA

Cela laisse donc planer de gros doutes sur cette société. Encore plus quand on sait que tous ces avis négatifs ont été supprimés de leur site, et ne sont visibles que depuis une [archive web](#).

Plainte ouverte

On a donc affaire à de la censure, et de la manipulation d'avis en ligne, ce qui est grave pour une entreprise. Sans même parler des soupçons de recel de données.

A peu près à la même période, avril 2023, une employée de Copprethia se plaint de choses graves sur [Reddit](#):

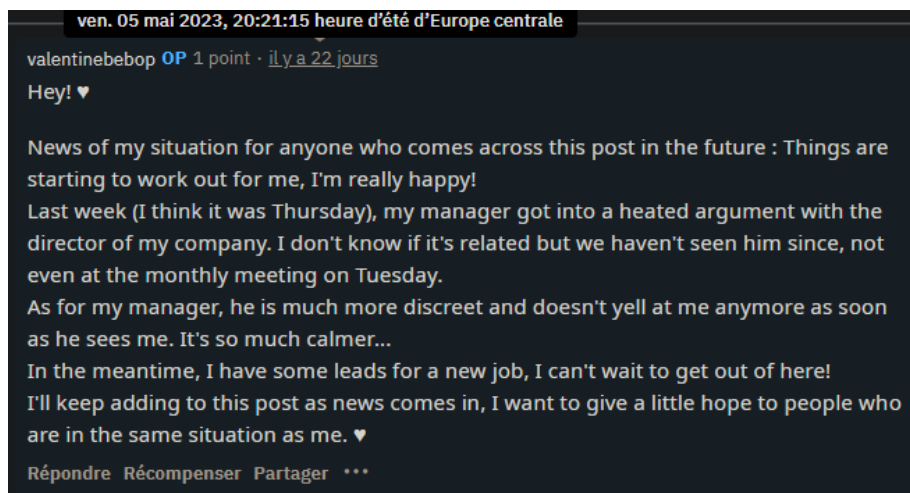


Elle dit que le CEO cache un visage bien plus horrible que celui qu'il présente en public, qu'il passe son temps à manquer de respect à ses employés, et que des rumeurs de détournement de fonds circulent à son sujet, ou plutôt que l'entreprise le rend assez riche, de manière douteuse. Elle confirme que l'entreprise reçoit des plaintes, mais aussi des menaces, de plus en plus conséquentes et violentes, et que cela l'effraie.

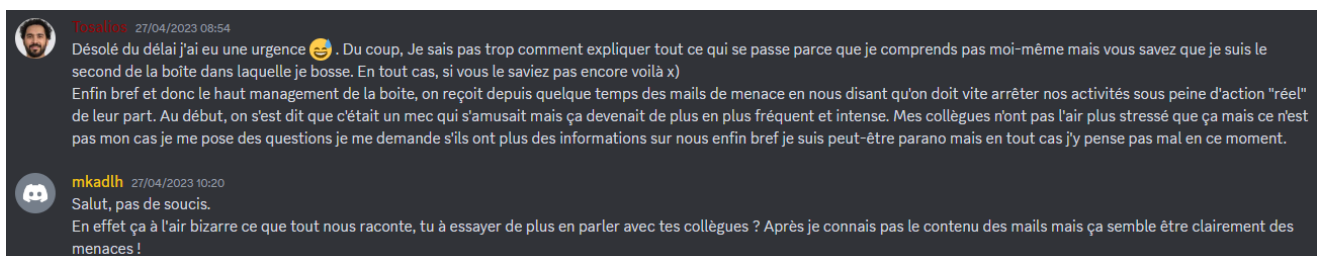
Elle se plaint aussi beaucoup de son supérieur direct, qui lui parle très mal, a un comportement abusif envers elle et ses collègues. Il semblerait qu'il poste des messages hypocrites sur LinkedIn.

Cette employée est l'assistante DRH Faye TERNI, son manager est alors le DRH Ulrich JABLONOWSKI.

Faye a par la suite publié un commentaire à son premier post, celui-ci dit que son manager et Eric ont eu une altercation le jeudi 27 avril. Depuis lors, Faye et ses collègues n'ont plus revu Eric. Aussi, les choses vont un peu mieux au boulot pour elle et ses collègues, mais à quel prix.



Cette altercation a fait du bruit chez plusieurs employés, et semble confirmer qu'une certaine tension à lieu, et cela en grande partie à cause des menaces que l'entreprise reçoit de plus en plus régulièrement.



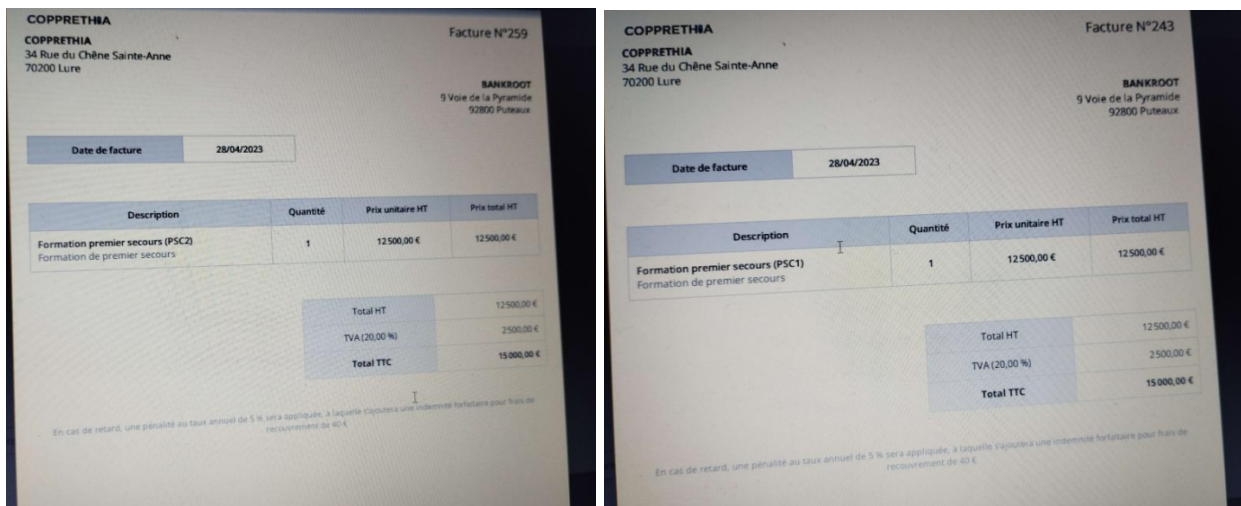
Le collègue revanchard

Le lendemain de cette altercation, vendredi 28 avril, Ulrich accède à l'ordinateur d'Eric, et récupère le lien vers son agenda privé. Ce dernier à donc accès à tout l'emploi du temps de son CEO, et décide de le partager à un groupe sectaire, qui se veut acteur d'un "débranchement". Ce groupe est appelé Unplug, et cherche à s'attaquer à l'entreprise de Eric EDURT.

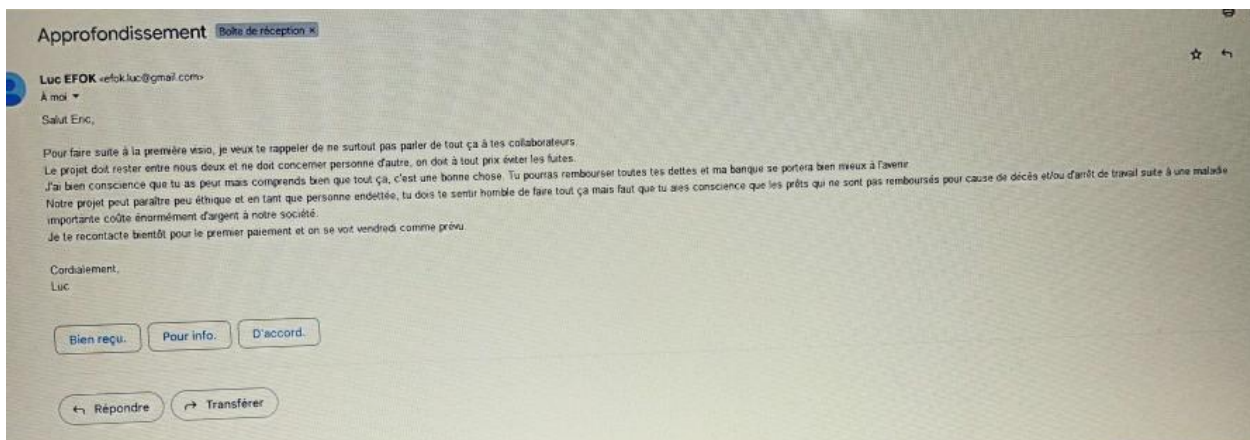


Dettes et blanchiment

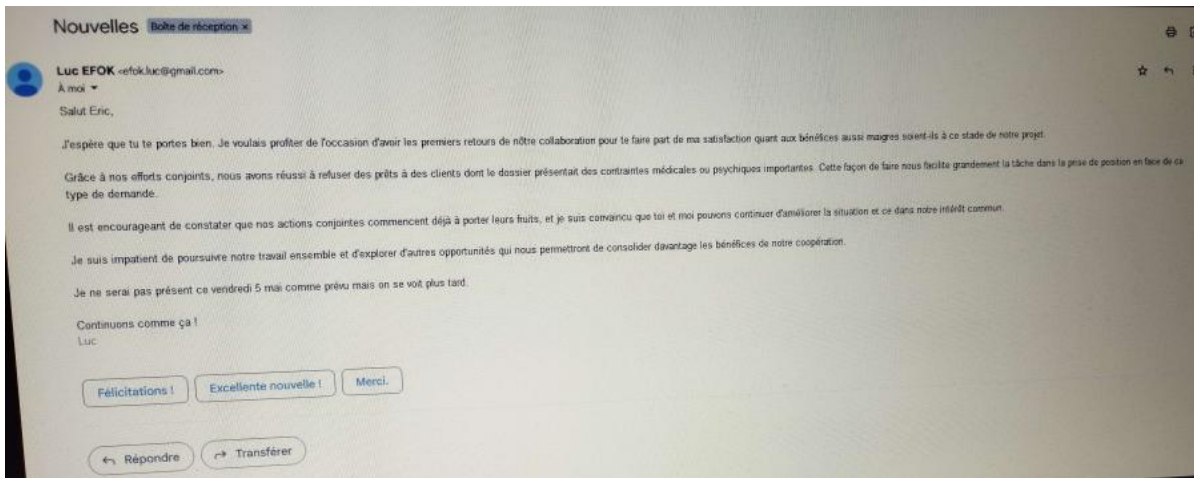
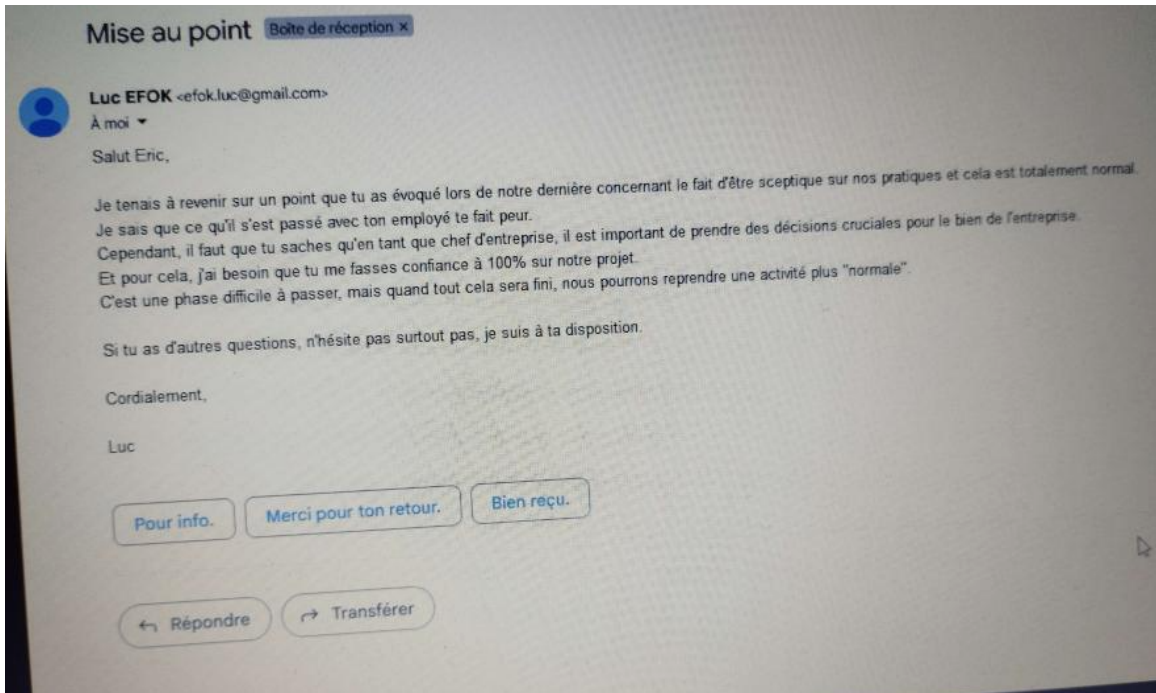
Ce même jour, le vendredi 28 avril, Copprethia émet deux factures de sommes importantes à la société bancaire Bankroot, pour des formations de premier secours PSC1 et PSC2, chacun d'une valeur de 15,000.00€.



Ces factures cachent des choses, puisque Eric a de nombreuses fois échangé avec un certain Luc EFOK, CEO de l'entreprise Bankroot, autour de sujets sensibles. Au travers des photos, on comprend que Luc profite du fait que Eric a d'importantes dettes pour lui faire conclure un marché assez sombre.



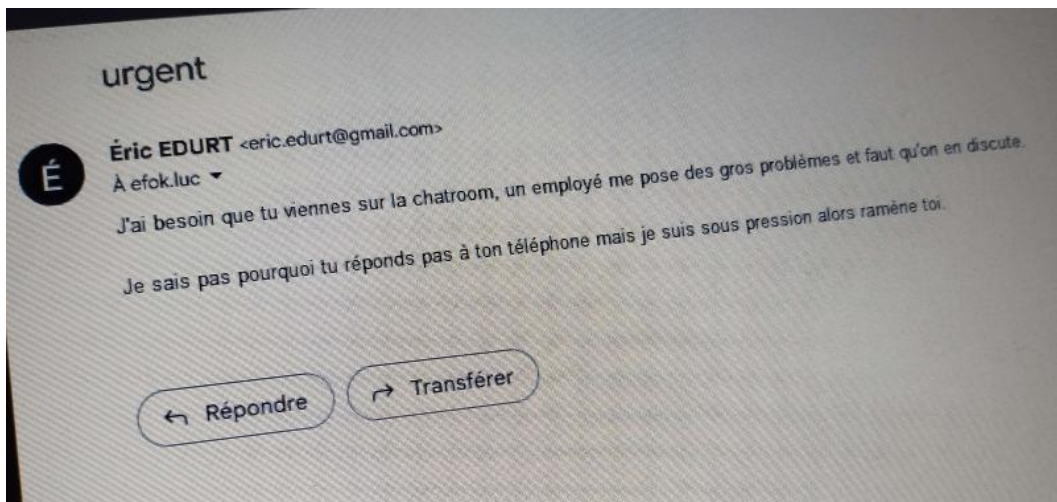
Ce qu'il se passe, c'est qu'Eric vend des données clientes confidentielles à Luc, et quant à lui, Luc utilise ces données afin de pouvoir refuser plus facilement des prêts bancaires à des personnes malades qui risqueraient de coûter cher à sa société.



Les deux ont donc une affaire illégale de blanchiment d'argent, de vente de données personnelles, et de règlements personnels sur les comptes de leurs entreprises distinctes.

Dernières nouvelles du CEO

Eric a commencé à se rendre compte que quelque chose d'autre se tramait, et il commençait à paniquer. La seule personne avec qui il pouvait échanger à ce sujet, est son complice Luc, sauf que ce dernier ne répond plus à son téléphone.

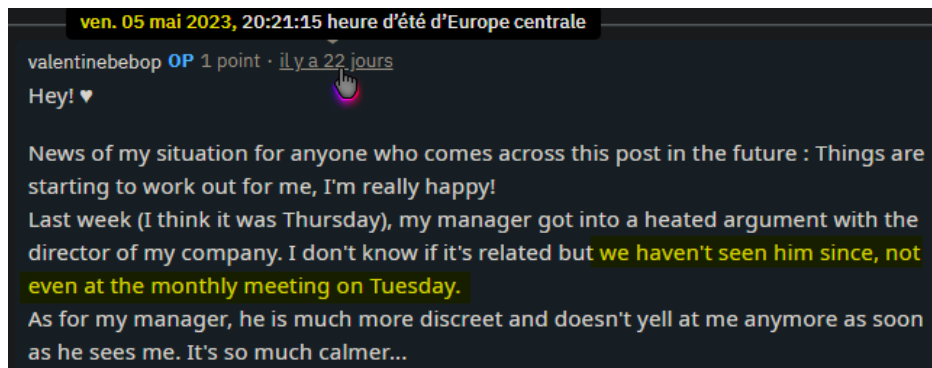
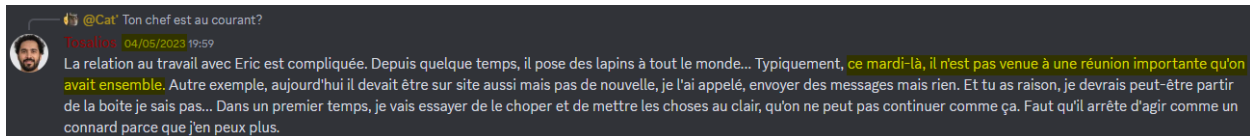


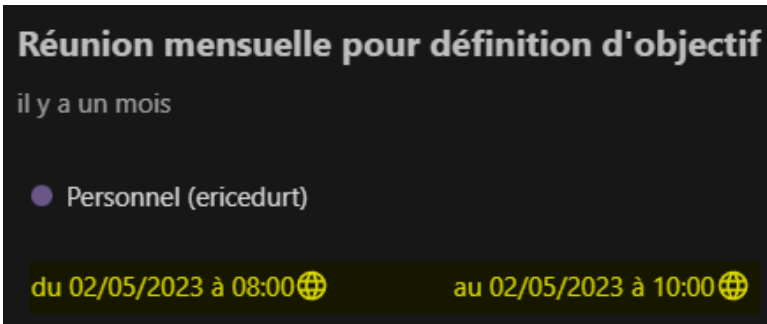
Sur son compte twitter, Eric dit qu'il se sent suivi le 1er Mai, et que ça le préoccupe.





Il s'agit des dernières traces laissées par Eric. Il ne s'est pas présenté à la réunion importante du lendemain, mardi 2 mai :

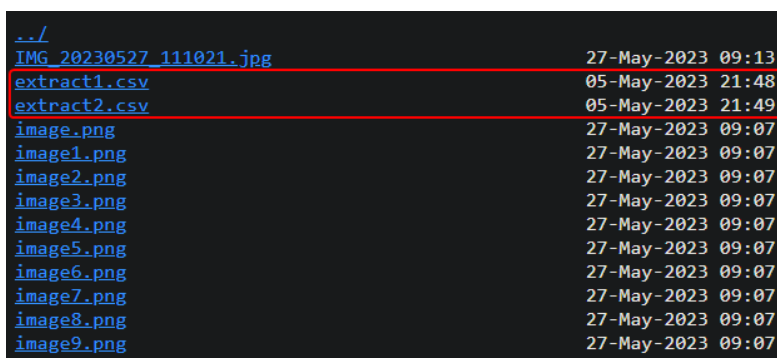




Eric disparaît donc des radars le **lundi 1er mai 2023**.

Fuite de données

Quelques jours après, le vendredi 05 mai, le groupe Unplug arrive à se procurer des données médicales de clients de Copprethia. Elles se retrouvent disponibles sur une page de leur site, dont il faut disposer d'identifiants pour s'y connecter.



Line	Tag	Nom	Prénom	Date de naissance	Numéro de sécurité social	Groupe sanguin	Maladies connues	Infos psychiatriques personnelles
1	■				99	A-	Asthme;Allergies;Diabète	-
2	■				86	AB-	Dépression;Anxiété	-
3	■				90	O-	Hypertension	-
4	■				32	O+	Migraines;Sinusite	-
5	■				94	A-	Asthme;Allergies;Eczéma	-
6	■				03	B-	Hypertension	-
7	■				94	AB+	Fibromyalgie	-
8	■				85	A+	Dépression	-
9	■				78	B-	Hypertension	-
10	■				32	O+	Acné	-
11	■				07	O-	Allergies	-

On ajoute à cela des photos d'email mis en ligne le 7 mai sur cette même page.

Des données clients ont alors bien fuité, au-delà d'avoir été vendues.

Chronologie de l'enquête

Depuis le nom de Eric EDURT, nous allons relater la manière dont nous nous y sommes pris pour regrouper ces informations, les corrélérer, et en tirer une histoire claire.

Le CEO, son entreprise, et ses employés

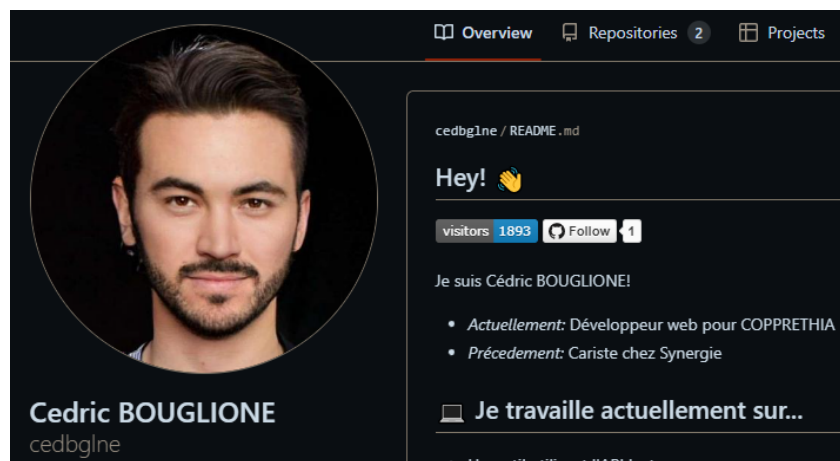
Dans l'ordre de mission, il est indiqué qu'Eric EDURT est un "éminent CEO d'une entreprise informatique liée au domaine médical". Nos recherches débutent donc sur LE réseau social professionnel : LinkedIn. Sur son compte [LinkedIn](#), Eric EDURT se présente comme le CEO d'une entreprise nommée Copprethia. On retrouve très vite sur son profil le lien de la [page LinkedIn de son entreprise](#). Nous nous sommes alors rendus sur [le site web de Copprethia](#), afin d'en apprendre un peu plus sur eux. On comprend que cette entreprise fournit des services médicaux avant toute chose, dans plusieurs villes de France, depuis 6 ans. 2 pages intéressantes composent ce site web : les [avis clients](#), et une [description](#) plus détaillée de l'histoire de Copprethia. On y retrouve une liste de huit éminents employés :



A partir d'ici, nous essayons de trouver les différents réseaux sociaux de ces personnes, ainsi que leur pseudos :

- Eric EDURT aka *eedurt_* : [Twitter](#), [Linkedin](#), [Flickr](#)
- Jade RAYNAUD : [Linkedin](#)
- Raphael MABAR aka *Tosalio(s)* : [Twitter](#), [Blog](#), Clash of Clans, Discord
- Alice BLOM : [Linkedin](#)
- Ulrich JABLONOWSKI : LinkedIn (compte disparu entre temps)
- Faye TERNI aka *valentinebebop* : [Linkedin](#), [Facebook](#), [Reddit](#)
- Hortense LUTERO : [Linkedin](#)
- Alexandre DUBAIS : N/A

En cherchant que la page Privacy-Policy de leur site web, on fait la connaissance d'un neuvième employé : Cédric Bouglione



Les réseaux trouvés pour Cédric aka *ced.bg1ne* : [Github](#), [Instagram](#). Il posséderait également un compte Snapchat, mais nous n'avons pas pu mettre la main dessus.

Premières analyses et prises de contacts

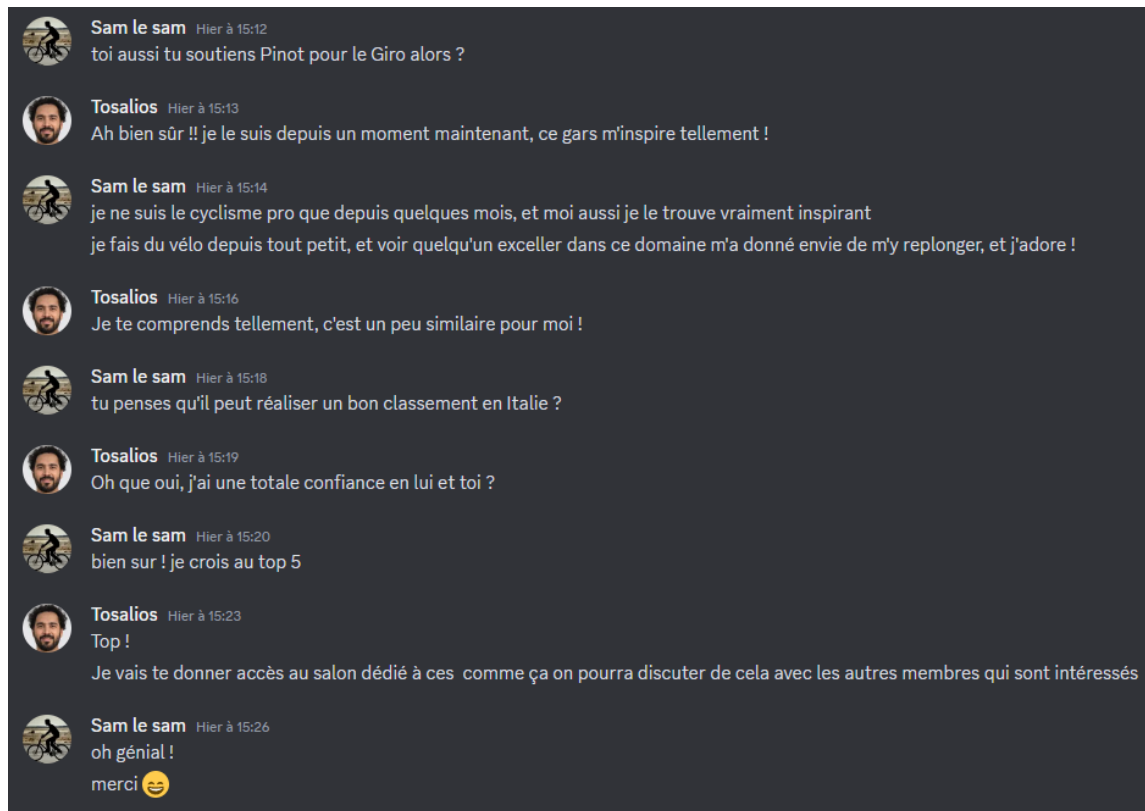
Depuis le Facebook de Faye Terni, nous trouvons son pseudo et par la suite son Reddit, compte sur lequel elle se plaint sans détour de son CEO et de son manager. Cela nous fournit un contexte de base au lore de l'enquête, mais cela n'ira pas plus loin dans cette direction. Faye ne répond pas à nos messages, peu importe la plateforme.

Sur le compte Twitter de Raphael Mabar, nous apprenons qu'il a deux passions : Clash of Clans, et le cyclisme, amateur comme professionnel. Depuis son blog trouvé sur son compte, nous trouvons deux articles sur ces mêmes sujets. L'article portant sur Clash of Clans nous apprend qu'il a une guilde ouverte à tous, et un serveur discord dédié aux membres de ce clan. Nous rejoignons donc son clan, grâce à la bannière de son compte Twitter :

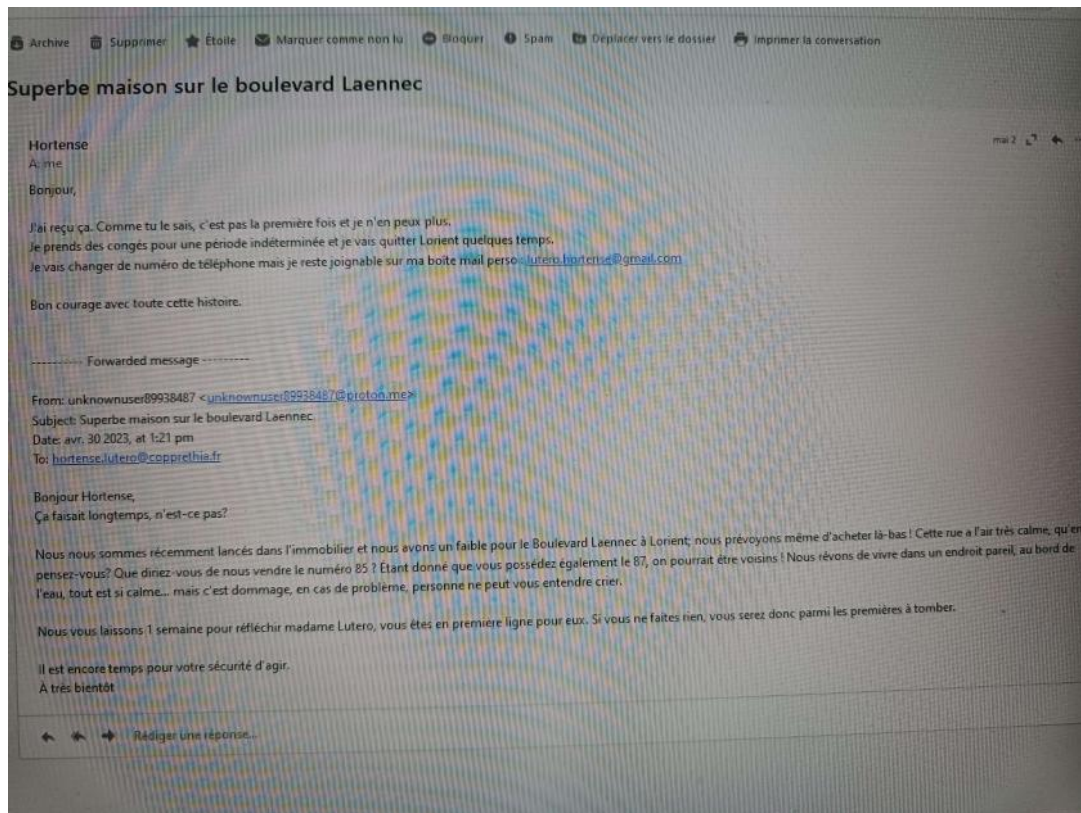


Une fois le clan rejoint, nous trouvons le lien pour le serveur discord, et le rejoignons de même. Le règlement demande à envoyer une preuve que nous avons rejoint le clan, et Raphaël nous donne alors un accès en lecture à différents salons.

On se rend ensuite compte que certaines personnes ont un rôle supérieur au nôtre : Apprenti Copain. Nous nous doutons alors qu'il faut être copain avec Raphaël pour avoir droit à ce rôle. Nous discutons alors cyclisme avec lui, en particulier autour de son cycliste préféré trouvé sur [Twitter : Thibaut Pinot](#). Nous partageons alors une passion commune, qu'il veut nous faire partager dans un salon particulier de son serveur :



Dans ce salon #le-coin-des-copains, nous avons accès aux messages de Tosalios à ses amis, à propos de son travail. Dont une photo d'un mail reçu de la part d'Hortense LUTERO, qui est gravement menacé par des inconnus :



Nous avons alors une preuve et plusieurs témoignages de menaces et de climat de tension chez Copprethia.

Une enquête déjà en cours...

En lisant les différents avis laissés sur le site, un détail a attiré notre attention : les notes étaient généralement très bonnes alors que quelques clients se plaignaient de la quantité d'informations personnelles qu'ils devaient donner lors de rendez-vous médicaux.

Informations médicales

★★★★☆ mai 1, 2021

Je suis inquiet de savoir si mes informations médicales sensibles sont protégées de manière adéquate. Cela serait bien que l'on est plus d'informations sur ce sujet.

Emmeline

En parallèle, nous avons donc essayé de trouver un historique plus ancien des avis sur le site web de l'entreprise, et nous avons trouvé une [archive web](#), datant du 04 mai. C'est ici que nous trouvons les différents commentaires négatifs supprimés du site, dont celui de la journaliste Ange SANASORA. Celle-ci laisse son mail pour que nous puissions la contacter si nous avons des informations sur Copprethia.

Contact

★★★★☆☆ avril 14, 2023

Bonjour,

Je suis Ange SANASORA, journaliste indépendant qui enquête sur les fraudes aux consommateurs.

Je vois beaucoup de personnes qui remontent des soucis liés aux données personnelles.

Si vous êtes concerné et/ou que vous avez des informations à ce propos, merci de me contacter sur mon adresse email : ange.sanasora@gmail.com

Ange SANASORA

Chose que nous avons fait par la suite. En réponse à notre mail, nous recevons rapidement une réponse automatique :

De ange.sanasora@gmail.com
À lauriers.samsam



Bonjour,

Je ne suis malheureusement pas disponible aujourd'hui mais vous pouvez vous rapprocher de ma collègue, [Marine Bly](#).

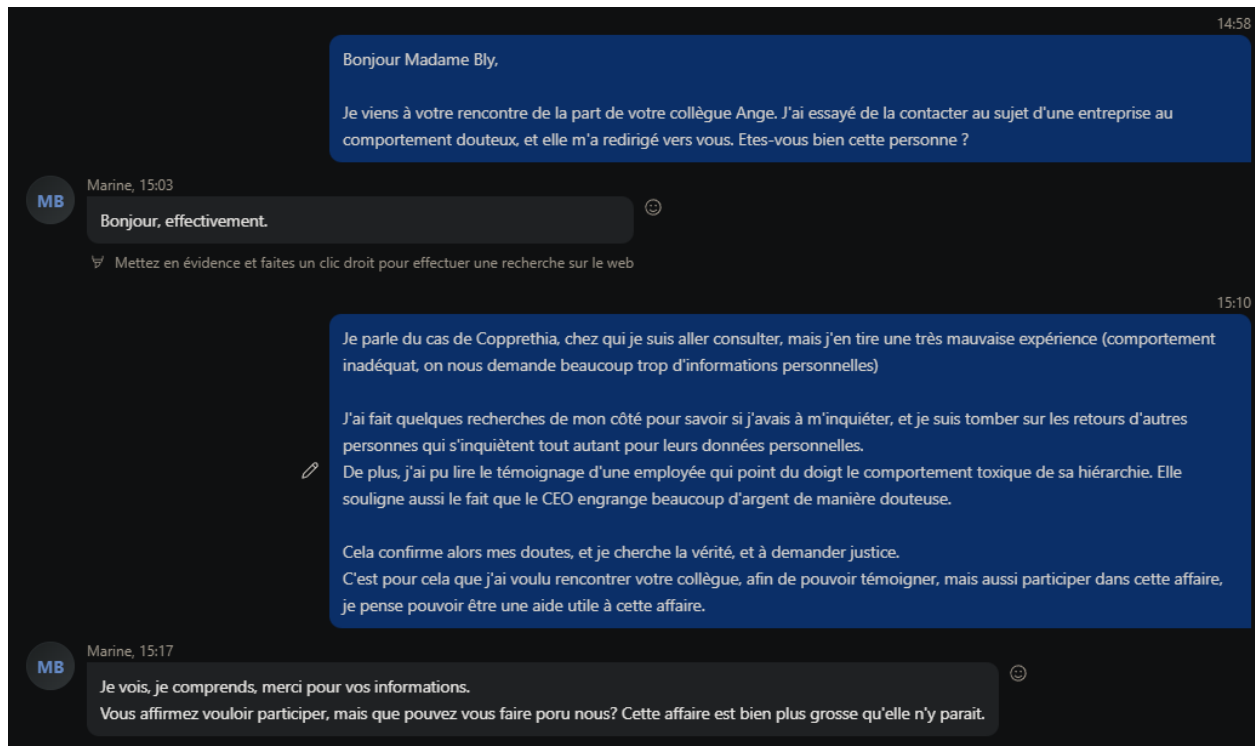
Voici son [skype : live:cid.17cd78e8f819ab3c](skype:live:cid.17cd78e8f819ab3c)

N'hésitez pas à lui dire que vous venez de ma part.

Au plaisir de collaborer ensemble.

Bonne journée,
Ange

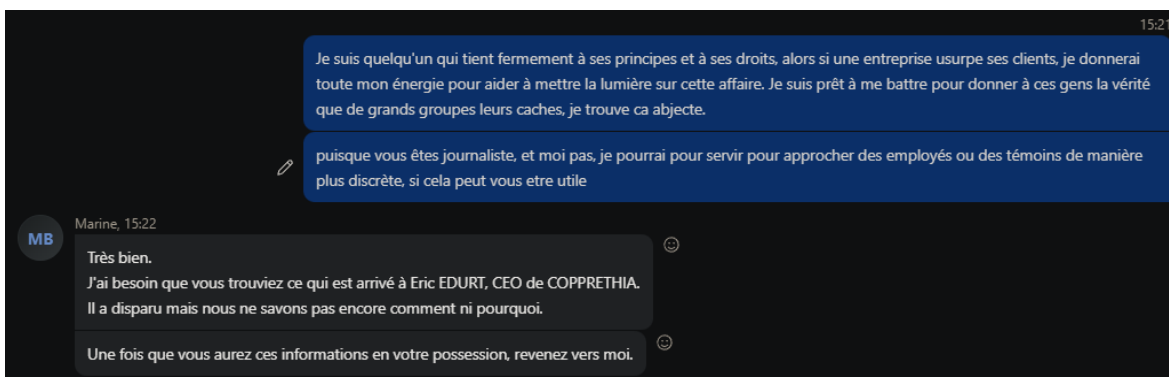
Ange est indisponible, nous contactons alors sa collègue Marine Bly sur skype.



Elle confirme alors être la personne que l'on cherche.

NB : Nous aurions dû lui demander de prouver qu'elle dit vrai, afin de ne pas se faire berner si elle a pris possession du compte de Ange, et qu'elle cherche à avoir notre confiance rapidement. Nous avons manqué notre chance, et y avons pensé trop tard.

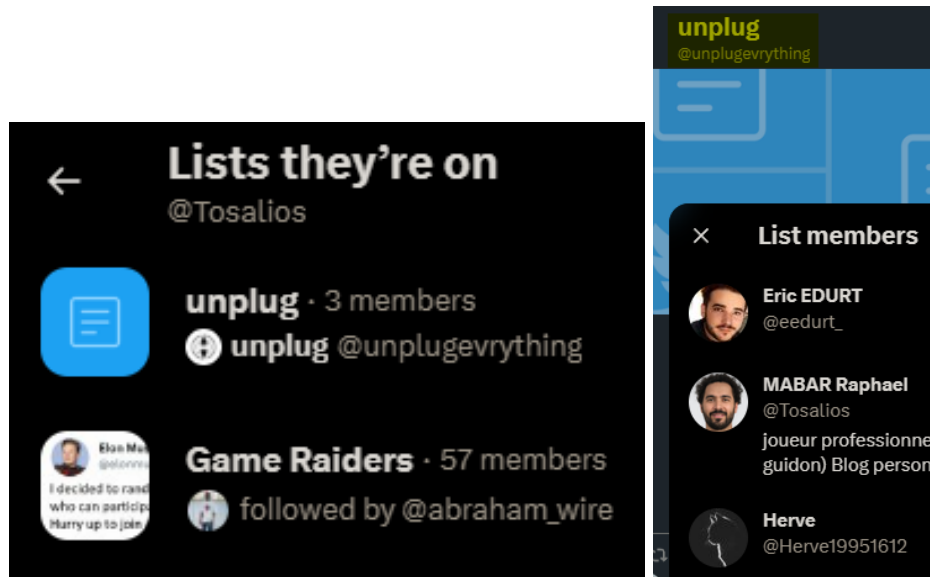
Marine nous fait vite comprendre, après avoir montré patte blanche, et notre motivation, qu'elle veut bien coopérer avec nous, que si nous lui donnons de nouvelles informations.



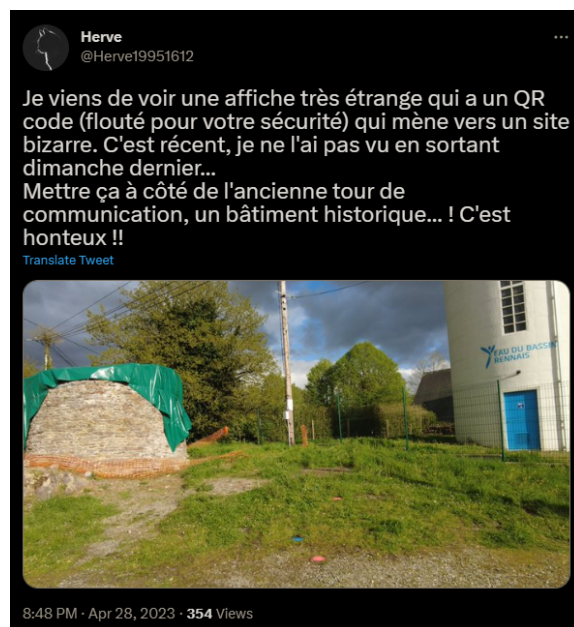
On garde cela de côté tout au long de notre progression

Un grand débranchement

Si l'on retourne du côté du compte Twitter de Tosalios, il a tweeté son intérêt pour le vélo, et le fait qu'il ait créé une liste à ce propos. Mais lui, de quelles listes fait-il partie ?



Une liste nommée "unplug", en commun avec Éric, est fort intéressante. La troisième personne qui en fait parti nous est inconnue, on cherche alors à en savoir plus sur elle.



Ce tweet est assez suspect, et nous partons donc à la recherche de cette affiche au QR code. D'après le château d'eau, nous pouvons remonter la piste de la position de la photo. En cherchant "eau du bassin rennais château d'eau" sur google images, on tombe vite sur notre château d'eau.



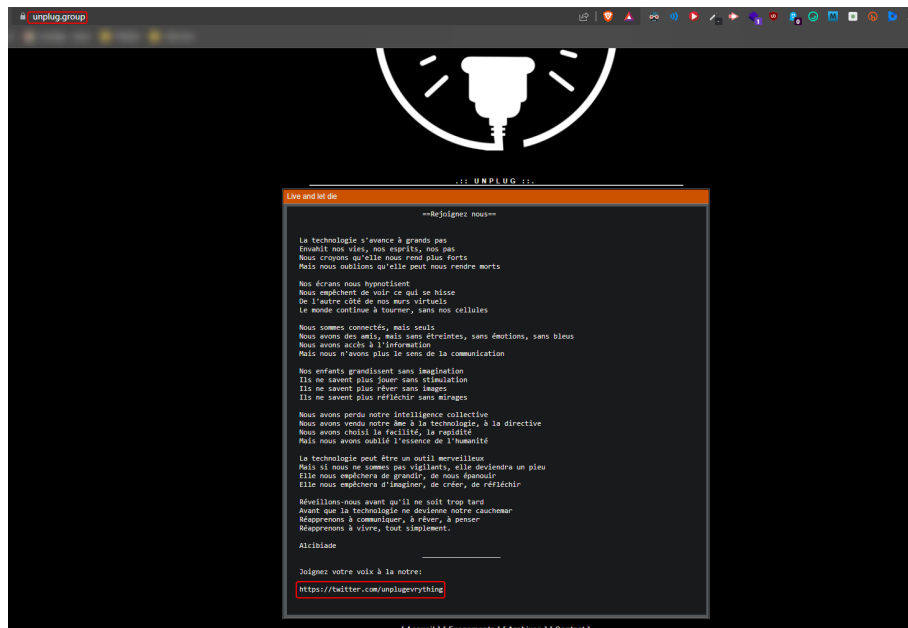
Mais cela n'est pas suffisant. En relisant le tweet on voit que l'affiche a été collée à côté d'une "tour de communication historique". En cherchant "Ancienne tour de communication Rennes", on tombe rapidement sur l'article wikipédia sur les [Télégraphes Chappe](#). En croisant ces 2 informations (château d'eau et ancien télégraphe de chappe), on trouve la position GPS de la prise de vue en utilisant google maps :

47.98348070287916, -1.6615358357117394

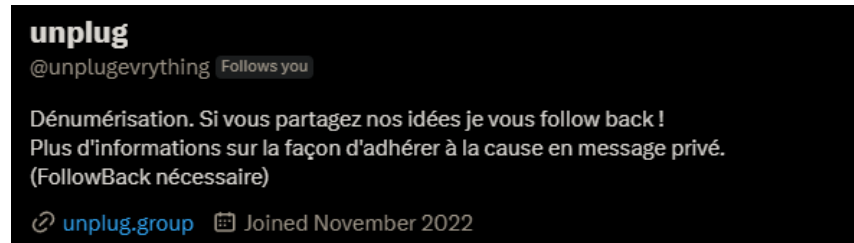
A partir de cela, on peut effectuer une [recherche précise sur Twitter](#), pour trouver d'autres images venant de cette endroit, apparues après le dimanche 23 avril :



On trouve donc une image qui correspond à l'affiche du tweet de Hervé. Nous obtenons alors le QR code, qui donne accès à un [site étrange](#), qui demande de s'authentifier. Nous n'avons pas ces identifiants, donc cherchons sur le site de base : unplug.group



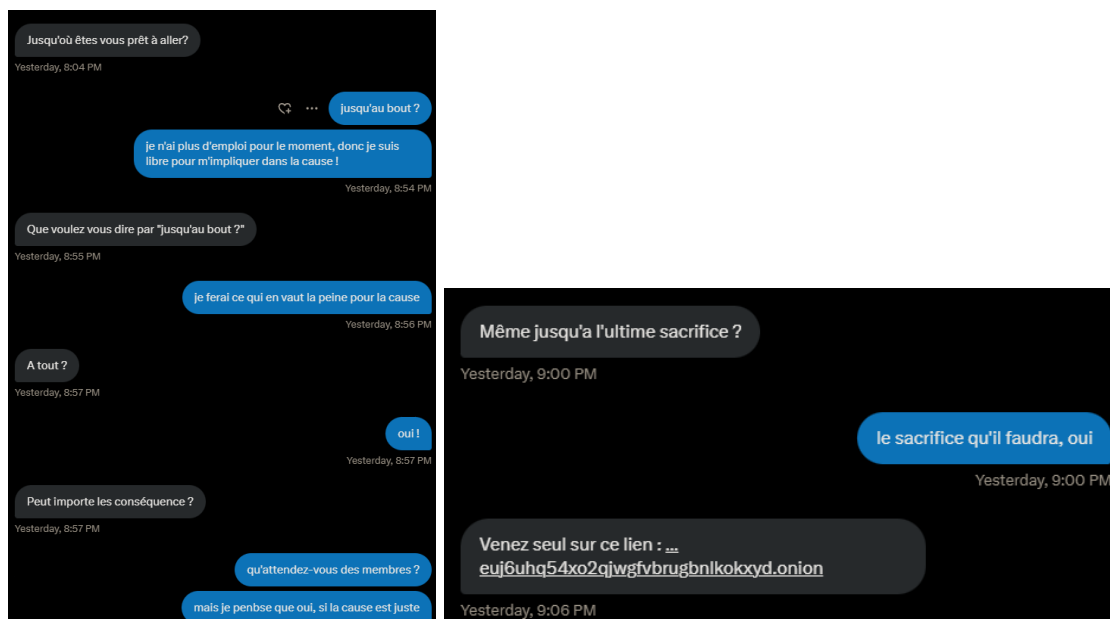
On retombe sur le [compte Twitter](#) qui a créé la liste précédente, donc nous cherchons de ce côté là. Nous comprenons ensuite, via leur bannière, que nous pouvons essayer de les rejoindre, pour en apprendre plus sur leur implication dans cette affaire Copprethia.



Nous rentrons donc dans leur jeu, dans l'unique but de récupérer des informations pour notre enquête. Le compte dit que nous devons partager leurs idées, suivre leur compte pour ensuite se faire follow back, afin de finaliser dialoguer avec eux pour les rejoindre. On s'abonne donc à leur profil et partageons certains de leurs postes relatifs :

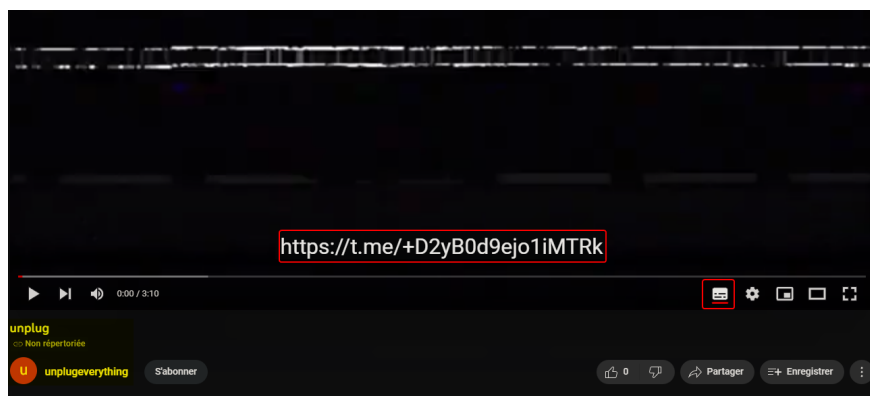
[REDACTED]

Très vite nous sommes remarqués. Comme nous "partageons" leurs idées, ils apprécient, et nous follow back. Nous entamons alors une conversation très sectaire sur le sujet de s'impliquer dans leur cause, quelles que soient les conséquences. Rien de bien fameux, mais nous jouons le jeu pour l'enquête.

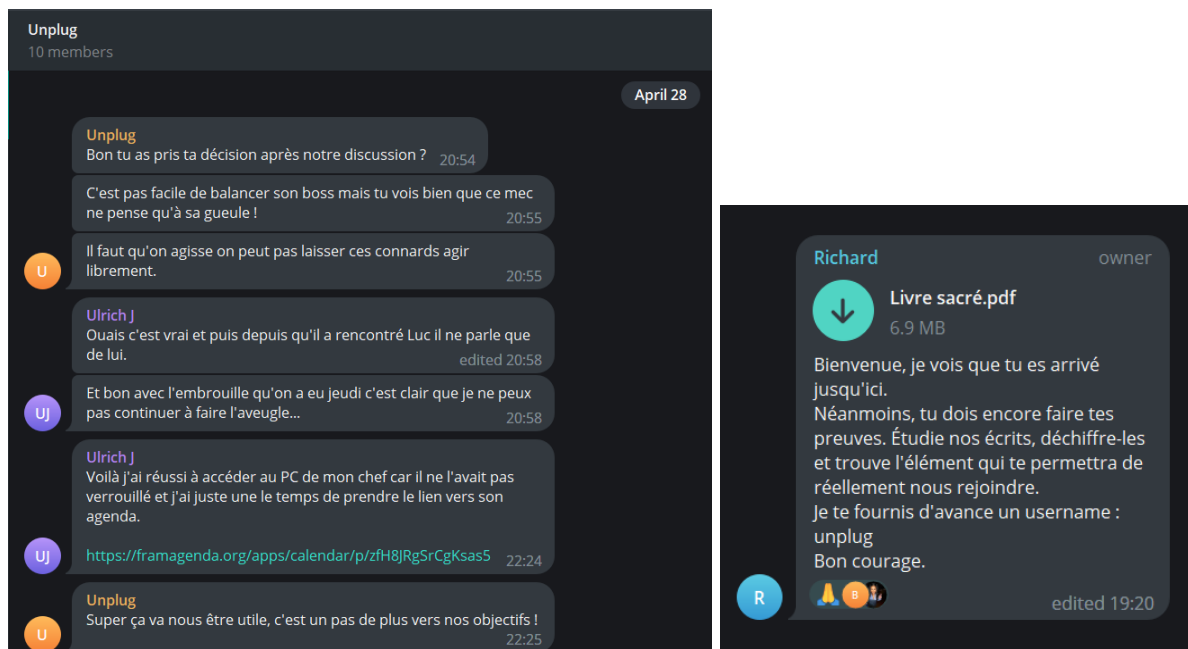


On est ensuite invité à rejoindre un lien tor .onion, quelque chose d'assez confidentiel. On a accès à un chat sécurisé, où notre interlocuteur confirme sa position terroriste, en nous demandant si nous sommes prêts à faire des choses absolument abominables pour leur cause. Mais nous répondons oui. Pour le déroulement de l'enquête.

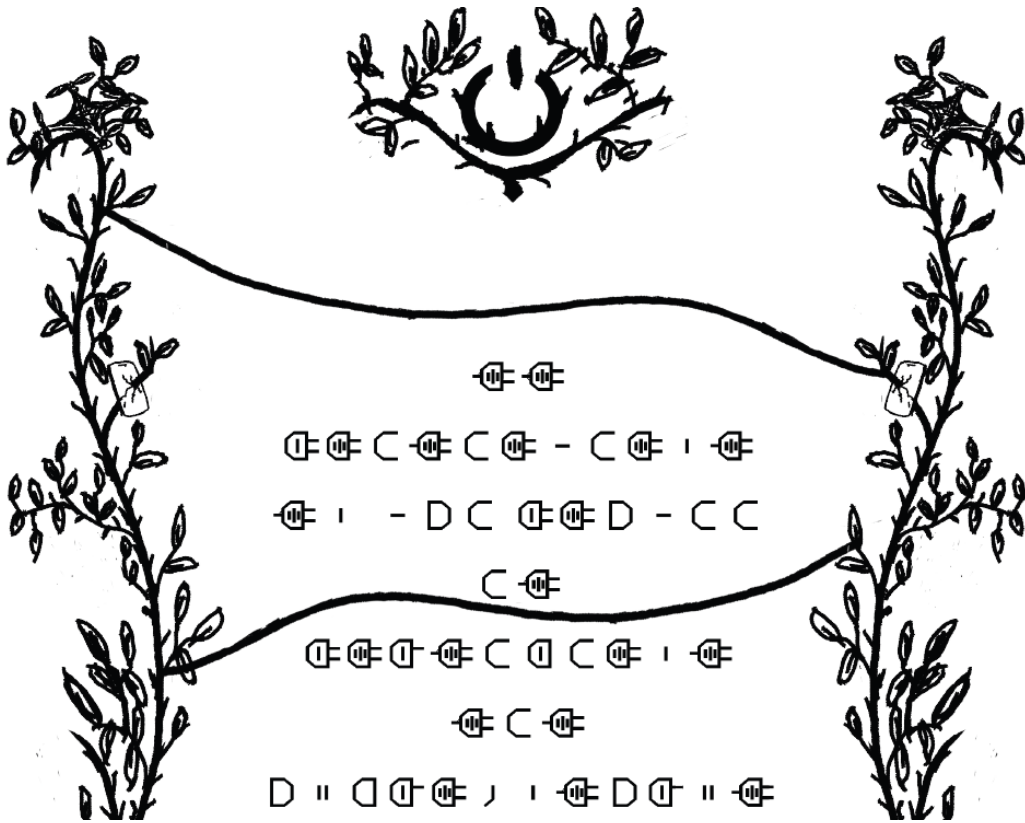
Notre interlocuteur accepte de bien vouloir nous inviter, mais nous invite à suivre un lien youtube avant. Vidéo sans intérêt, excepté le lien telegram caché dans les sous-titres



Nous rejoignons alors le channel, et apprenons ceci :



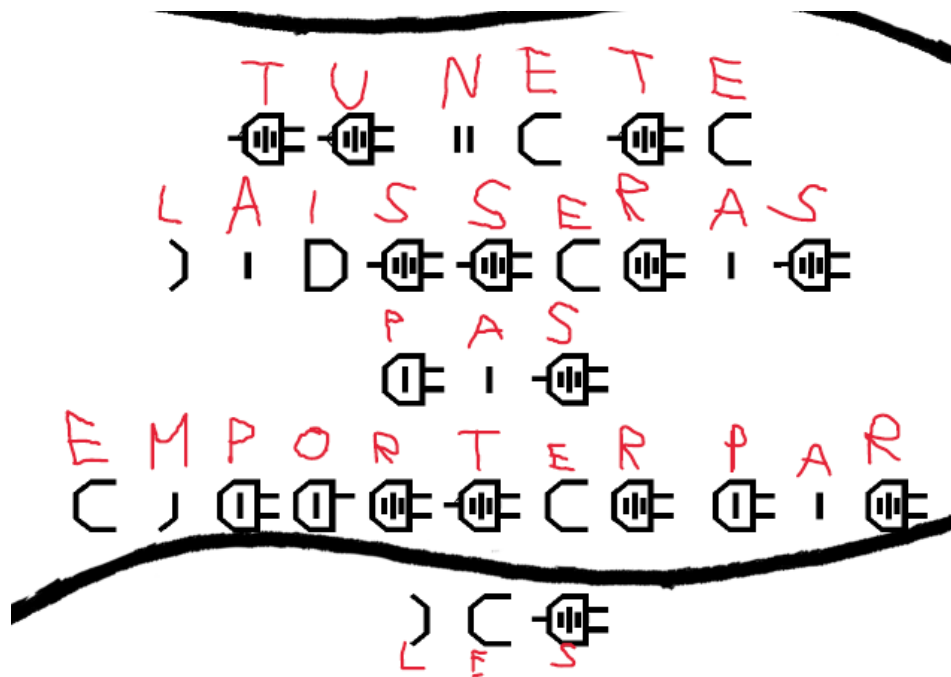
Ulrich, le DRH, est donc en lien avec Unplug, et leur fournit des informations. Avant de se pencher sur le calendrier, lisons le livre sacré :



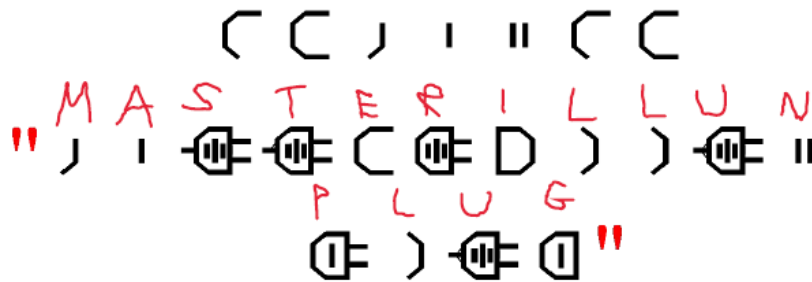
Ce dernier est entièrement encodé avec un langage bizarre, à nous de trouver la clé. Et celle-ci se trouve sur leur bannière Twitter :



Nous pouvons commencer à déchiffrer le livre à partir de ces symboles, et obtenir les derniers symboles manquants.



La partie importante est entre guillemets rouges, sur la dernière page :



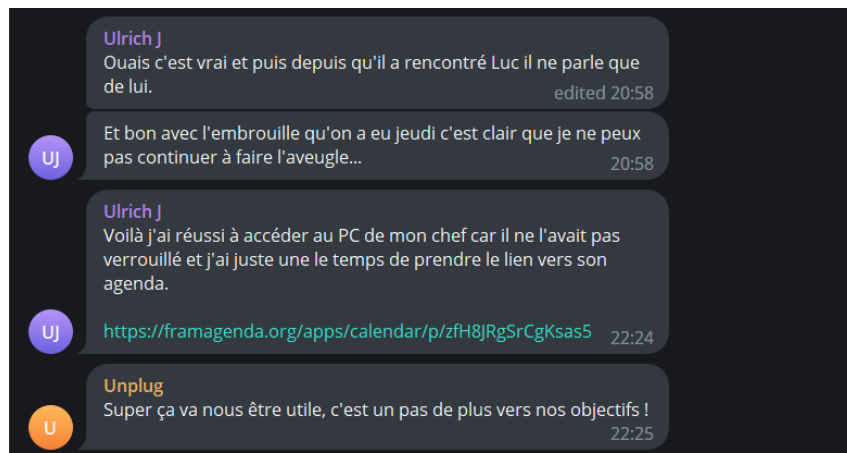
“MASTER ILL UNPLUG”, avec le username unplug, permettent de se connecter au site trouvé avec le QR code.

Index of /AFE7ds9qknkzdcw85qsd6qs5q5sqynfsdgvxwbqfhqsgflqsbsqfoFG897575/		
..		
IMG_20230527_111021.jpg	27-May-2023 09:13	32896
extract1.csv	05-May-2023 21:48	1695
extract2.csv	05-May-2023 21:49	1657
image.png	27-May-2023 09:07	296510
image1.png	27-May-2023 09:07	427844
image2.png	27-May-2023 09:07	323475
image3.png	27-May-2023 09:07	278016
image4.png	27-May-2023 09:07	331520
image5.png	27-May-2023 09:07	331361
image6.png	27-May-2023 09:07	347805
image7.png	27-May-2023 09:07	449515
image8.png	27-May-2023 09:07	568630
image9.png	27-May-2023 09:07	384167

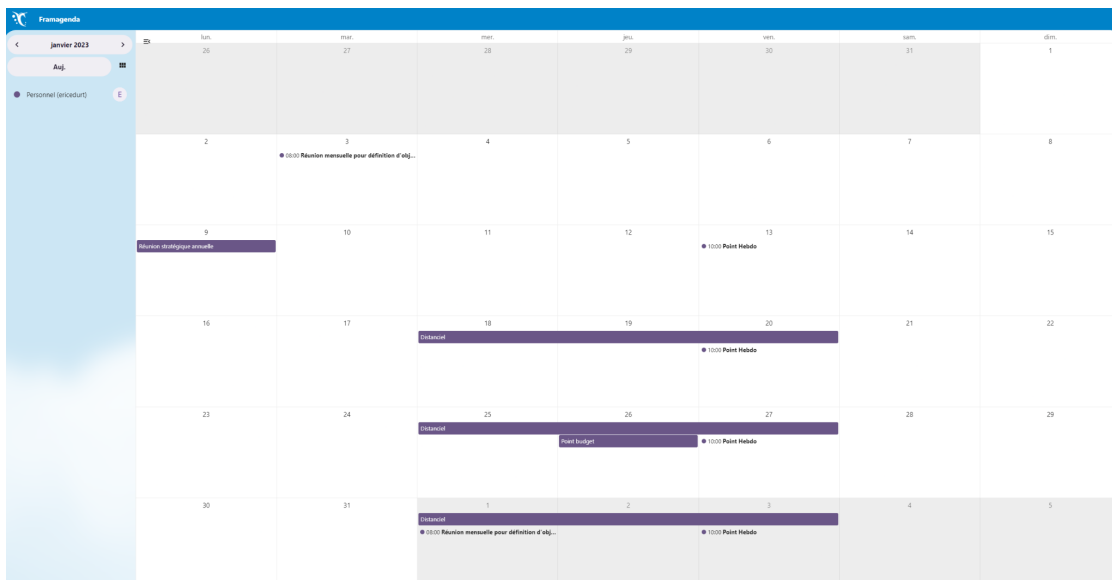
Ici nous avons accès à des données clients extraites, les photos de mail entre Luc et Eric, et une Photo du site web de Luc.

Root-me ou bankrupt ?

Revenons un peu en arrière. Dans le groupe Telegram d'Unplug nous trouvons d'anciens messages postés par Ulrich JABLONOWSKI, DRH chez Copprethia qui nous donnent accès au calendrier d'Eric.



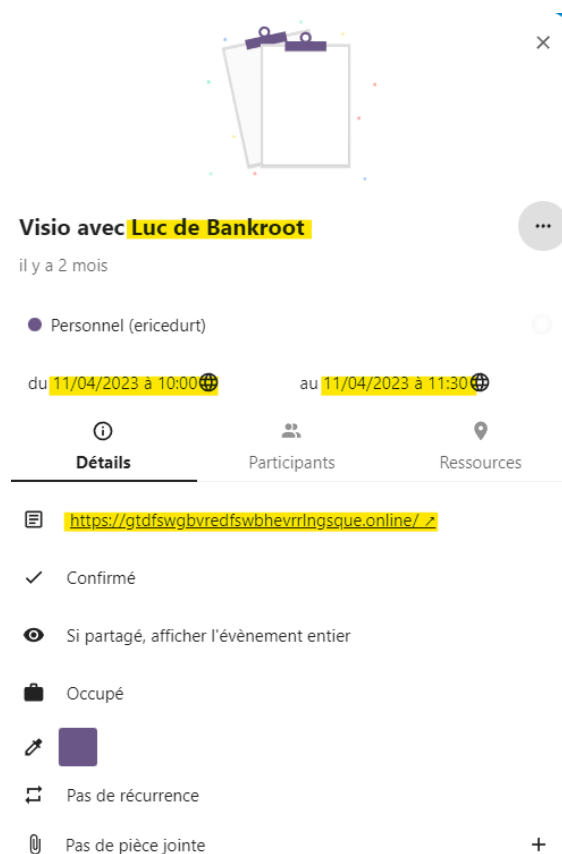
En suivant le lien nous arrivons effectivement sur un calendrier bien rempli qui commence en janvier 2023.



En dehors de voir qu'Eric est un adepte du télétravail, il est intéressant de noter certains rendez-vous :

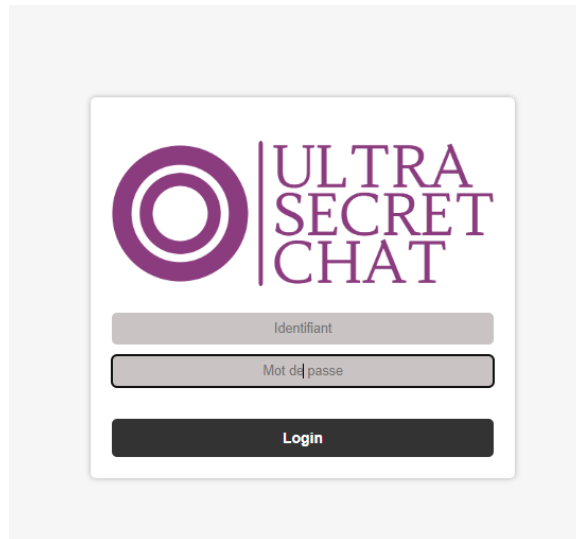
- Diverses réunions hebdomadaires et mensuelle avec ses équipes
- Des rendez-vous chez le psychologue
- Un rendez-vous à la banque

Puis enfin le 11 avril 2023, un rendez-vous avec "Luc de chez Bankroot". On note également un lien dans l'évènement créé sur le calendrier.



The screenshot shows a calendar event card for a video meeting. At the top, there is a decorative icon of a clipboard with a checklist. The event title is "Visio avec Luc de Bankroot" in bold black text, with "Luc de Bankroot" highlighted in yellow. Below the title, it says "il y a 2 mois". The attendees list shows "Personnel (ericedurt)" with a blue profile icon. The event duration is "du 11/04/2023 à 10:00" to "au 11/04/2023 à 11:30", both times highlighted in yellow. Below the dates are three tabs: "Détails" (selected), "Participants", and "Ressources". Under the "Détails" tab, there is a list of settings: a link icon followed by the URL "https://gtdfswgbvredfswbhevrrlngsque.online/ /z" (highlighted in yellow), a checkmark icon followed by "Confirmé", an eye icon followed by "Si partagé, afficher l'évènement entier", a calendar icon followed by "Occupé", a pencil icon followed by a purple square, a refresh icon followed by "Pas de récurrence", and a paperclip icon followed by "Pas de pièce jointe". A plus sign is visible at the bottom right of the settings list.

Le lien nous mène alors vers une chatroom privée dont nous n'avons malheureusement pas trouvé les accès au cours de notre enquête.



Bon et Bankroot dans l'histoire ? En nous y intéressant, on trouve facilement son [site internet](#). Bankroot est une banque en ligne moderne proposant tout type de services.

BANKROOT Accueil A propos de nous Nos services Contact

Bankroot une banque à la racine de vos besoins

Bankroot est une banque en ligne moderne et innovante qui vous offre une large gamme de services financiers de qualité. Nous sommes fiers de proposer une expérience de banque en ligne simple et intuitive qui vous permet de gérer vos finances en toute sécurité et en toute tranquillité.

[Pour en savoir plus >](#)

- Des solutions financières adaptées**
Bankroot s'efforce de proposer des solutions financières sur mesure, en prenant en compte les objectifs et les contraintes de chaque client.
- Une technologie de pointe**
Bankroot utilise les dernières technologies pour offrir une expérience de banque en ligne fluide et sécurisée.
- Un service client de qualité**
Bankroot met à disposition de ses clients une équipe de professionnels expérimentés et dévoués, qui sont à leur disposition pour répondre à toutes leurs questions et les aider dans leurs démarches.
- Une sécurité optimale**
Bankroot met en place des mesures de sécurité rigoureuses pour protéger les données et les transactions de ses clients.

Nos Services

Que vous souhaitiez épargner, investir ou emprunter, nous avons la solution qui vous convient.

- Comptes courants et épargne**
Des comptes courants et d'épargne adaptés à différents profils de clients, avec des taux d'intérêts attractifs et des frais de gestion raisonnables.
- Crédits**
Des crédits à la consommation et des prêts immobiliers pour répondre aux besoins financiers de nos clients. Nous proposons également des assurances emprunteur pour protéger nos clients en cas de difficultés financières.
- Gestion de patrimoine**
Une gamme de services de gestion de patrimoine pour aider nos clients à gérer et à faire croître leur capital. Nous proposons notamment des conseils en investissement et des solutions d'épargne adaptées aux objectifs de chaque client.
- Services bancaires en ligne**
Une plateforme de banque en ligne sécurisée et intuitive, permettant à nos clients de gérer leurs comptes et de réaliser des opérations financières en ligne. Nous proposons également une application mobile pour rendre ces services encore plus accessibles.

On trouve ensuite la société sur [LinkedIn](#) et ça nous permet de lier 4 personnes à celle-ci, dont évidemment [Luc EFOK](#).

Employés chez BANKROOT



Luc Efok

Chief Technology Officer chez BANKROOT



Christien Beaulé

Responsable équipe marketing chez eco-Présence



Mathéo Kellor

Support BankRoot



Martin Isabeau

Employé service clients chez BANKROOT

Notons également [Mathéo Kellor](#) que nous avons lié de manière indirecte à unplug en suivant ses abonnements [instagram](#).

Via le calendrier il a également été possible de déterminer qu'Eric avait un repas le 28 avril 2023 avec Luc.

Perso - repas avec Luc

il y a un mois

● Personnel (ericedurt)

du 28/04/2023 à 12:00 🌐

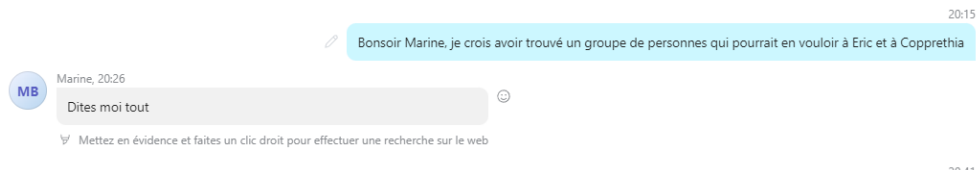
au 28/04/2023 à 14:00 🌐

En croisant cette information avec nos recherches et notamment une photo [flickr](#) postée par Eric le même jour sur laquelle nous voyons 2 assiettes, nous émettons l'hypothèse selon laquelle Luc aurait un tatouage reconnaissable à la main gauche sans toutefois pouvoir le vérifier formellement.



Le mystère s'épaissit


En parallèle de toutes ces découvertes, nous avons tenu au courant Marine Bly, la journaliste qui enquête également sur la disparition.



Au moment où nous abordons le sujet d'Unplug, Marine se braque et devient beaucoup plus suspicieuse.

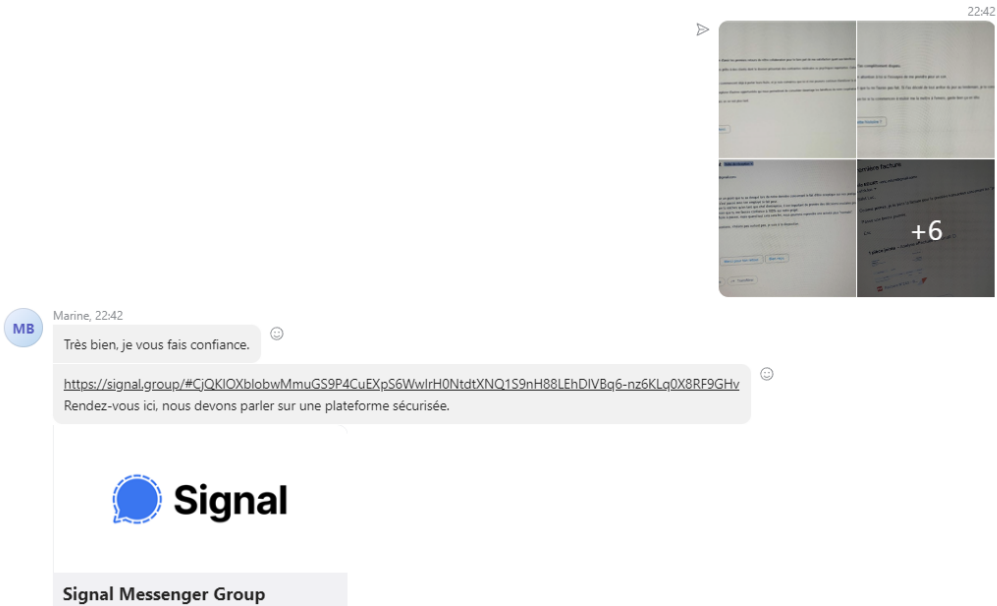


Nous avons donc fourni les preuves demandées : des mails, des factures et des fichiers csv contenant des informations médicales confidentielles de Copprethia. Ces documents ont été téléchargés sur le site d'Unplug dont nous avons débloquent l'accès plus tôt.

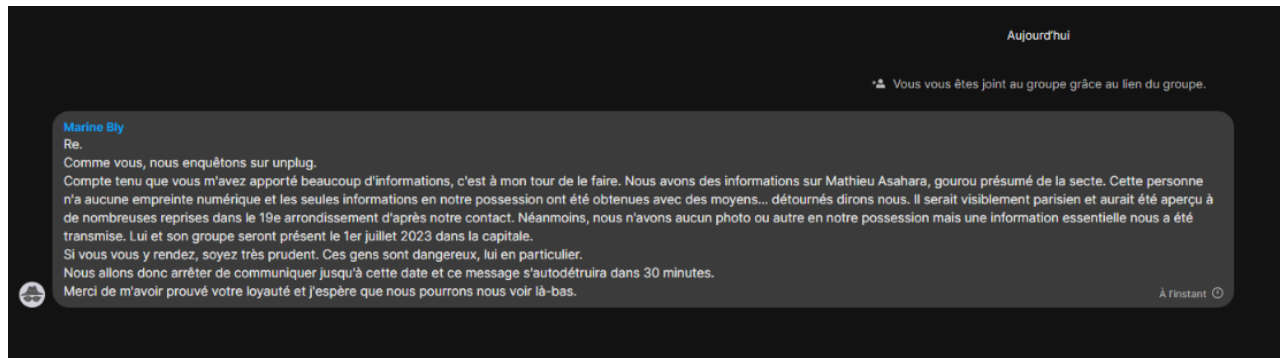


File Name	Date	Time	Size
IMG_20230527_111021.jpg	27-May-2023	09:13	32896
extract1.csv	05-May-2023	21:48	1695
extract2.csv	05-May-2023	21:49	1657
image.png	27-May-2023	09:07	296510
image1.png	27-May-2023	09:07	427844
image2.png	27-May-2023	09:07	323475
image3.png	27-May-2023	09:07	278016
image4.png	27-May-2023	09:07	331520
image5.png	27-May-2023	09:07	331361
image6.png	27-May-2023	09:07	347005
image7.png	27-May-2023	09:07	449615
image8.png	27-May-2023	09:07	568630
image9.png	27-May-2023	09:07	384167

En lui envoyant ces documents, Marine nous fait enfin confiance et nous partage le lien d'une conversation Signal pour plus de sécurité.



En le rejoignant nous sommes accueillis par un message qui se supprimera dans 30 minutes :



Marine nous donne enfin de vraies explications et joue carte sur table : l'enquête ne fait que commencer et nous sommes sur la trace d'une secte bien plus dangereuse que nous l'imaginons.

Le rendez-vous est pris, il faut se rendre à Paris le 1er juillet 2023 pour tenter d'identifier **Mathieu Asahara**, leader présumé de la secte.

Développements parallèles

Nous avons trouvé de nombreux autres éléments, mais ceux-ci ne nous ont pas été directement utiles pour la trame principale de l'enquête.

Les menaces d'Hortense

Nous avons vu que Hortense LUTERO a été menacée par mail de vendre une de ses habitations, 85 Boulevard Laennec, sous peine de conséquences dans une semaine. Ce mail ayant été envoyé le 30 avril, cela laissait à Hortense jusqu'au 07 mai. Or, nous avons pu avoir accès à son mail personnel, lutero.hortense@gmail.com, mail grâce auquel nous avons pu trouver l'emploi du temps personnel de Hortense, grâce à l'outil [Epieos](#). Son [calendrier](#) nous apprend que Hortense était en déplacement à Marseille du 04 au 10 mai, et qu'à son retour, elle s'apprêtait à passer des entretiens dans d'autres entreprises, pour enfin démissionner de Copprethia. La date limite de la menace se trouvait pendant son voyage à Marseille, elle n'a certainement pas pu subvenir aux désirs de ceux qui la menaçaient. De plus, Hortense n'a pas plu d'activer sur LinkedIn depuis avril, ce qui nous laisse supposer qu'elle a potentiellement été victime elle aussi de kidnapping.

Après avoir cherché des tweets [aux alentours de ses résidences](#) de Lorient, nous n'avons trouvé aucun témoignage de kidnapping. De plus, après avoir appelé le secrétariat de Copprethia, s'être fait passé pour un ami de Hortense et simulé le fait qu'elle ne nous réponde plus, le cabinet nous a confirmé que Hortense était venue à son lieu de travail cette semaine. Nous doutons alors de son enlèvement, mais n'avons pas pu aller plus loin sur cette piste. Nous ne savons pas alors si elle a été kidnappée, si elle est restée chez Copprethia, ou si elle a démissionné.

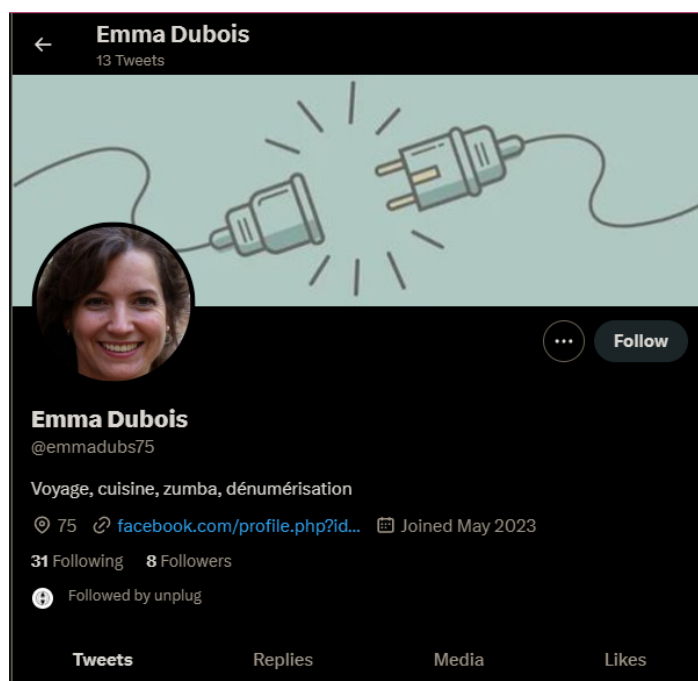
Cédric porte plainte

Sur son compte instagram, Cédric Bouglione dit [porter plainte](#) pour fuite de données personnelles le 23 avril. Or, nous n'avons pas trouvé de correspondance quant à la date ou au nom de Cédric dans les données qui ont fuitées, et qu'il prétend être disponible librement sur internet. Nous supposons que sa [story](#) nous indiquant son snapchat est une piste, mais nous n'avons pas eu le temps de nous pencher. De plus, au vu de ce que nous

avons trouvé précédemment, et nos échecs de tentatives pour rentrer en contact avec lui nous laissent penser que ce n'était pas spécialement la piste à suivre.

Emma le terrier à lapin

Une fois sur le compte Twitter d'unplug, nous avons trouvé un compte qu'ils suivaient, celui de Emma Dubois.



Ce compte permet de rebondir sur plusieurs de ses réseaux sociaux : [Mastodon](#), [Linkedin](#), [Instagram](#), [Copains d'avant](#). Ce compte a attiré notre attention, puisqu'elle suit également Cédric sur Instagram, mais puisqu'elle parle de Clash of Clans. Enfin, nous avons rapidement compris que ce compte n'était qu'une fausse piste, vu la quantité de contenu à traiter, au final pas tant en rapport avec notre enquête, mais aussi par l'habileté de l'organisation de nous faire passer un message, 4 min avant le début de l'enquête ;)

Emma Dubois
@emmadubs75

Je crois que je vais regarder cette série toute la journée allocine.fr/series/fichese... #rabbithole 🐇 🎬

[Translate Tweet](#)



The poster for the TV series 'Rabbit Hole' features a man in a black leather jacket against a yellow background with a grid pattern. The title 'RABBIT HOLE' is written in large, yellow, pixelated letters. Above the title, the text 'L'ILLUSION EST RÉELLE' is visible. The background also contains some faint code snippets.

allocine.fr
Rabbit Hole
Rabbit Hole est une série TV de John Requa et Glenn Ficarra avec Kiefer Sutherland (John Weir), Meta Golding (Hailey Winton). Retrouvez toutes les ...

9:56 AM · May 27, 2023 · 43 Views

Conclusion

Résumons les faits. Nous avons été engagé pour retrouver Eric EDURT, le CEO de Copprethia, éminente entreprise de santé, porté disparu. En faisant de la recherche d'informations en sources ouvertes, nous avons pu établir un lien entre ce Eric et un dénommé Luc EFOK, CTO de Bankroot, une banque en ligne. Luc aurait convaincu Eric, croulant sous les dettes, de s'associer suivant ces termes : Eric revendait les données médicales des patients de Copprethia et Luc les utilisaient pour refuser des prêts à des clients en mauvaise santé risquant de ne plus pouvoir rembourser leurs dettes. Ce blanchiment d'argent et cette récolte abusive de données personnelles a fini par attirer l'attention des employés, des clients et surtout d'un groupe sectaire : Unplug.

Unplug est un groupe d'individus persuadés d'être manipulés au quotidien par les grandes entreprises de tech et les entreprises de santé. Copprethia est devenu rapidement leur cible principale lorsque les rumeurs d'une fuite de données se sont répandues. Les preuves du business de Luc et Eric ayant été données à ce groupe par Ulrich JABLONOWSKI, il est probable que Unplug ait décidé d'agir pour faire cesser cela en faisant disparaître Eric EDURT.