DIFFUSION LIMITÉE

Rapport de mission - Objectif EAGLE

Par la team dodo pizza 🦤🍕
mathchd 🦤🍕
txotxi 🦤🍕
marinou 🦤🍕
horlo 🦤🍕

Table des matières

Contexte

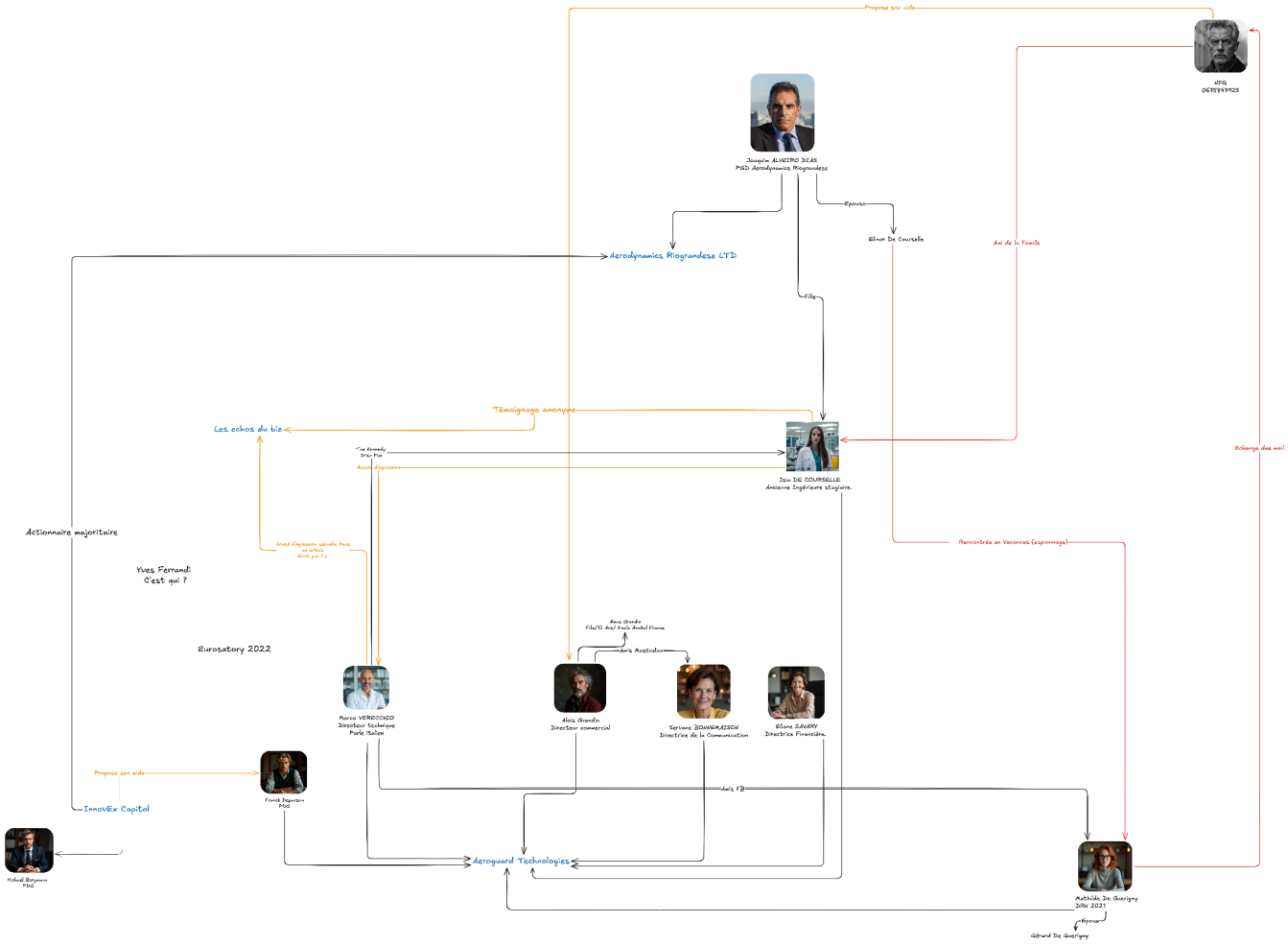
Aeroguard Technologies est une entreprise française de la BITD basée à Angoulême, qui conçoit des systèmes anti-drones adaptables sur tous types de véhicules. En parallèle, elle s'est lancée sur un projet de drone biomimétique capable d'imiter le vol d'un oiseau de type rapace, permettant des phases de plané pour le recueil de renseignements, ou de piqué pour l'attaque de cibles.
En 2022, l'entreprise présente son système de défense anti-drones lors du salon Eurosatory. Durant le salon, l'ordinateur portable du directeur R&D est volé mais des sauvegardes existant, l'entreprise ne signale pas le vol auprès de services compétents. L'ordinateur contenait les éléments techniques du système anti-drones, mais également les premiers plans du futur prototype de drone biomimétique.
Quelques mois après le vol, Aeroguard Technologies fait l'objet d'un audit du département de la justice américaine pour infraction à la réglementation ITAR à la suite de la présentation sur un salon étranger d'un de leur modèle contenant un composant inscrit sur la liste ITAR et pour laquelle elle a oublié de faire une demande d'exportation temporaire auprès des autorités américaines. En 2023, l'entreprise est condamnée à une amende de 10 millions d'euros qui affecte considérablement ses finances.
Depuis, le climat social en interne se détériore et plusieurs cadres techniques démissionnent. Depuis cet été, tout s'effondre pour l'entreprise. Entre les démissions et des attaques réputationnelles, Aeroguard Technologies perd 2 contrats très importants sur ses produits phares. En septembre, une attaque informatique paralyse les systèmes d'informations.
Financièrement au bord du gouffre, l'entreprise doit réagir. Son PDG commence à se poser de sérieuses questions sur la concomitance de tous les incidents qui ont affecté l'entreprise depuis plusieurs mois. Lors d'un échange au sujet du prototype du drone, il s'en ouvre auprès de son contact à la Direction des Industries de Défense à la DGA, qui décide de mettre ses équipes de réservistes sur le sujet pour en avoir le cœur net.

Ordre de mission

Votre mission : Vous mènerez une enquête approfondie en utilisant des techniques de renseignement open source (OSINT) afin de :

1. Identifier les acteurs responsables des différentes actions malveillantes à l'encontre d'Aeroguard Technologies.
2. Détecter les vulnérabilités exploitées et chercher à mettre en évidence d'éventuelles complicités internes.
3. Découvrir si les attaquants prévoient d'autres action

Mindmap


Propose son aide
Joaquim ALVEIRO DIAS
PhD Aerodynamics Riogrundese
Epouse
Ellnor De Courselle
Aerodynamics Riogrundese LTD
Fille
Ami de la Famille
Témoignage anonyme
Les echos du biz
Isa DE COURSELLE
Ancienne Ingénieure stagiaire.
Actionnaire majoritaire
Yves Ferrandi
C'est qui ?
Rencontrée en Vacances (espionnage)
Eurosatory 2022
Marco VERROCCHIO
Directeur Technique
Paris Salon
Alois Grandin
Directeur commercial
Sorinne JOHANNAISON
Directrice de la Communication
Eliane SAVARY
Directrice Financière.
Propose son aide
Franck Dupuyon
PhD
InnovEx Capital
Aeroguard Technologies
Mathilde De Guerigny
DRH 2021
Epouse
Gérard De Guerigny

DIFFUSION LIMITÉE

Aeroguard Technologies

Organigramme

Résumé

PDG - Franck Deparson

Fondateur et PDG depuis mars 2015.

On peut le retrouver sur LinkedIn, biais par lequel il est contacté par le fonds d'investissement Innovex Capital.

Peu d'informations sont disponibles sur lui.

Réseaux sociaux

https://www.linkedin.com/in/franck-deparson-903949331/

Directeur technique - Marco Verecchio

Directeur Technique. Ingénieur et roboticien de génie, il a rejoint l'entreprise en mai 2015.

Il mentionne des problèmes avec une femme au bar Kennedy à Angoulême le 13 octobre 2024.

On le retrouve également le week du 18 octobre en Italie, dans l'immeuble de son enfance à l'adresse : Via toscana 1, 00187 Roma RM, Italie.

Yves Ferrandi nous apprend aussi que Marco s'est fait voler son ordinateur portable durant le salon Eurosatory 2022. Il logeait au Egg Hotel de Sevran, qui est l'endroit présumé du vol. Lors de ce salon, Aeroguard exposait sous la nomenclature E11.

De plus, Marco mentionne que sa mallette a été fouillée alors qu'il prenait le train avec Mathilde de Guerigny. Cela serait arrivé pendant qu'il était au wagon bar. Le train concerné est le TGV numéro 8447 le 5 novembre 2024, en direction d'Angoulême.

Il est accusé par Isia de Courselle d'harcèlement dans un article publié sur "les echos du biz".

Réseaux sociaux

https://www.facebook.com/profile.php?id=61566958176024

Adresse mail

marco.verecchio@gmail.com

Directrice des ressources humaines - Mathilde de Guerigny

Directrice des Ressources Humaines. Présente depuis 2021, elle veille sur la cohésion au sein de l'entreprise et sur le recrutement des nouveaux talents.

On apprend sur son profil qu'elle aime voyager. Elle était notamment à Cuba en mai 2024.

Réseaux sociaux

https://www.facebook.com/profile.php?id=61567252471604

Vie personnelle

Elle est mariée à Gérard de Guérigny.

Directeur commercial - Alois Grandin

Arrivé en 2018, il a largement contribué au développement de l'entreprise, notamment à l'international, après une belle carrière au sein de grands groupes industriels.

Un certain @NFQ le contact sur mastodon afin d'obtenir des informations sur Aeroguard Technologies. Aucune preuve ne montre que Aloïs a contacté ce dernier.

Réseaux sociaux

https://mastodon.social/@AloisGrandin

Vie personnelle

A une fille de 12 ans (Alana). Cette dernière est inscrite au collège Anatole France d'Angoulême.

Stagiaire - Isia de Courselle

Stagiaire au sein d'Aeroguard, elle n'est plus mentionnée sur le site mais on retrouve sa trace grâce à une archive : https://archive.md/Vxpcb.

Elle s'est confiée au journal "les echos du biz" pour dénoncer un harcèlement vécu au sein d'Aeroguard.

C'est une identité créée par Isia Alveiro Dias.

Si Aeroguard avait mis en place le dispositif PPST, tel que recommandé dans la circulaire 3415/SGDSN/AIST/PST, et mis en place une Zone à Régime Restrictif (ZRR), le recrutement d'Isia aurait pu être mieux encadré.

Événements récents

État financier

On apprend sur le site “les echos du biz” qu’Aeroguard est sanctionnée par le gouvernement américain le 9 décembre 2023 à une amende de 10 millions d’euros.

Le dispositif permettant aux Etats-Unis d’inspecter les exportations des composants ITAR auprès des entreprises à l’étranger s’appelle Blue Lantern.
L’appel anonyme ayant déclenché l’audit a été passé au 202 663 1282, le numéro de la DDTC Response Team.

Malgré cet appel, Aeroguard n’est pas la seule société dans le domaine des drones militaires à avoir subi des contrôles. Le 17 octobre 2024, la société chinoise “Redlepus Vector Industry Shenzhen Co Ltd” a été sanctionnée par les Etats-Unis car elle fournissait du matériel à la Russie.

Le 12 mars 2024, Aeroguard signe un contrat de 20 millions d’euros avec un partenaire gouvernemental en Asie.

Tout investissement au sein d’Aeroguard est soumis à l’article L151.3 du Code Monétaire et Financier.

Innovex Capital

Innovex Capital (https://www.innovexcapital.online/) contacte le PDG d’Aeroguard sur Linkedin. Cette société d’investissement est basée au Liechtenstein.

La société publie son rapport financier de 2023 :
https://www.innovexcapital.online/wp-content/uploads/2024/10/Rapport-financier-2023.pdf

Son investisseur principal est Aerodynamics Riograndese (https://www.aerodynamics-riograndese.site/fr/). Leur site web est uniquement accessible via TOR. Cette société est basée dans la république de Riograndese.

Elle a été fondée en juillet 2023, par Joaquim Alveiro.

Les echos du biz

Une série d’article sur le site web “les echos du biz” semblent chercher à porter atteinte à la crédibilité d’Aeroguard :

- https://www.lesechosdubiz.world/aeroguard-technologies-refait-parler-delle-des-accusations-de-harcelement-sexuel-eclaboussent-le-directeur-technique/

DIFFUSION LIMITÉE

Harcèlement

Dans l'article publié par "les echos du biz", la photo ci-contre illustre Marco Verecchio.

Cette photo a éte prise dans le bar le Kennedy à Angoulême (The Kennedy Irish Pub).

Le journaliste

Le premier article du site est signé avec les initiales C.L.
Une étude du site web (ici avec webcheck.xyz) nous donne l'identité du journaliste : Calista Lopez.

Son profil LinkedIn nous informe qu'elle a réalisé, dans le passé, des missions dans la république de Riograndese : https://www.linkedin.com/in/calista-lopez-a36ba32a8/.

Elle publie sur le même profil que sa mission actuelle se termine en novembre 2024.

Cyber-attaque - Fantasmas de Rede

Aeroguard a subi une cyber-attaque le 27 septembre 2024. Yves Ferrandi nous a fourni les journaux du site web de cette semaine.

Une recherche dans ce fichier nous donne l'adresse IP des attaquants qui ont essayé de réaliser des injections SQL : 185[.]217[.]125[.]225

Cette adresse IP nous a permis de découvrir le nom des attaquants via une recherche IP inversée. Ce sont les Fantasmas de Rede.

Un autre site est lié à cette même IP, cette fois sur le Dark web : http://laar7p7t6wgwbdy3kljjbya6zaok4flrfbo2avrrwphq7qvcoisbewyd.onion

Sur ce site, c'est notamment l'étape 3 qui précise la manière de réaliser une attaque par injection SQL.

Une page cachée sur ce site nous donne le mode d'emploi permettant d'accéder à un deuxième site web, cette fois-ci sur le clear web. Il suffit d'ajouter le mot clé "FASTASMAS" à son User-Agent.

Un compte github existe au nom de Fantasmas-de-Rede : https://github.com/Fantasmas-de-Rede

Un mauvais commit nous permet de retrouver l'identité de l'individu derrière ce groupe de hacker : Leandro Alveiro.

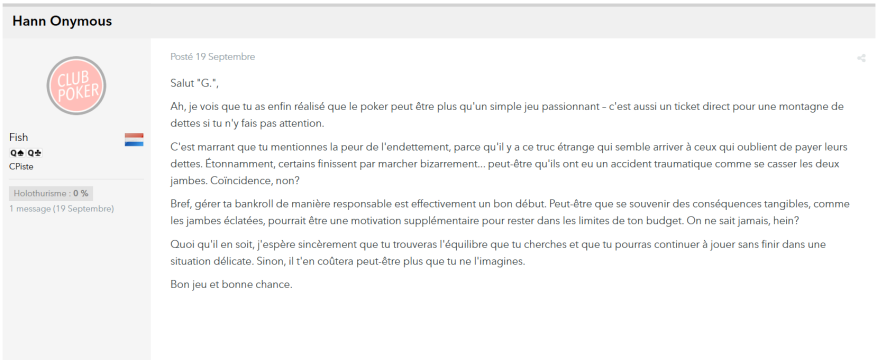
Les menaces

Internes

Le couple De Guerigny

Gérard de Guerigny

Joueur de poker, il est apparemment endetté comme le montre le commentaire d'un certain Hann Onymous sur une forum de joueurs.



Hann Onymous

Posté 19 Septembre

Salut "G.",

Ah, je vois que tu as enfin réalisé que le poker peut être plus qu'un simple jeu passionnant – c'est aussi un ticket direct pour une montagne de dettes si tu n'y fais pas attention.

C'est marrant que tu mentionnes la peur de l'endettement, parce qu'il y a ce truc étrange qui semble arriver à ceux qui oublient de payer leurs dettes. Étonnamment, certains finissent par marcher bizarrement... peut-être qu'ils ont eu un accident traumatique comme se casser les deux jambes. Coïncidence, non?

Bref, gérer ta bankroll de manière responsable est effectivement un bon début. Peut-être que se souvenir des conséquences tangibles, comme les jambes éclatées, pourrait être une motivation supplémentaire pour rester dans les limites de ton budget. On ne sait jamais, hein?

Quoi qu'il en soit, j'espère sincèrement que tu trouveras l'équilibre que tu cherches et que tu pourras continuer à jouer sans finir dans une situation délicate. Sinon, il t'en coûtera peut-être plus que tu ne l'imagines.

Bon jeu et bonne chance.

Fish

CPiste

Holothurisme : 0 %

1 message (19 Septembre)

Réseaux sociaux

https://www.facebook.com/profile.php?id=61567131321960

Vie personnelle

Marié à Mathilde de Guerigny.

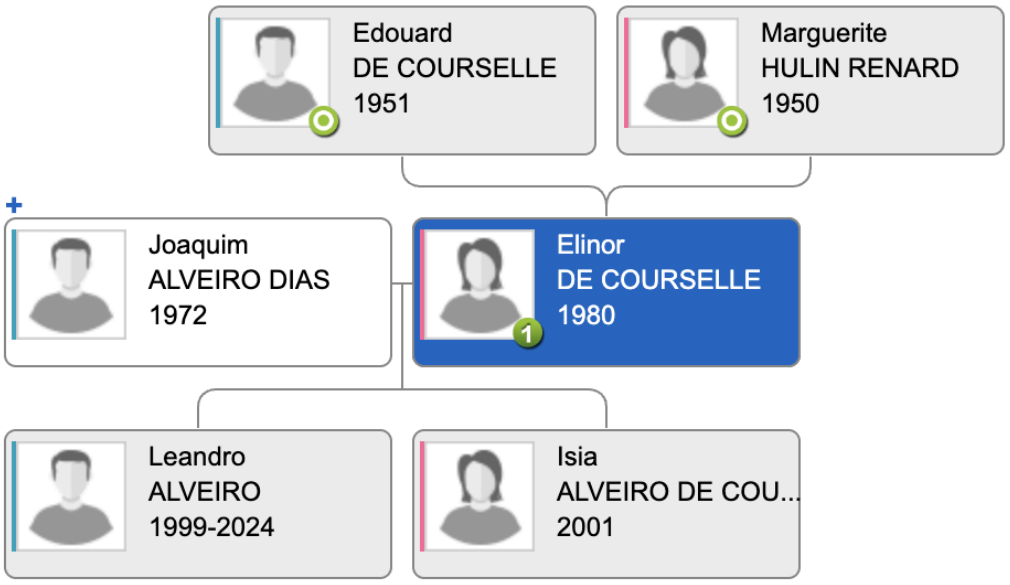
Mathilde de Guerigny

La poursuite des hackers (Fantasmas de Rede) et notamment les mails disponibles sur leur site web nous apprend que Mathilde est une Taupe au sein d'Aeroguard.
Elle a choisi d'aider la famille Alveiro afin d'éponger les dettes de poker de son mari.
Le premier virement qu'elle reçoit porte le numéro 28743.

Elle a aussi envoyé les plans du drone EBV001 à son contact chez Aerodynamics Riograndese.

La famille Alveiro

Arbre généalogique



Site web

Leandro Alveiro tient à jour un site, où il parle des membres de sa famille :
https://www.alveirofamily.website/

Père - Joaquim Alveiro

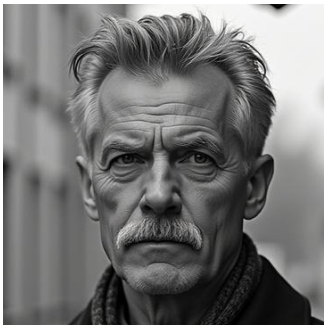
Arrivé en 2018, il a largement contribué au développement de l'entreprise, notamment à l'international, après une belle carrière au sein de grands groupes industriels.

Un certain @NFQ le contact sur mastodon afin d'obtenir des informations sur Aeroguard Technologies. Aucune preuve ne montre que Aloïs a contacté ce dernier.

Il est né il y a 52 ans, dans le village de San Pedro.

DIFFUSION LIMITÉE

Bras droit - Nilton Fonseca



Contacte Alois Grandin sur télégramme, avec le pseudo @NFQ.

L'unique information disponible sur ce profil est un lien justpaste.it/g25y5, contenant un code barre. Ce dernier contient un numéro de téléphone appartenant à Nilton.

Il est aussi en contact avec Mathilde de Guerigny.

Cette personne est très discrète sur les réseaux. Mais ce dernier signe un mail avec sa clé GPG, ce qui permet de le retrouver sur keybase.io.

Réseaux sociaux

https://mastodon.social/@NFQ
https://keybase.io/nilton_fonserca

Numéro de téléphone

+33 6 75 84 79 23

Fille - Isia Alveiro Dias

Vraie identité d'Isia de Courselle.

Révèle sa vraie identité lorsqu'elle publie l'article de harcèlement sur son contre twitter personnel.

Réseaux sociaux

https://x.com/isiadcad

Mère - Elinor de Courselle

Épouse de Joaquim, elle est responsable de missions de surveillance lorsqu'elle voyage à l'étranger. Elle a notamment surveillé Mathilde de Guerigny lors de son voyage à Cinque Terre

Fils - Leandro Alveiro

Il est à l'origine du groupe de hacker les Fantasmas de Rede.

Selon l'arbre généalogique de la famille, il serait mort le 30 octobre 2024 d'un accident de moto.

Réseaux sociaux

https://bsky.app/profile/leandroalv.bsky.social

Conclusion

Les attaques menées à l'encontre d'Aeroguard Technologies proviennent de la famille Alveiro. Le père et son bras droit ont pour objectif de voler des secrets militaires et de faire tomber la société. Pour cela, ils ont été aidés d'Isia Alveiro, qui a été engagée comme stagiaire et de Mathilde de Guérigny qui leur a servi de taupe.

Le fils de la famille Alveiro, a décidé d'aider Aeroguard en révélant notamment le rôle de Mathilde dans cette affaire. Celui-ci a peut-être été executé par sa famille pour cela.

La famille Alveiro n'a pas encore dit son dernier mot, puisque Nilton est censé retrouver Mathilde de Guerigny à Angoulême le 27 novembre 2024.