Write Up - Broken by Design

Sommaire

Introduction

But de l'enquête

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 votre mission est de découvrir la vérité et de comprendre ce qui est arrivé à notre cible.
À l'aide de sources ouvertes, vous devrez récolter le maximum d'informations afin de comprendre la situation et de pouvoir intervenir physiquement, si toutefois cela est nécessaire, dans le futur.

Présentation des "sock puppets"

Dans le cadre de notre enquête OSINT, nous avons établi plusieurs comptes "sock puppets" pour faciliter la collecte et l'analyse des informations. Ces profils, créés sous le pseudonyme de **Benoit Gamelin**, nous ont aidés à naviguer de manière anonyme à travers différentes plateformes, tout en nous permettant d'interagir avec des individus et des groupes d'intérêt.

Voici une brève description de ces comptes :

1. **Gmail (benoit.gamelin67@gmail.com)** : Cette adresse email a été utilisée pour l'inscription et la gestion des différents comptes de réseaux sociaux.
2. **Facebook (Benoit Gamelin)** : Un profil a été créé sur cette plateforme largement utilisée, permettant de collecter des informations en participant à des groupes spécifiques, en suivant des pages et des profils d'intérêt, et en observant les interactions publiques.
3. **LinkedIn (Benoit Gamelin)** : Ce profil professionnel fictif nous a permis de créer et d'entretenir des relations avec

d'autres profils professionnels, de suivre des entreprises d'intérêt et d'accéder à des informations partagées sur cette plateforme.

4. **Discord (benoit67)** : Utilisé pour se connecter à divers serveurs et canaux de chat. La plateforme Discord a été particulièrement utile pour observer et participer à des discussions en temps réel sur des sujets spécifiques.
5. **Twitter (Benoit Gamelin)** : Sur Twitter, le compte a été utilisé pour suivre des comptes pertinents, surveiller certaines discussions ou hashtags et interagir de manière limitée avec d'autres utilisateurs.

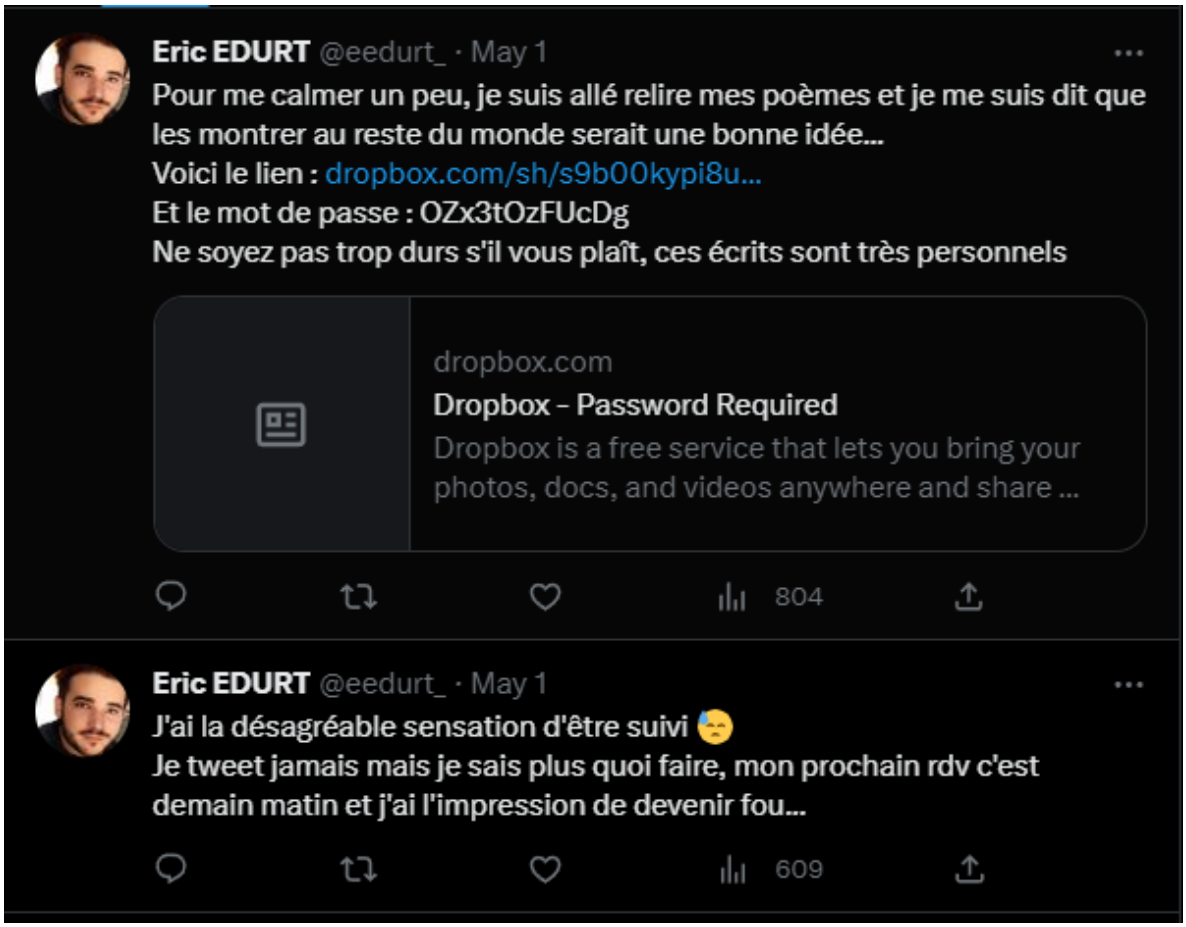
Investigation

La cible est Eric EDURT, on sait qu’il est CEO d’une entreprise informatique lié au domaine du médical.

Recherche des réseaux de la cible

1. Recherche sur Google :
   Nous avons commencé par effectuer une recherche sur Google en utilisant le nom d'Eric EDURT. Cette recherche nous a permis de trouver son profil LinkedIn. Nous avons noté que Eric EDURT était affilié à une entreprise nommée Copprethia (.fr).
2. Utilisation de l'outil OSINT :
   Pour obtenir des informations supplémentaires, nous avons utilisé l'outil OSINT (Open Source Intelligence) disponible sur le site https://osint.industries. En utilisant l'adresse e-mail eric.edurt@gmail.com associée à Eric EDURT, nous avons pu découvrir d'autres comptes potentiellement liés à lui.

3. Compte Flickr :
   Parmi les résultats obtenus grâce à l'outil OSINT, nous avons identifié un compte Flickr qui correspondait à Eric EDURT. Nous avons examiné les photos et les informations disponibles sur ce compte afin de recueillir des indices sur sa vie personnelle et ses intérêts.
4. Utilisation de l'outil WhatsMyName :
   Pour approfondir notre recherche, nous avons utilisé l'outil WhatsMyName disponible sur le site https://whatsmyname.app. Nous avons saisi le pseudo "eedurt_" utilisé par Eric EDURT sur son compte Flickr. Cet outil nous a fourni des résultats supplémentaires en identifiant un lien vers son compte Twitter.
5. Compte Twitter :
   Grâce aux informations obtenues à partir de l'outil WhatsMyName, nous avons pu localiser le compte Twitter associé à Eric EDURT. Nous avons analysé attentivement les tweets, les interactions et les informations partagées sur ce compte dans l'espoir de trouver des indices ou des messages pertinents liés à sa disparition.



6. Lien Dropbox :
   Pendant notre investigation du compte Twitter d'Eric EDURT, nous avons découvert un message qui contenait un lien vers un compte Dropbox. Nous avons immédiatement procédé à une analyse approfondie de ce lien et de son contenu.

Recherche des contacts de la cible

1. LinkedIn de l'entreprise Copprethia :
   En consultant le profil LinkedIn de l'entreprise Copprethia, nous avons identifié les personnes travaillant dans cette entreprise. Parmi ces profils, nous avons remarqué qu'Eric

EDURT avait interagi en likant des publications de Luc Efok, le CEO de l'entreprise Bankroot. Il suivait également la page LinkedIn de Bankroot.

2. Analyse de la photo postée sur Flickr :
   Nous avons examiné attentivement la photo publiée par Eric EDURT sur son compte Flickr. Sur cette photo, nous avons remarqué la présence d'un individu avec un tatouage distinctif sur la main. En comparant cette photo avec une image de Luc Efok sur son profil LinkedIn, nous avons pu établir une correspondance entre les deux individus. Par conséquent, nous en concluons que Luc Efok est un ami d'Eric EDURT.

3. Titre de la photo sur Flickr :
   Le titre de la photo postée sur Flickr par Eric EDURT était "Lunch with a friend" (Déjeuner avec un ami). Cette indication renforce notre conclusion selon laquelle Eric EDURT et Luc Efok sont proches.

Recherche des contacts de la cible (suite) :

En poursuivant notre enquête pour identifier les contacts et relations professionnelles d'Eric EDURT, nous avons examiné de plus près les profils des employés de l'entreprise Copprethia. Voici les informations que nous avons recueillies :

1. Raphael Mabar :
   En consultant la section "Notre Histoire" du site copprethia.fr, nous avons identifié Raphael Mabar
2. Hortense Lutero : Chief Legal Officer
3. Cedric Bouglione :
   En bonus, nous avons découvert que Cedric Bouglione était le créateur du site Copprethia. Bien que n'étant pas directement un employé de l'entreprise.

Suite à notre investigation et à la découverte du profil de Raphael Mabar, nous avons effectué des recherches supplémentaires sur ses activités en ligne. Voici les informations pertinentes que nous avons recueillies :

1. Profil Twitter :
   Nous avons identifié un profil Twitter qui semble appartenir à Raphael Mabar. Cette découverte est prometteuse, car elle pourrait fournir des indices supplémentaires sur sa relation avec Eric EDURT et sur les événements entourant sa disparition.

En ce qui concerne Hortense Lutero, nous n'avons pas encore trouvé d'informations supplémentaires pertinentes.

Quant à Cédric Bouglione, nous avons découvert un compte GitHub qui pourrait lui être associé. L'exploration de ce compte pourrait nous fournir des informations sur ses activités et ses éventuels liens avec Eric EDURT.

Suite à notre enquête approfondie, nous avons fait une découverte significative : nous avons identifié un compte Instagram appartenant à Eric EDURT en utilisant son pseudo. Ce compte était lié à plusieurs personnes de son entourage, et indirectement à Cédric .

En examinant les liens entre les comptes Instagram des personnes de son entourage, nous avons pu identifier des interactions et des connexions entre Eric EDURT et celui de Cedric.

Selon ses publications, il aurait été victime d'une cyberattaque qui aurait entraîné une fuite de ses données personnelles.

Cédric a mentionné qu'il donnerait plus de détails sur cette attaque sur son compte Snapchat.

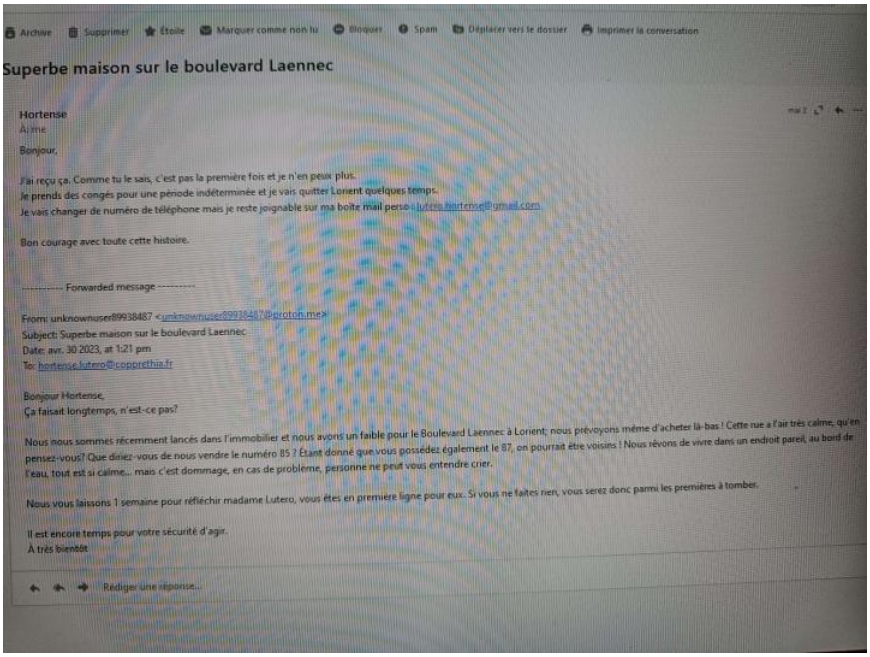
Il est donc recommandé d'examiner attentivement le compte Snapchat de Cédric afin d'obtenir des informations supplémentaires sur la cyberattaque dont il a été victime.

Suite à notre investigation approfondie, nous avons pu identifier facilement le compte Twitter de Raphael en utilisant son prénom et son nom. En explorant son profil, nous avons découvert qu'il était passionné par le vélo et le jeu mobile "Clash of Clans".

Un détail important a attiré notre attention : son tag COC (Clash of Clans) apparaît sur sa bannière Twitter. Nous avons décidé de l'ajouter en tant qu'ami sur le jeu et avons constaté qu'il avait un serveur Discord lié à son clan. Nous avons rejoint ce serveur Discord et avons contacté Raphael directement pour obtenir un rôle d'utilisateur.

Lors de nos échanges avec Raphael, nous avons constaté de nombreux points communs entre lui et notre équipe d'enquête. Il nous a fait confiance et nous a attribué un rôle important sur le Discord, nous permettant ainsi d'accéder à une conversation concernant la disparition d'Eric et le harcèlement dont ses collègues ont été victimes de la part d'un individu malveillant.

Cette conversation pourrait fournir des informations cruciales sur les événements entourant la disparition d'Eric EDURT et l'implication d'un harceleur.



Dans cet e-mail, Hortense explique qu'elle prévoit de quitter Lorient, une information importante pour notre enquête. De plus, nous avons pu récupérer son adresse Gmail grâce à cette capture d'écran. En ayant accès à son compte Gmail, nous avons pu consulter son Google Calendar, qui nous a révélé qu'elle avait l'intention de quitter son emploi chez Copprethia.

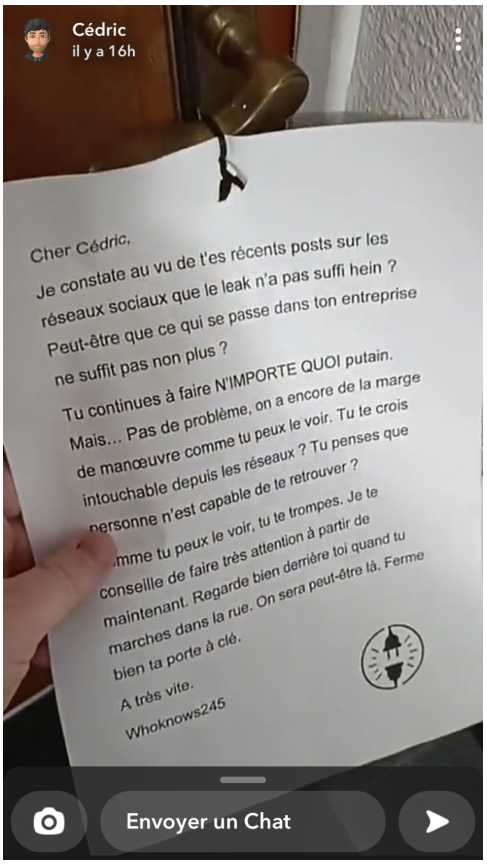
Dans la suite de la conversation, nous avons également appris que Eric était absent depuis plusieurs jours et qu'il était en mauvais termes avec Raphael. Ces informations fournissent des éléments supplémentaires pour comprendre les relations et les circonstances entourant la disparition d'Eric EDURT.

Il est crucial de continuer à échanger avec les membres du Discord, en particulier avec Hortense et Raphael, pour recueillir davantage d'informations sur les événements récents, les tensions entre Eric et Raphael, ainsi que sur le rôle joué par le méchant dont il est question.

Grâce à notre recherche approfondie basée sur le compte Instagram de Cedric Bouglione, nous avons découvert qu'il avait été victime d'une fuite de ses informations personnelles. Cette information nous a conduit à explorer le site Pastebin.com, qui est connu pour héberger ce type d'informations sensibles.

En recherchant le nom de famille "Bouglione" sur Pastebin.com, nous avons eu de la chance et trouvé un fichier .txt contenant les informations personnelles de Cedric.

Dans ce fichier, nous avons pu récupérer son numéro de téléphone. Utilisant ce numéro, nous avons pu l'ajouter en tant qu'ami sur Snapchat. Une fois connectés sur Snapchat, nous avons eu accès à ses stories qui expliquaient ce qui lui était arrivé et pourquoi il envisageait de porter plainte, comme il l'avait mentionné sur Instagram.



D'après les stories de Cedric, nous avons maintenant connaissance du pseudonyme utilisé par le méchant, qui est "Whoknows245". Nous avons également pu obtenir un logo associé à ce pseudonyme.

Merci pour votre lecture !