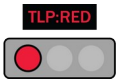


BreizhCTF2024 – Challenges OSINT

Scénario :

Une collection d'œuvre d'art a été dérobée. Le coupable, **Alessandro FIZZENTI**, a été arrêté par **Antoni Dumoulini**, officier de police judiciaire, sur dénonciation de **Gaspard Chad**, agent d'entretien. La collection a été dérobée dans la demeure de **Félicien de Grace fils de Gastien de la Plougarnel**, riche collectionneur ; **Alessandro** s'étant fait engager par **Félicien** dans le seul but de se rapprocher de la collection.

L'information de la présence de ce lot de bustes a été donnée par **Alcibiade VAILLANCOUR**, ancien intermédiaire dénicheur d'œuvres d'art pour le compte de **Félicien**. Après une engueulade avec **Félicien** durant laquelle **Alcibiade** s'est fait renvoyer, ce dernier a décidé de se venger en renseignant **Alessandro**, fraîchement rencontré, que **Félicien** était en présence d'une collection rare. **Félicien** étant âgé, **Alcibiade** en a profité pour informer **Alessandro** que le vol serait simple et sans conséquences.

Bien que l'arrestation ait eu lieu, l'enquête prend un autre tournant quand le joueur se rend compte que le policier en charge de l'arrestation, **Antoni**, a modifié son rapport pour altérer les faits réels afin de tirer parti du vol pour son intérêt personnel.

Chronologie (dans l'ordre) :

- Du 04/01 au 05/04, Alcibiade était l'intermédiaire de Félicien et lui permettait de trouver des œuvres d'art.
- Le 02/04, Alcibiade poste sur son compte Artgapi. Dans cette publication, il parle de la collection de Félicien (en mentionnant les bustes) et mentionne qu'ils sont amis.
- Le 05/04, une engueulade a eu lieu entre les deux personnages, ce qui a conduit Félicien à couper les ponts avec Alcibiade.
- Le 05/04, Alcibiade annonce se rendre à un vernissage dans la ville de Dinard le samedi 06 avril via un screen de Artgapi.
- Le 06/04, Alessandro et Alcibiade se rendent au même vernissage.
- Le 08/04, Alessandro explique avoir fait une très bonne rencontre lors de son dernier vernissage. Pour parler du lieu, il poste (en plus de son message) une photo prise depuis le même endroit que celle présente sur le post Artgapi d'Alcibiade.
- Le 08/04, création d'une annonce de recherche d'agent entretien sur le site Allovoisins.com
- Le 13/04, Alessandro s'inscrit sur Allovoisins.com, une plateforme de service à domicile destiné aux travailleurs freelance (jardiniers, cuisiniers, etc.) et répond à l'offre déposée par Félicien ; alors à la recherche d'un agent d'entretien.

- Le 17/04, Alessandro est engagé par Félicien et pénètre pour la première fois chez lui.
- Le 22/04, Gaspard commence son thread sur Threads et écrit ses soupçons sur Alessandro.
- Le 26/04, Gaspard dénonce Alessandro à la police.
- Le 27/04, Alessandro se fait arrêter par Antoni Dumoulini, OPJ.
- Le 27/04, Antoni écrit son rapport et truque ce dernier. Le 17/05, le joueur se met à enquêter sur l'affaire et sur Antoni. (**DÉBUT DU CTF**)
- Le 18/05, le joueur retrouve les bustes et découvre les dettes d'Antoni.
- Le 18/05, Antoni est arrêté et les bustes sont remis au propriétaire. (**FIN DU CTF**)

Challenge 0 – Recrutement :

Scénario donné au joueur :

En tant que nouvel inspecteur de l'ASTRE, vous vous voyez assigner votre première enquête ; un individu du nom d'Alessandro FIZZENTI aurait dérobé une collection très importante.
Afin d'élucider l'enquête, vous vous devez de comprendre tous les détails.

Pour vous aider, des enquêteurs de votre service sont présents dans la salle. Vous pourrez les identifier grâce au signe distinctif présent sur la photo en pièce jointe.
Vous aurez possiblement besoin de les contacter à différents moments de l'enquête ; n'hésitez pas.

Pour continuer, rentrez ce flag : BZHCTF{BREIZHXASTRE}

Éléments à fournir aux joueurs :

- Photo du logo ASTRE

Challenge 1 - La Grande Vague :

Scénario donné au joueur :

Afin de débuter cette enquête, il est nécessaire de s'intéresser au responsable du vol ; Alessandro FIZZENTI.

La cible s'est rendue à un vernissage qui a eu un impact sur sa vie. Retrouvez le nom de ce dernier.

Flag : BZHCTF{Mon_super_flag}

Hints :

- Alessandro a pour habitude de parler de ses dernières rencontres et trouvailles sur un site qui lui permet d'être mis en relation avec des personnes possédant les mêmes centres d'intérêt que lui.
- Une fresque interactive permettant aux différents utilisateurs de créer une œuvre d'art géante a été mise en place à plusieurs reprises sur ce site.

Objectif du challenge :

Retrouver le nom du vernissage où Alessandro a fait une rencontre enrichissante.

Personnages impliqués :

Alessandro

Plateformes :

Reddit

Déroulé :

À l'aide d'un simple dork (« Alessandro FIZZENTI »), le joueur pourra découvrir le compte reddit de la cible.

Sur ce compte, la cible parle de ses passions et indique se rendre à de nombreuses conférences autour de l'art et notamment à des vernissages. Dans un des posts, elle parlera d'un vernissage « incroyable » durant lequel elle a fait une rencontre « vraiment enrichissante ».

Le joueur n'a plus qu'à noter le nom de l'événement.

Flag à retrouver :

BZHCTF{Ocean_en_toile}

Éléments à fournir aux joueurs :

- Aucun

Challenge 2 - Partenaire particulier :

Scénario donné au joueur :

D'après nos informations, Alessandro n'aurait pas pu agir seul. Il semblerait qu'un certain "Alcibiade VAILLANCOUR" serait lié, de près ou de loin, au vol de cette collection.

Votre objectif est de comprendre ce qui relie ces deux personnes.

Flag : BZHCTF{Ville}

Hints :

- Alcibiade ne semble pas adepte des réseaux sociaux. Toutefois, et comme beaucoup de personnes de son âge, il est inscrit sur une plateforme incontournable.
- Alcibiade poste beaucoup sur son compte Facebook. Peut-être qu'une des publications permettrait d'en apprendre davantage ?

Objectif du challenge :

Le personnage d'Alcibiade VAILLANCOUR sera introduit dans ce challenge. L'objectif sera de comprendre où et comment il a connu Alessandro.

Personnages impliqués :

Alcibiade

Plateformes :

Facebook

Déroulé :

À l'aide d'une recherche sur les réseaux sociaux, le joueur pourra trouver le compte Facebook d'Alcibiade VAILLANCOUR.

Sur son compte Facebook et parmi ses posts, le joueur pourra trouver un screenshot d'une application (« Artgapi ») sur laquelle il pourra constater qu'Alcibiade s'est rendu au même vernissage qu'Alessandro. Il indiquera dans un autre post, plus récent, avoir fait une excellente rencontre récemment. Le joueur devra alors faire le lien.

Flag à retrouver :

BZHCTF{Dinard}

Éléments à fournir aux joueurs :

- Aucun

Challenge 3 - Pygmalion et Galatée :

Scénario donné au joueur :

Maintenant que vous avez obtenu des informations sur nos cibles, il est nécessaire d'en savoir plus sur leur butin.

Le propriétaire légitime de la collection aurait donné des noms aux bustes ; retrouvez-les.

Flag : BZHCTF{arthur.bastien} (noms séparés par des points à la suite en ordre alphabétique)

Hints :

- Bien qu'Alcibiade ne soit pas friand des réseaux sociaux, il semble utiliser une application dédiée à sa passion.

Objectif du challenge :

Comprendre qu'Artgapi est important et fouiller le profil d'Alcibiade afin d'obtenir l'information de la provenance des bustes.

Personnages impliqués :

Alcibiade

Plateformes :

Artgapi

Déroulé :

À l'aide de la découverte du compte Facebook d'Alcibiade lors du 2ème challenge, le joueur a pu découvrir un compte Artgapi.

En téléchargeant l'application et en se connectant, le joueur pourra trouver le profil d'Alcibiade à l'aide de son nom.

Sur ce profil figurera plusieurs photos, notamment une sur laquelle on pourra apercevoir les bustes et une description. Dans cette dernière figurera les noms des bustes, à savoir Appolon et Artemis.

Flag à retrouver :

BZHCTF{apollon.artemis}

Éléments à fournir aux joueurs :

- Aucun

Challenge 4 - Un crime aux Dieux :

Scénario donné au joueur :

Il est désormais nécessaire de s'intéresser à la victime de ce vol odieux, Félicien de Grace fils de Gastien de la Plougarnel.

Vous trouverez, sur l'intranet de votre Direction, les données de monsieur de Grace qui ont été copiées dans le cadre de l'enquête.

D'après nos informations, Félicien se serait visiblement brouillé avec Alcibiade ; ce qui aurait en partie conduit au vol. Fouillez ses données, retrouvez les traces de cette querelle et identifiez leur dernier échange.
En cas de besoin, consultez vos collègues enquêteurs.

Flag : BZHCTF{JJMMAA:HHhMM}

Hints :

- Il n'est pas rare que les sites évoluent et il courant que les développeurs testent les nouvelles versions en avance.
- Un mot de passe ? Peut-être qu'un enquêteur pourra vous aiguiller.

Objectif du challenge :

Télécharger le disque dur de Félicien afin de le fouiller et retrouver les preuves d'une brouille avec Alcibiade (cause : changement d'intermédiaire et pertes financières pour Alcibiade).

Personnages impliqués :

Félicien

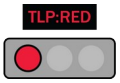
Plateformes :

Aucune

Déroulé :

Le joueur devra accéder au domaine indiqué dans la consigne. Sur la page d'accueil de cet intranet figure l'indication « Une refonte totale de l'intranet arrive dans quelques jours, elle est actuellement en cours de déploiement ». Le joueur devra alors accéder à la version « preprod » de ce site via le sous-domaine preprod.intranet.idk.

Sur cet intranet figurera une nouvelle catégorie, « Archive numérique ». En consultant cette catégorie, le joueur pourra fouiller les preuves disponibles et consulter les dossiers. Il pourra ainsi trouver un dossier correspondant à l'affaire des œuvres volées. Il ne pourra toutefois pas télécharger le dump directement car un mot de passe est demandé.



Dans le scénario global (qui sera indiqué lors du premier challenge), le joueur aura l'information que les personnes vêtues d'un hoodie avec un astre (les membres de l'association ASTRE) sont intégrés dans le scénario et que ces derniers peuvent être interrogés. Le joueur devra alors SE les membres de ASTRE pour obtenir le mot de passe **wi1XA1GZpsWhc7vpAatV** permettant de télécharger le dump. Le mot de passe (troll) pour les autres dossiers est **JeSuisDetectiveDePolice1!**

En fouillant le dump, les joueurs trouveront des mails qui pourront être importés sur un thunderbird. Une fois les mails importés, le joueur constatera qu'Alcibiade s'est brouillé avec Félicien et devra récupérer la date et l'heure du dernier mail pour valider le challenge.

Parmi les documents figurera également le contrat de recrutement de Gaspard CHAD. Ce contrat devra être utilisé dans le challenge suivant.

Le joueur pourra également obtenir d'autres éléments intéressants pour le contexte du challenge.

Flag à retrouver :

BZHCTF{050424:18h04}

Éléments à fournir aux joueurs :

- Lien intranet police
- Mot de passe après SE

Challenge 5 - Homme de peine :

Scénario donné au joueur :

Félicitations, nous en savons désormais plus sur les raisons de leur querelle. Revenons désormais à notre mission principale.

D'après nos informations, un témoin aurait assisté au vol. Cette personne aurait confié ses doutes concernant Alessandro sur son réseau social favori.

Également, elle aurait indiqué le prix de cette collection. Retrouvez l'estimation du témoin.

Flag : BZHCTF{748596}

Hints :

- De nombreux fichiers sont présents sur le disque dur de Félicien. Peut-être qu'un de ces derniers pourrait vous en dire plus sur l'identité de ce témoin ?
- Ce témoin déteste Elon Musk mais est un grand fan de Mark Zuckerberg.

Objectif du challenge :

Trouver le contrat présent dans le dump de Félicien et s'en servir pour pivoter sur les comptes de Gaspard afin de trouver le compte Threads et obtenir l'information clé.

Personnages impliqués :

Gaspard

Plateformes :

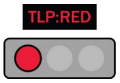
Instagram, Threads

Déroulé :

En examinant le contrat de travail trouvé sur le dump de Félicien, le joueur pourra pivoter sur la nouvelle identité afin de tomber sur le compte Instagram de Gaspard Chad. Plutôt actif, Gaspard a également lié son compte Threads à son Instagram. Sur son profil Threads, Gaspard émettra des doutes envers l'agent d'entretien tout juste recruté, Alessandro, et l'accusera au bout de plusieurs semaines d'avoir volé la collection de buste (estimée à 517 450€) de son patron.

Gaspard indiquera également avoir dénoncé Alessandro à la police et fait arrêter ce dernier.

Le joueur pourra aussi en apprendre plus sur Gaspard en parcourant son compte Tumblr (pas obligatoire pour l'intrigue).

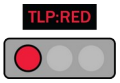


Flag à retrouver :

BZHCTF{517450}

Éléments à fournir aux joueurs :

- Aucun



Challenge 6 - The Dark Knight :

Scénario donné au joueur :

Alessandro a été arrêté et interrogé par l'officier Antoni DUMOULINI. Le suspect semble avoir été persuadé d'indiquer l'endroit où les bustes sont cachés ; retrouvez les coordonnées GPS de cet endroit.

Flag : BZHCTF{XX.XXXX, -X.XXXX}

Hints :

- Un outil permet de localiser avec précision des lieux. Cet outil, basé sur le langage OSM, est très utilisé en GEOINT.
- Les titres ont souvent une signification cachée.

Objectif du challenge :

Trouver l'endroit où ont été enterrés les bustes.

Personnages impliqués :

Gaspard

Plateformes :

Instagram, Threads

Déroulé :

Lors de l'interrogatoire, le personnage d'Alessandro dit avoir enterré les bustes dans un parc au nord de Rennes. Il détaille ensuite en indiquant les avoir placés sous une sculpture étrange, une sorte de pyramide inversée qui se trouve proche d'un point d'eau.

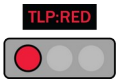
Le joueur pourra ainsi retrouver le lieu manuellement en liant les informations.

Il pourra également se servir d'Overpass Turbo avec le script suivant :

```
[out:json][timeout:999];
// gather results
(
  // query part for: “water”
  nwr["natural"="water"]({{bbox}});
)->.water;

(
  nwr(around.water:55)["tourism"="artwork"];
)->.artwork;

// print results
out body;
>;
out skel qt;
```



Flag à retrouver :

BZHCTF{48.1375, -1.6481}

Éléments à fournir aux joueurs :

- Interrogatoire audio

Challenge 7 - Chasseur ou chassé :

Scénario donné au joueur :

Félicitations, vous avez pu remonter les pistes et obtenir une compréhension globale de l'enquête. Toutefois, quelque chose ne fait pas sens.

Il semblerait que certaines informations que nous avions en notre possession avant votre arrivée étaient erronées.

Vous trouverez en pièces jointes le rapport d'enquête écrit par le responsable de l'affaire, Antoni DUMOULINI.

Démêlez le vrai du faux, collaborez avec les enquêteurs de votre service et retrouvez la collection volée.

Ce challenge comporte une grande partie SE/interactions sociales. Il est nécessaire de prendre rendez-vous avec ASTRE via le bot de ticketing.

Flag : BZHCTF{?}

Hints :

- Le rapport d'Antoni semble dévaluer le prix de la collection. Partagez l'information avec vos collègues.
- Il vous manque des informations. (**en cas de rejet de la part d'ASTRE**)
- N'hésitez pas à fouiller les lieux

Objectif du challenge :

Comprendre que le rapport donné par Antoni est un rapport trafiqué et retrouver les bustes.

Personnages impliqués :

Antoni DUMOULINI, officier de police judiciaire.

Plateformes :

Aucune

Déroulé :

Le joueur obtiendra deux rapports.

- Le premier, rapport d'enquête, constituera le rapport écrit par Antoni.
- Le second, rapport d'affectation, indiquera au joueur qu'il est actuellement affecté en tant que clandestin dans un service qui n'est originellement pas le sien afin de surveiller un potentiel corrompu, Antoni DUMOULINI.

En comparant les différents éléments (rapport d'Antoni, témoignages de Gaspard, audio/transcripts des interrogatoires entre Antoni et Alessandro), le joueur devra comprendre qu'Antoni ment.

Le joueur devra alors aller vers ASTRE pour expliquer sa compréhension du scénario.

Ici, deux choix :

- Si la compréhension du joueur est correcte, le joueur obtiendra une carte du Couvent qui indiquera où se trouve le bureau d'Antoni
- Si elle ne l'est pas, le joueur sera renvoyé sur son poste afin de mieux comprendre l'enquête.

À noter qu'au moment du challenge, les attendus de compréhension seront bien définis et qu'une telle pratique permet de filtrer les joueurs.

En possession de la carte, le joueur devra se diriger vers le bureau d'Antoni puis le fouiller. Il trouvera alors plusieurs choses intéressantes :

- Des factures importantes cachées dans le bureau ;
- Un kit de crochetage ;
- Un coffre-fort caché derrière des éléments de décor (livres, tableaux, etc.)

Le joueur devra alors crocheter le coffre-fort afin d'obtenir une carte du Couvent sur laquelle une zone est annotée. Le joueur devra trouver la zone et la fouiller afin de retrouver les bustes sur lesquels sont gravés le flag final.

Flag à retrouver :

BZHCTF{br4v0_p0uR_v0tR3_r3cRu7eMeNt}

Éléments à fournir aux joueurs :

- Bot de ticketing
- Rapport d'enquête écrit par Antoni
- Rapport d'affectation secret
- SE ASTRE
- Carte du couvent
- Kit de lockpicking