THEIVENDRAM HariHarani, 1R3

RAPPORT PFMP N°1

22 Novembre au 17 Décembre 2021 (soit 20 jours)

BNP PARIBAS

BACCALAUREAT PROFESSIONNEL SYSTEMES NUMERIQUES

Lycée Professionnel Gustave Ferrié,
7 Rue des Ecluses St Martin, 75010 Paris
01 42 02 19 55

SOMMAIRE

I. REMERCIEMENTS

Il m’est agréable à remercier M. Cyril RIGHI, manager de l’équipe Cyber Security Operation Center (SOC) de BNP Paribas, pour m’avoir donnée l’opportunité de réaliser ce stage.

D’autre part, je remercie plus particulièrement M. Aurélien CIRACQ et Mme. Patria AZZAM, mes tuteurs qui ont tenu le rôle de guide durant cette insertion professionnelle. Ils ont su me rassurer et me donner les moyens de concrétiser des projets en autonomie, ainsi qu’en équipe à leurs côtés. Merci à l’équipe Cyber SOC pour son soutien et son écoute, chacun a su rendre mon stage plus agréable et instructif.

Je remercie par ailleurs tous mes enseignants pour toutes les connaissances qu’ils m’ont inculquées. Je souhaite que le travail réalisé soit à la hauteur de leurs espérances.

II. INTRODUCTION

Du 22 novembre au 17 décembre 2021, j’ai effectué un stage au sein de l’entreprise BNP Paribas, située à Montreuil. Au cours de ce stage que j’ai réalisé dans le département du Cyber Security Operation Center (SOC), j'ai pu m'intéresser à la cybersécurité.

Plus largement, ce stage a été l'opportunité pour moi de comprendre mieux le monde de la cybersécurité. Mes maîtres de stage étant dans la threat intelligence, j'ai pu apprendre dans d'excellentes conditions.

L'élaboration de ce rapport a pour principale source, les différents enseignements tirés des tâches auxquelles j'étais affectées. Enfin, les nombreux entretiens que j'ai pu avoir avec les employés des différents services de la banque m'ont permis de donner une cohérence à ce rapport.

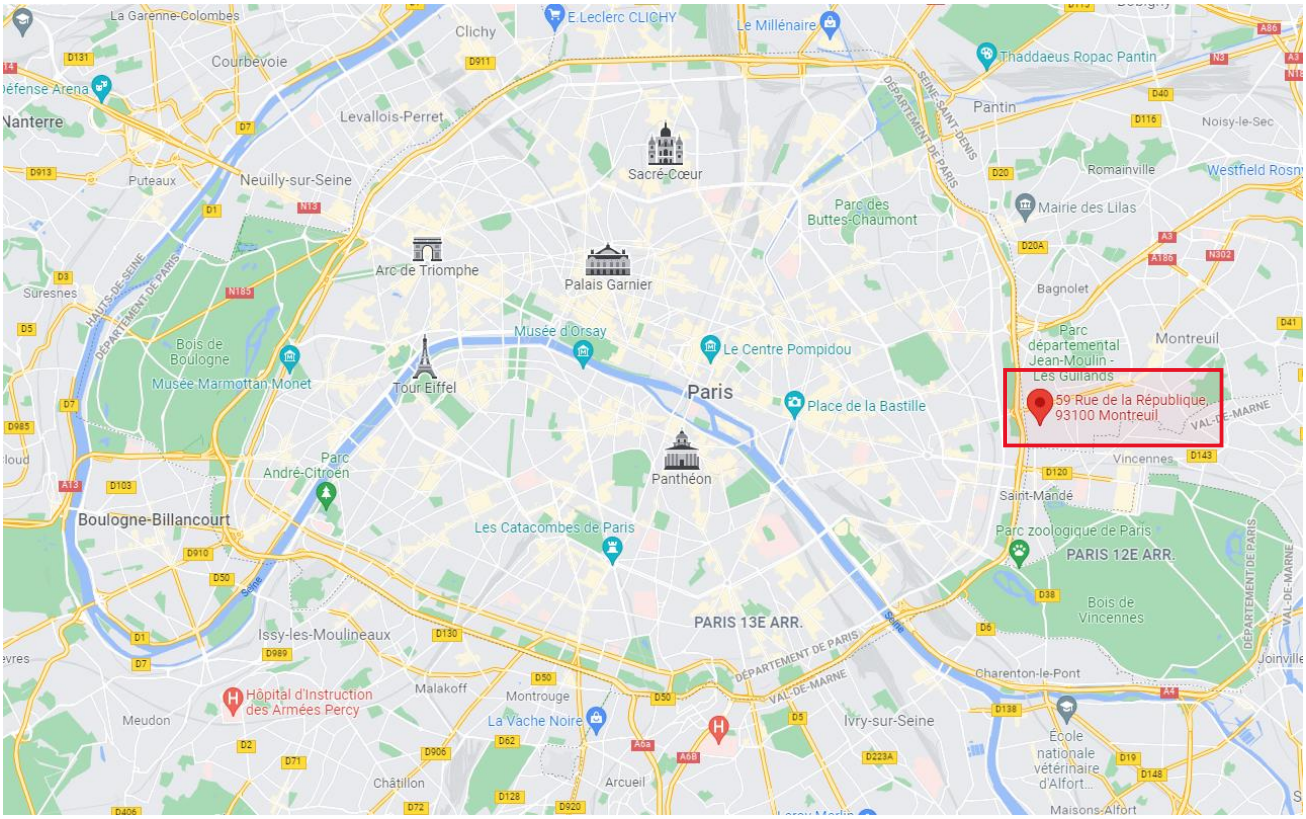
En vue de rendre compte de manière fidèle et analytique de la période passé au sein de BNP Paribas, il paraît logique de présenter à titre préalable l'environnement informatique du stage, à voir le secteur de la cybersécurité. Enfin, il sera précisé les différentes missions et tâches que j'ai pu effectuer au sein du département, et les nombreux apports que j'ai pu en tirer.

III. PRESENTATION DE L'ENTREPRISE

a. Coordonnées

Nom : BNP Paribas – Valmy 1
Adresse : 59 Rue de la République, 93100 Montreuil
N° de téléphone : 06 33 30 36 66
N° de Siret : 662 042 449 000 14

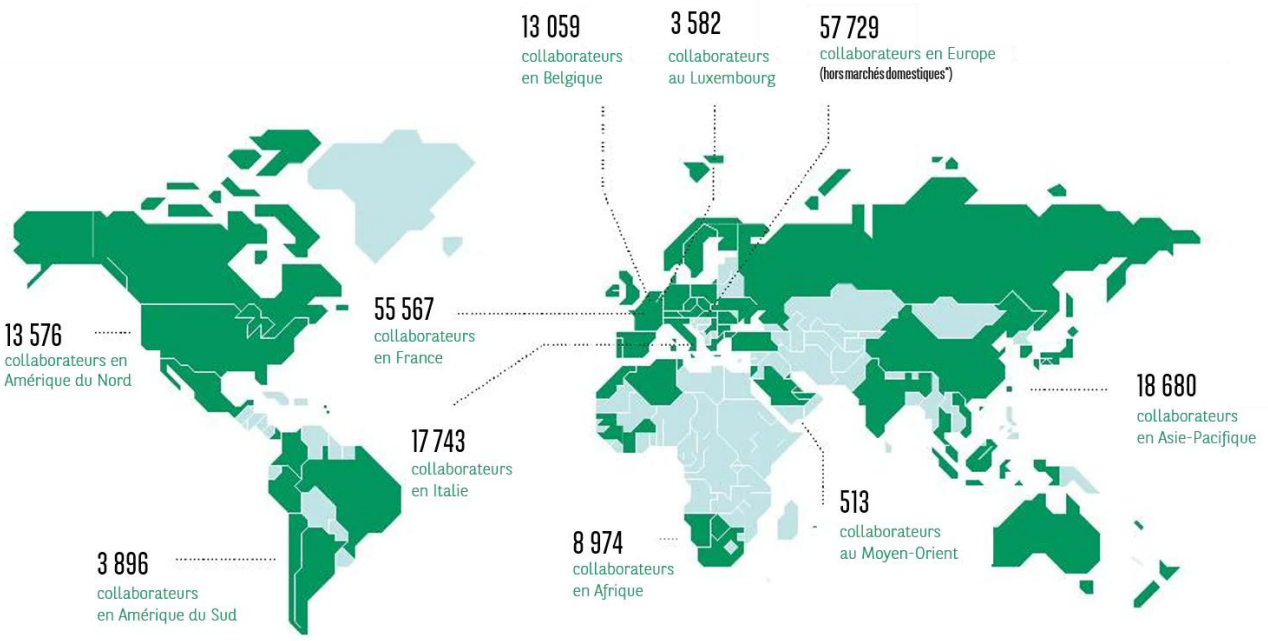
b. Situation géographique



c. Histoire de BNP Paribas dans la dimension économique

L'histoire de BNP Paribas débute au XIXème siècle, alors que les banques ancêtres du Groupe naissent et se développent. Entrainées par le formidable essor industriel de l'Europe, elles drainent l'épargne nécessaire au financement du développement économique. En remontant aux sources du Groupe, ce sont près de 2 siècles d'histoire du secteur de la banque, mais aussi d'histoire de l'Europe, voire du monde, que l'on peut parcourir.

BNP Paribas est présent dans 68 pays avec plus de 193 000 collaborateurs dont près de 148 000 en Europe. Le Groupe accompagne tous ses clients – particuliers, associations, entrepreneurs, PME-ETI, grandes entreprises et institutionnels – dans la réussite de leurs projets grâce à ses solutions de financement, d'investissement, d'épargne et de protection.



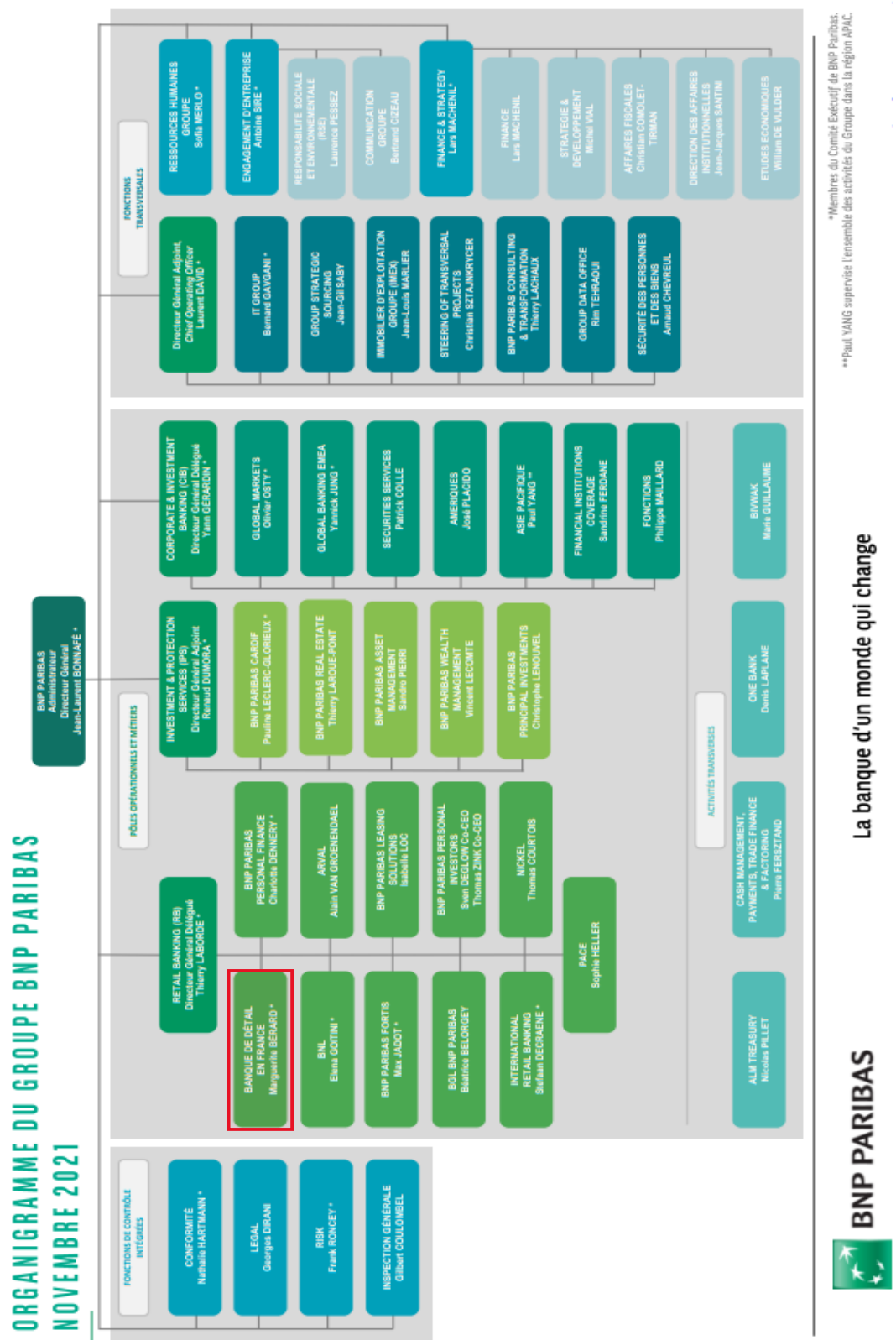
Quelques chiffres d'affaires en 2020 :

- **44,3Md€** Produit net bancaire
- **7,1Md€** Résultat net part du groupe
- **432 Md€** Réserve de liquidité immédiatement disponible
- **809 Md€** de crédits à la clientèle
- **1 165 Md€** d'actifs gérés par les équipes de l'Asset Management de BNP
- **396 Md€** de financement levé pour les clients sur les marchés de crédits syndiqués, d'obligation et d'actions
- **N°1 Mondial** avec 24.2 Md€ d'obligations durables à fin 2020

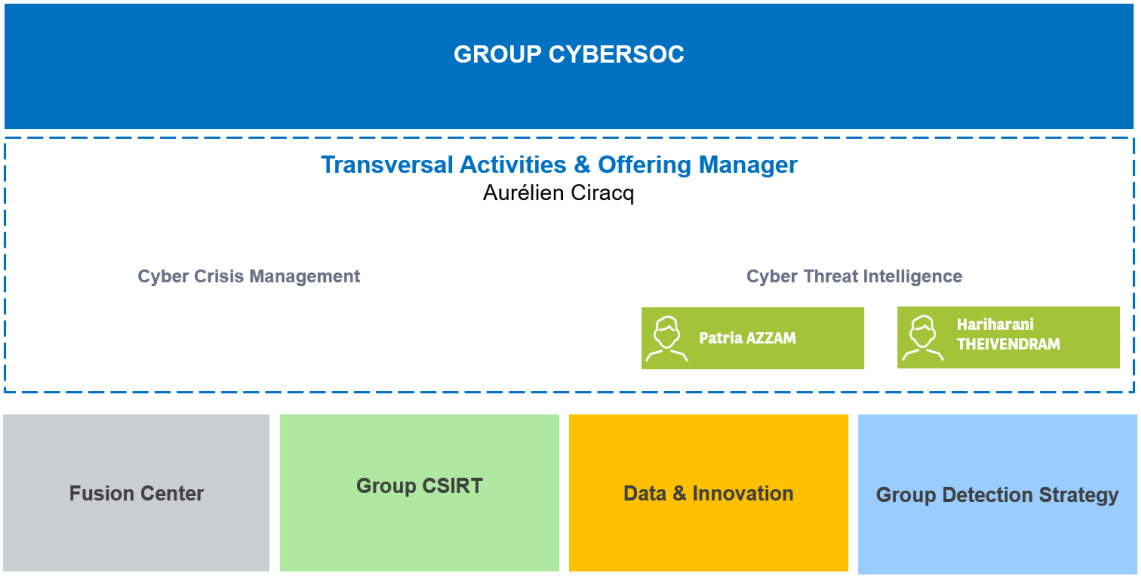
Dates importantes :

- 1822 : création à Bruxelles de la Société générale de Belgique
- 1848 : création du Comptoir National d'Escompte de Paris (CNEP) et Comptoir National d'Escompte de Mulhouse
- 1872 : création de la Banque de Paris et des Pays-Bas (Paribas)
- …
- 1966 : fusion du CNEP et de la BNCI pour former la banque Nationale de Paris (BNP)

d. Organigramme de l'entreprise



e. Organigramme du groupe CYBER SOC



Lors de mon stage, j'ai travaillé avec le groupe CYBER SOC. Voici les rôles des différentes activités du département :

- **Fusion center :** gère la gouvernance et gestion des risques de cyber-fraud (la fraude est une attaque commise dans l'intention de voler de l'argent à des clients ou à l'entreprise).

- **CSIRT (Computer Security Incident Response Team) :** s'occupe de faire la réponse aux incidents de sécurité cyber.

- **Data & Innovation** : pilote la collecte, la transformation et l'enrichissement des données dans le but d'augmenter les capacités d'investigation et de détection ainsi que d'automatiser tous les processus de pré et post détection.

- **Detection Strategy** : gère la gouvernance du programme Cyber SOC afin d'améliorer les capacités de détection du Groupe.

- **Transversal Activities & Offering Management** : définit et maintient la feuille de route des différents services du SOC. Cette activité inclut en plus :

    - **Cyber Threat Intelligence** : collecte d'information sur les incidents de cybersécurité qui ont touché d'autres entreprises pour améliorer la capacité de détection du Groupe.
    - **Cyber crisis management** : préparation d'un exercice d'entraînement, pour tester la procédure déjà défini afin d'être prêt lors d'une vraie attaque.

IV. COMPTE-RENDU D'ACTIVITES

Pendant mon stage, j'ai pu participer à divers :

Rencontres avec :

- Les membres de l'équipe SOC m'ont expliqué leurs rôles.
- Les Pentesters (penetration test) : qui m'ont permis de voir comment ils faisaient leurs tests d'intrusions c'est-à-dire, simuler une attaque d'un utilisateur mal intentionné, pour évaluer la sécurité d'un système d'information.

Réunions :

J'ai participé à des réunions en Visio-conférences sur les thématiques suivantes :

- **Purple Team :** Cette équipe a le rôle d'interfacer avec la « blue team » (défenseur) et la « red team » (testeur) afin d'améliorer la défense du système d'information (SI).
- **Phishing :** Ce type d'attaque permet au fraudeur de se faire passer pour un organisme connu (exemple-une banque) pour tromper la victime. Ainsi, il va envoyer un mail, avec un lien vers des sites web infectés, pour voler les coordonnées bancaires de la cible.
- **Cyber Crisis exercice**

Formations :

J'ai participé aux formations ci-dessous qui sont obligatoire pour tous les employés :

- **Sensibilisation sur la cybersécurité**
- **Sécurisation des bureaux :**

Le badge d'un collaborateur chez BNPP est très important car c'est son passeport et il doit l'avoir toujours sur soi. Ce badge couvre plusieurs niveaux de sécurité :

- Les accès physiques : pouvoir badger à l'entrée du bâtiment, la circulation entre les étages et pour le Groupe SOC, l'accès à l'espace sécurisés aux personnes qui y travaillent.
- Les accès logiques : utiliser pour la connexion du poste professionnelle et authentification sur les applications de travail par le certificat présent sur la carte à puce. Lorsque l'on quitte le bureau, il faut toujours :
    1. Verrouiller les fenêtres
    2. Fermer la session de l'ordinateur
    3. Ranger les documents dans les placards et les fermer à clefs.
    4. Détruire les documents à jeter.

Activités personnelles :

Veille média (Média Watch en anglais) : lecture des actualités mondiales pour suivre les dernières menaces, vulnérabilités et attaques cyber.

V. ETUDE DE CAS

➔ Introduction

Emotet est un cheval de Troie[1] qui cible des données bancaires. L'objectif de ce cheval de Troie est d'accéder aux appareils des personnes et d'espionner leurs données privées sensibles. Emotet est capable de tromper les programmes antivirus sans se faire détecter. Une fois l'appareil infecté, le programme se propage comme un ver informatique[2].

Emotet se propage principalement via des spams. Ce mail contient un lien malveillant ou un document infecté. En cliquant sur le lien ou en téléchargeant le document, un autre malware se télécharge automatiquement sur l'appareil.

Emotet a été détecté pour la première fois en 2014. Les cibles de ce cheval de Troie étaient les clients des banques allemandes et autrichiennes. Le programme est parvenu à accéder aux données de connexions des clients. Au fil du temps, ce programme s'est propagé dans le monde entier.

D'un cheval de Troie ciblant les données bancaires, Emotet est devenu un dropper[3]. Ce sont ces chevaux de Troie qui sont responsables des dégâts que nous rencontrons sur nos systèmes. Dans la plupart des cas, les programmes suivants ont été déposés :

1. **Trickbot :** cheval de Troie ciblant les données bancaires, qui tente d'accéder aux données des connexions des comptes bancaires.

2. **Ryuk :** cheval de Troie de chiffrement, également appelé ransomware[4] (ou cryptotrojan).

1 C'est un programme malveillant utiliser pour infecter le système PC cible et causer l'activité malveillante pour voler des informations personnelles.
2 Logiciel malveillant qui se reproduit sur plusieurs ordinateurs en utilisant un réseau informatique comme Internet.
3 Dropper (anglais) une forme minimaliste du cheval de Troie, appelé programme seringue ou virus compte-gouttes est un programme informatique crée pour installer un logiciel malveillant comme cible.
4 Rançongiciel (français) est un logiciel informatique malveillant, prenant en otage les données.

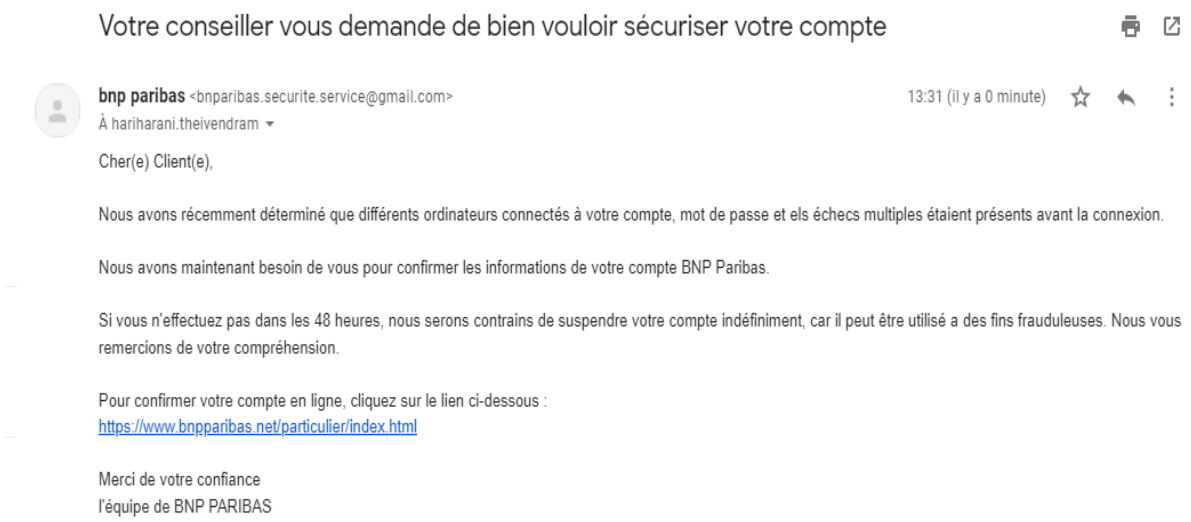
Emotet fait une collecte Outlook. Il lit les emails des utilisateurs déjà affectés et crée un contenu faussement authentique. Emotet envoie ces mails de phishing aux cibles. Généralement, les emails contiennent un lien ou un document Word dangereux que le destinataire est supposé télécharger. Les destinataires sont ainsi aveuglés par un faux sentiment de sécurité car ce mail semble parfaitement normal.

Une fois qu'Emotet a accès au réseau, il peut se propager tranquillement. Il essaie de trouver les mots de passe à l'aide de la méthode de force brute[1]. Une autre méthode qui figure les vulnérabilités sous Windows, autorisent l'installation du programme malveillant sans intervention humaine.

➔ Problématique :

Comment se protéger de ce Cheval de Troie ?

Prenons l'exemple de la banque. On reçoit un mail **soupçonneux** et on l'ouvre.
Exemple :


Votre conseiller vous demande de bien vouloir sécuriser votre compte

bnp paribas <bnparibas.securite.service@gmail.com> 13:31 (il y a 0 minute)
À hariharani.theivendram

Cher(e) Client(e),

Nous avons récemment déterminé que différents ordinateurs connectés à votre compte, mot de passe et els échecs multiples étaient présents avant la connexion.

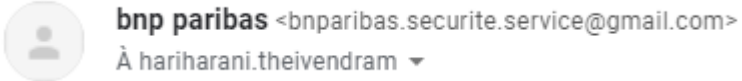
Nous avons maintenant besoin de vous pour confirmer les informations de votre compte BNP Paribas.

Si vous n'effectuez pas dans les 48 heures, nous serons contrains de suspendre votre compte indéfiniment, car il peut être utilisé a des fins frauduleuses. Nous vous remercions de votre compréhension.

Pour confirmer votre compte en ligne, cliquez sur le lien ci-dessous :
https://www.bnpparibas.net/particulier/index.html

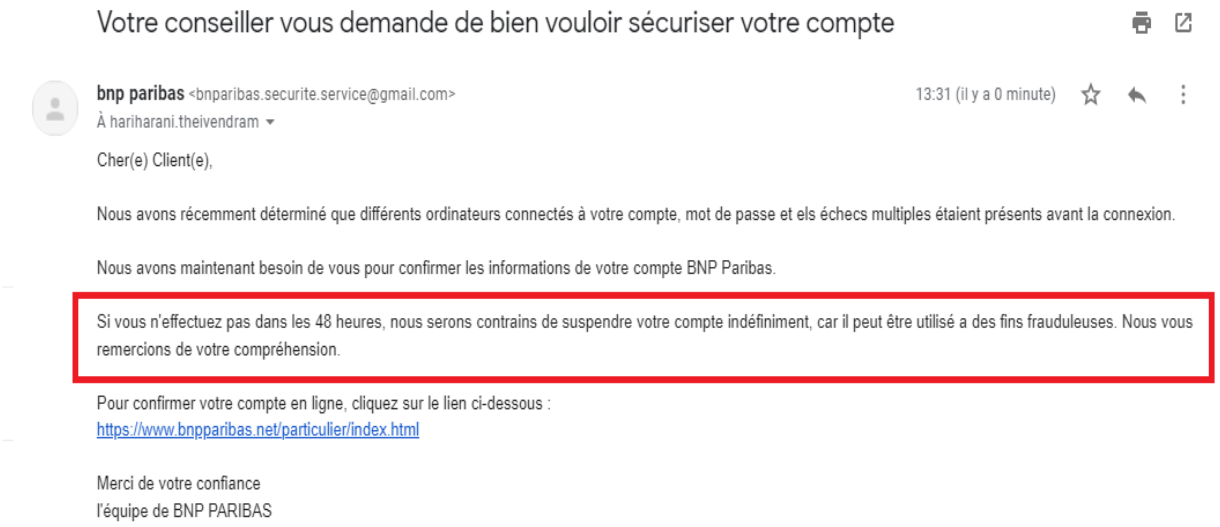
Merci de votre confiance
l'équipe de BNP PARIBAS

<u>Etape 1 :</u> De qui provient ce mail ?


bnp paribas <bnparibas.securite.service@gmail.com>
À hariharani.theivendram

On doit toujours vérifier de qui provient le message. Ici, on voit clairement que ce n'est pas un collaborateur de BNP Paribas.

Etape 2 : Le contenue



Votre conseiller vous demande de bien vouloir sécuriser votre compte

bnp paribas <bnparibas.securite.service@gmail.com> 13:31 (il y a 0 minute)
À hariharani.theivendram

Cher(e) Client(e),

Nous avons récemment déterminé que différents ordinateurs connectés à votre compte, mot de passe et els échecs multiples étaient présents avant la connexion.

Nous avons maintenant besoin de vous pour confirmer les informations de votre compte BNP Paribas.

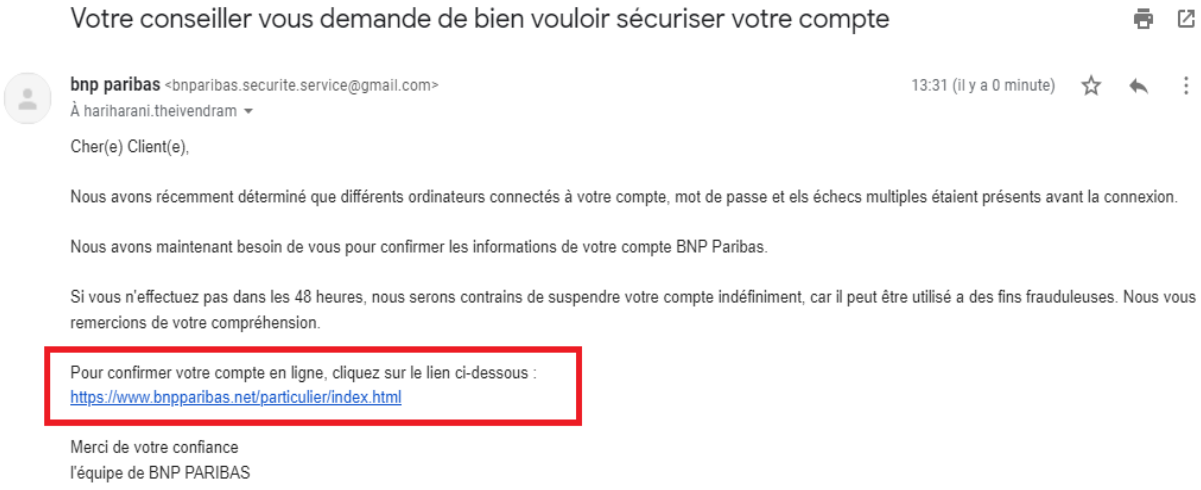
Si vous n'effectuez pas dans les 48 heures, nous serons contrains de suspendre votre compte indéfiniment, car il peut être utilisé a des fins frauduleuses. Nous vous remercions de votre compréhension.

Pour confirmer votre compte en ligne, cliquez sur le lien ci-dessous :
https://www.bnpparibas.net/particulier/index.html

Merci de votre confiance
l'équipe de BNP PARIBAS

En regardant bien le contenue, nous voyons que l'attaquant insiste sur le fait que nous devons nous connecter dans un délai de 48h.

Etape 3 : Le lien



Votre conseiller vous demande de bien vouloir sécuriser votre compte

bnp paribas <bnparibas.securite.service@gmail.com> 13:31 (il y a 0 minute)
À hariharani.theivendram

Cher(e) Client(e),

Nous avons récemment déterminé que différents ordinateurs connectés à votre compte, mot de passe et els échecs multiples étaient présents avant la connexion.

Nous avons maintenant besoin de vous pour confirmer les informations de votre compte BNP Paribas.

Si vous n'effectuez pas dans les 48 heures, nous serons contrains de suspendre votre compte indéfiniment, car il peut être utilisé a des fins frauduleuses. Nous vous remercions de votre compréhension.

Pour confirmer votre compte en ligne, cliquez sur le lien ci-dessous :
https://www.bnpparibas.net/particulier/index.html

Merci de votre confiance
l'équipe de BNP PARIBAS

Lorsqu'on soupçonne un mail frauduleux, il ne faut JAMAIS cliquer sur le lien.
C'est le lien malveillant.
Si la victime clique sur le lien et rentre ses coordonnées bancaires, cela permettra à l'attaquant de les voler. Ensuite, il fera des virements.

Etape 4 : La contamination d'Emotet

Une fois qu'Emotet a accès au réseau, il peut se propager tranquillement. Il essaie de trouver les mots de passe à l'aide de la méthode de force brute[1]. Une autre méthode qui figure les vulnérabilités sous Windows, autorisent l'installation du programme malveillant sans intervention humaine.

<u>Etape 5 :</u> Compte vide

Lorsque la victime aura remarqué qu'il y a eu des virements, il va appeler la banque et la banque dira que ce n'était pas eux.

<u>Etape 6 :</u> Comment ça se passe chez BNP Paribas ?

Chez BNPP, chaque collaborateur à son propre PC et Téléphone Portable professionnelle. Seuls les membres de BNP peuvent communiquer entre eux. Lorsqu'ils reçoivent un mail externe, leurs messageries affichent « [EXTERNAL] ». Si ce mail externe contient un fichier ou un lien malicieux, ce mail est envoyé à l'équipe CSIRT pour vérifier s'il s'agit bien d'un phishing et prendre les mesures ci-nécessaires.

Emotet est le programme le plus complexe et le plus dangereux de l'histoire de la cybercriminalité. Le virus est polymorphe[2].

Selon le FCO (Federal Criminal Office), l'infrastructure du programme malveillant Emotet a été anéantie et mise hors d'état de nuire en janvier 2021. Les autorités ukrainiennes ont été en mesure de prendre le contrôle de l'infrastructure et ont saisi de nombreux ordinateurs et disques, de l'argent et des lingots d'or. L'opération dans son ensemble a été coordonnée par Europol et Eurojust, l'organisme de l'Union européenne de coordination juridique pour la gestion des affaires criminelles.

En prenant le contrôle, les autorités ont réussi à rendre les systèmes affectés des victimes allemandes inutilisables par les auteurs de l'attaque. Pour les empêcher de reprendre le contrôle, les forces opérationnelles ont placé en quarantaine le programme malveillant sur les systèmes affectés des victimes.

1 Méthode pour trouver le mot de passe ou la clé cryptographique afin de pouvoir accéder à un service en ligne, à des données personnelles ou un ordinateur.
2 Son code change légèrement à chaque fois qu'il y a un accès.

➔ Frise chronologique d'Emotet

2014
- le début d'Emotet : première détection en ciblant les clients des banques allemandes et autrichiennes

2018
- Infection de l'hôpital allemand Fuerstenfeldbruck

2019
- Janvier : découverte que les appareils Apple était infectés
- Septembre : Cour d'appel de Berlin
- Décembre : Université de Giessen

2020
- Février : découverte que le logiciel attaque les réseaux Wi-Fi

2021
- Janvier : destruction d'Emotet
- Novembre : Retour d'Emotet

VI. SYNTHESE

Il va de soi que la différence entre le monde de l'école et celui de l'entreprise est très importante. Ce stage de 4 semaines au sein du groupe SOC et sur un site aussi important m'a permis de découvrir la réalité du monde cyber.

L'accueil de l'entreprise de BNP Paribas étant bien préparé et détendu, cela m'a mis immédiatement en confiance avec l'équipe. D'autant plus que mes tuteurs de stage m'ont apporté toute l'aide dont j'avais besoin. Une bonne ambiance règne dans l'équipe et tous les personnels ont été très coopératifs et attentif à toutes mes questions. Le travail d'équipe est très important car tous les services sont liés et doivent communiquer entre eux.

Cette expérience est enrichissante tant du côté technique que du côté humain : c'était l'occasion de mener des projets, d'une manière totalement autonome avec une liberté de choix ainsi que d'acquérir des responsabilités, des connaissances, des capacités d'organisation, d'être précis et efficace et surtout constater des rapports humains.

Je remercie une fois de plus toutes les personnes que j'ai rencontrées pour m'avoir permis de mener à bien mes projets et de m'avoir accordé leurs confiances et leur sympathie durant cette période de stage.