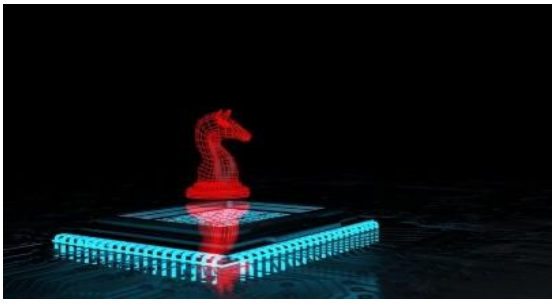
ETUDE DE CAS

➔ 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 :

> **Trickbot :** cheval de Troie ciblant les données bancaires, qui tente d'accéder aux données des connexions des comptes bancaires.
>
> **Ryuk :** cheval de Troie de chiffrement, également appelé ransomware[4] (ou cryptotrojan).

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.

---

[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.

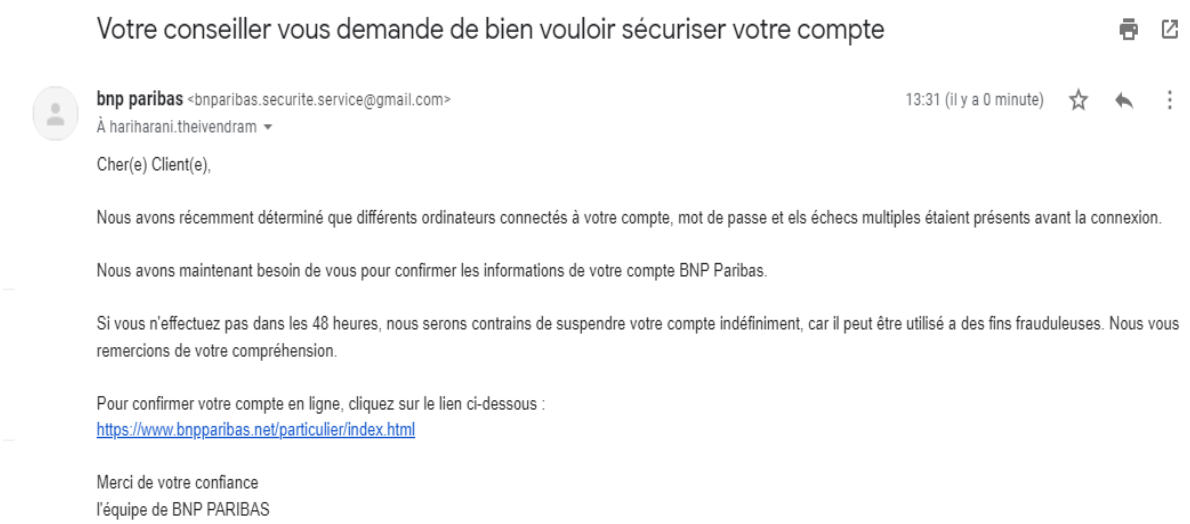
3 Dropper (anglais) une forme minimaliste du cheval de Troie, appelé programme seringue ou virus compte-gouttes est un programme informatique crée pour installer un logiciel malveillant comme cible.

4 Rançongiciel (français) est un logiciel informatique malveillant, prenant en otage les données.

➔ 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.

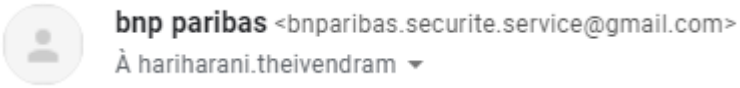
Nous avons maintenant besoin de vous pour confirmer les informations de votre compte BNP Paribas.

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

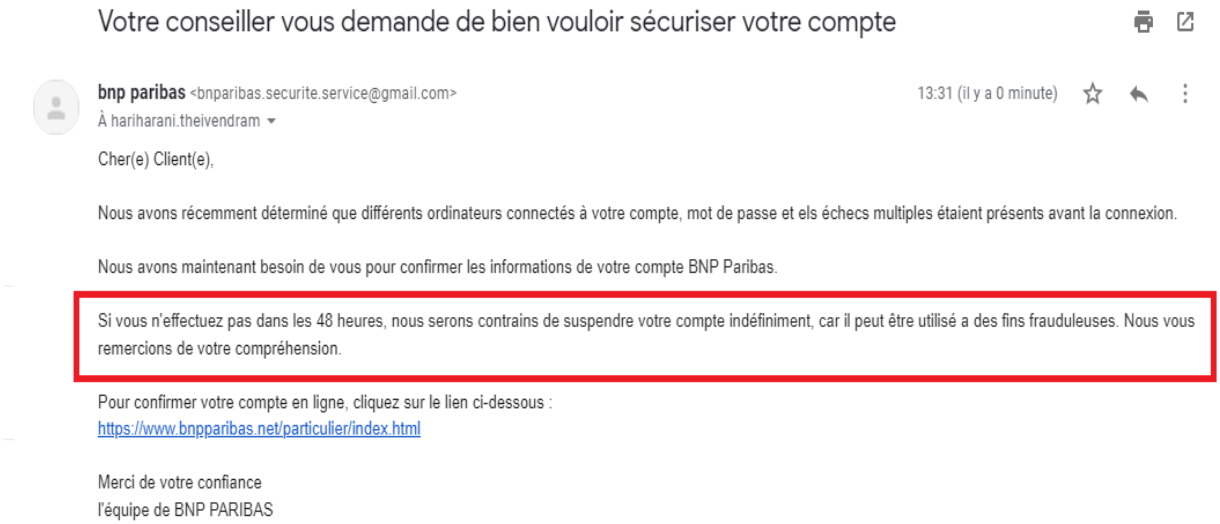
Merci de votre confiance
l'équipe de BNP PARIBAS

<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.

<u>Etape 2</u> : 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.

<u>Etape 3</u> : 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.

<u>Etape 4 :</u> 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.

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.

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.

➔ 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

2 Son code change légèrement à chaque fois qu'il y a un accès.