THEIVENDRAM
Hariharani

EMOTET

BTS SIO – SISR

2023/2024 – 2024/2025

SOMMAIRE

Table des matières

I. INTRODUCTION

1. Qu'est-ce que Emotet ?

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.

2. Première apparition

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).

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.

---

[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.

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.

3. Qui Emotet cible-t-il ?

Emotet ciblait principalement des entreprises, alors que maintenant il vise majoritairement les particuliers. De nombreuses entreprises n'ont pas voulu signaler par crainte de salir leurs réputations mais aussi de faire l'objet de faire l'objet de nouvelles attaques.

4. Quels sont les appareils exposés à Emotet ?

Ce cheval de Troie étaient uniquement détectées sur les systèmes d'exploitation les plus récentes de Windows. Au début de 2019, les chercheurs l'ont découvert sur les ordinateurs Apple. Grâce à un mail frauduleux, les attaquants piégeaient les utilisateurs. L'email indiquait que l'entreprise avait « restreint l'accès à son compte ». Les victimes ont cliqué sur le lien pour éviter la désactivation de leurs comptes et la suppression de leurs services Apple.

5. Comment se propage-t-il ?

Emotet fait une collecte Outlook. Il lit les mails 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 dentinaires 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. Une autre méthode qui figure les vulnérabilités sous Windows, autorisent l'installation du programme malveillant sans intervention humaine.

6. L'infrastructure du programme réduit à néant

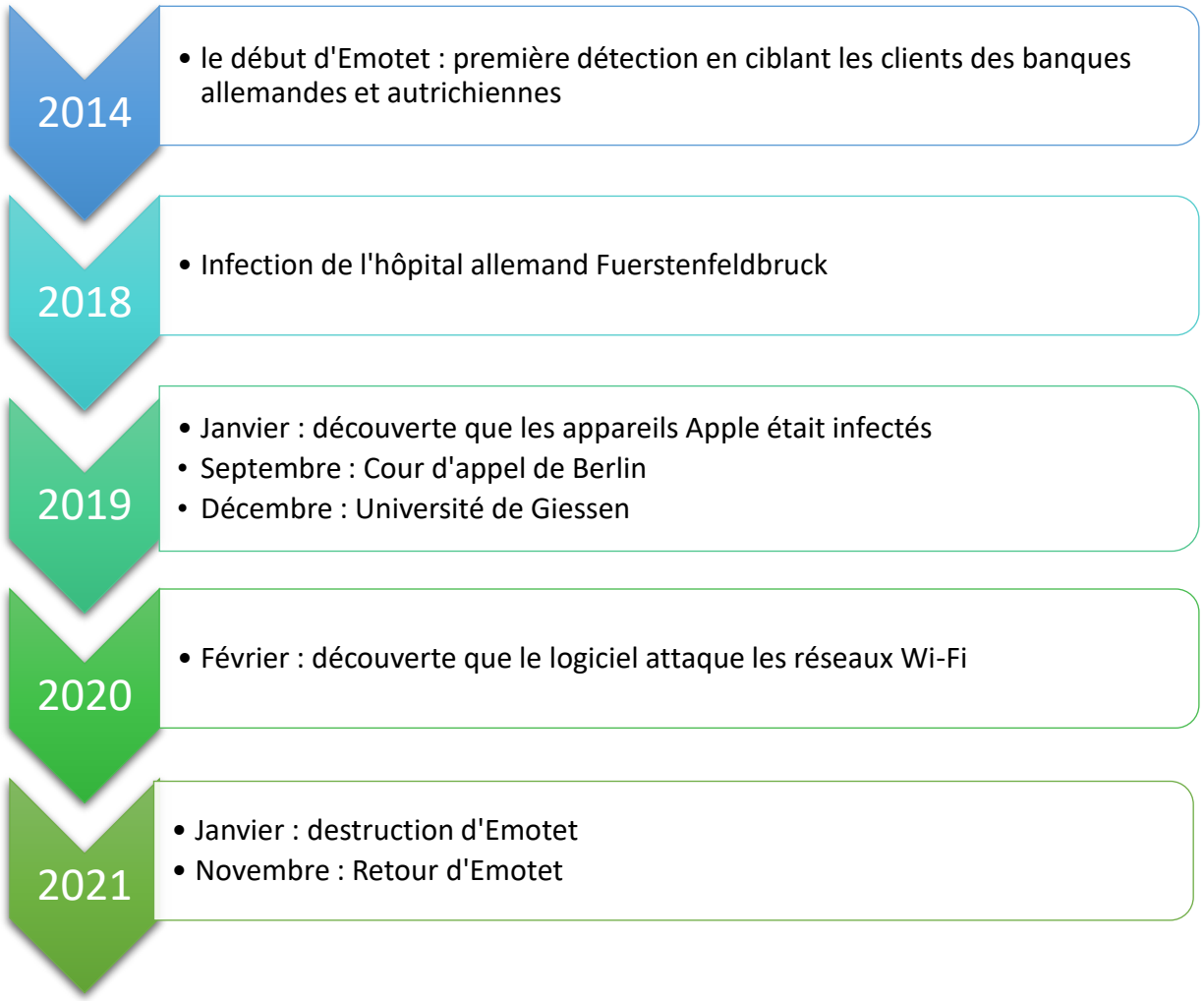
A la fin du mois de janvier 2021, le Bureau du procureur général de francfort – le bureau central de la lutte contre la cybercriminalité et le bureau fédéral des affaires criminelles ont annoncé qu'Emotet avait été « contrôlé et réduite » dans le cadre de l'effort international.

7. Le retour d'Emotet

Divers experts en cybersécurité ont indiqué un regain d'activité du logiciel malveillant Emotet en novembre 2021. L'alerte a été donnée par Cryptolaemus, un groupe de chercheurs en sécurité qui s'est spécialisé dans la lutte contre Emotet.

Cryptolaemus explique qu'une nouvelle version d'Emotet a été observée et qu'elle utilise particulièrement des machines qui s'étaient autrefois retrouvées infectées par un autre malware, Trickbot.

8. Frise chronologique d'Emotet



II. ACTUALITES

1. 13/02/2022 : Contamine des PC via WiFi

https://www.phonandroid.com/emotet-ce-dangereux-cheval-de-troie-contamine-dautres-pc-via-wi-fi.html

Il ne se contente pas de se connecter aux réseaux connus : il attaque les autres réseaux un par un via brute force, c'est-à-dire que le module va tester une par une toutes les combinaisons possibles de chaque réseau alentours dont il ne connait pas le mot de passe. Cette méthode, mois efficace que l'attaque par dictionnaire par exemple, ne lui permet donc de se connecter qu'à des réseaux dont le mot de passe est relativement court et simple.

Néanmoins, on voit bien ce nouveau vecteur d'attaque fonctionner dans certains réseaux WiFi d'entreprises ou résidentiels dont les mots de passe sont volontairement simples. Une fois que le virus a accès au réseau, il tente de deviner les mots de passe des machines qui y sont connectées via la même méthode, pour ensuite s'y copier et les inoculer. En cas de succès, le cycle peut recommencer et l'infection se propager.

Binary Defense note que toutes les versions de Windows sont potentiellement touchées par ce malware, à l'exception de Windows XP – à cause de son grand âge et du fait que le trjoan utilise des fonctionnalités récentes de Windows. Cette variante du malware existerait depuis avril 2018, mais il n'avait pas été détecté jusqu'ici. Binary Defense conseille donc plusieurs choses pour éviter sa propagation. D'abord, renforcer la sécurité des réseaux wifi, y compris dans les locaux des entreprises.

Autrement dit : fini les mots de passe simplistes, seuls à pouvoir être découverts par brute force. Ce conseil est particulièrement valable dans les espaces partagés, par exemple les plateaux d'immeubles loués par plusieurs entreprises pour y installer leurs open space, chacune avec leur réseau WiFi propre : les employés d'une entreprise B peuvent y être infectés par des ordinateurs de l'entreprise A à leur insu.

2. 14/06/2022 : Vol de données bancaires sur Chrome

https://www.phonandroid.com/le-malware-emotet-est-de-retour-sur-chrome-pour-voler-les-donnees-de-votre-carte-bancaire.html

Emotet tente d'infecter les victimes potentielles avec un module de vol de cartes de crédit conçu pour récolter les informations relatives aux cartes de crédit stockées dans les profils des utilisateurs de Google Chrome. Il se propage principalement par le biais de courriers indésirables et incite les utilisateurs à cliquer sur les fichiers et le sliens infectés. A l'origine, le virus Emotet était utilisé pour accéder aux informations sensibles et privées d'appareils étrangers.

Une fois les données exfiltrées, y compris le nom d'utilisateur, les numéro de carte et les informations de carte de crédit dans leur profil. Comme toujours avec les menaces de logiciels malveillants, il existe quelques bonnes pratiques que vous pouvez mettre en place pour vous protéger de cette menace. Puisqu'il est largement diffusé par le biais des mails, on ne peut donc

que vous conseiller de ne jamais cliquer sur une pièce jointe ou un lien d'un mail suspect.

3. 04/11/2022 : Chambre des Notaires de Paris

https://www.phonandroid.com/emotet-le-terrible-botnet-revient-en-se-faisant-passer-pour-la-chambre-des-notaires-de-paris.html

Emotet utilise dorénavant des documents qui prennent en charge les macros afin de récupérer la charge utilise du virus à partir de serveurs de contrôle et commande gérés par les pirates. Pour ce faire, les opérateurs viennent de lancer une nouvelle campagne de phishing qui exploite notamment le nom et l'image de la Chambre des Notaires de Paris

4. 14/03/2023 : fichier joint pesant plus de 500Mo

https://www.phonandroid.com/le-terrible-malware-emotet-est-de-retour-dans-votre-boite-mail-mefiez-vous-des-fichiers-joints.html

Cela dit, le malware ne peut pas s'exécuter tout seul. Au moment d'ouvrir le fichier joint, les victimes doivent autoriser la modification du document Word. Cela a pour effet de déclencher une macro, et d'installer Emotet. Celui-ci télécharge alors des utilitaires lui permettant de voler les mots de passe de votre système et de votre client mail, mais aussi un module de spam.