Revue de presse des Cybermenaces

Com CyberGend

#4 – Avril 2022

Département Fusion et analyse de la menace
revue-presse-comcybergend@gendarmerie.interieur.gouv.fr

A retenir

L'actualité Cyber reste dense ce mois-ci avec les tensions internationales et de nouvelles recherches enrichissant notre connaissance de la menace. En complément, nous vous proposons de débuter ce mois-ci une série d'articles sur l'escroquerie au président, une fraude bien huilée faisant de nombreuses victimes parmi les entreprises françaises. Bonne lecture.

Le chiffre du mois

1082 Il s'agit du nombre d'intrusions avérées dans des systèmes d'information rapportées à l'ANSSI en 2021, soit une hausse de 37 % sur un an. Ceci s'explique par une fragilité numérique importante offrant ainsi de nombreuses opportunités à des acteurs malveillants qui se professionnalisent et se spécialisent de plus en plus. Source : ANSSI

Informations générales

L'ANSSI a publié son « panorama de la menace informatique » début mars. Ce document revient sur les grandes tendances de 2021 et propose quelques perspectives d'évolution. Comme l'indique le chiffre du mois (Cf. ci-dessus), le niveau de menace est en hausse. L'ANSSI cite notamment : une porosité entre des profils d'attaquants étatiques et criminels, le développement de capacités offensives par des entreprises privées, des campagnes d'espionnage moins visibles mais qui restent la principale finalité poursuivie par les attaquants étatiques et qui constituent l'essentiel de l'activité traitée par l'ANSSI. Pour finir, l'agence anticipe des opérations d'influence et de déstabilisation notamment à l'approche d'évènements majeurs en France (coupe du monde de Rugby, Jeux Olympiques...).

Informations sur la menace

Le groupe Cybercriminel **Conti** spécialisé dans les rançongiciels a été ciblé par de nombreuses fuites d'information. Des conversations internes ainsi que le code source du rançongiciel ont été publiés. Cette fuite serait l'œuvre d'un chercheur ukrainien en sécurité informatique et fait suite à la prise de position du groupe Cybercriminel en faveur de la Russie. Pour autant, la franchise poursuit ses activités, remontant son infrastructure après que celle-ci ait été largement exposée par ces fuites.

Déchiffrement des données issues du rançongiciel **Hive** : des chercheurs ont identifié une vulnérabilité dans l'utilisation des moyens cryptographiques permettant de générer et stocker les clés de chiffrement. Les chercheurs ont déclaré avoir réussi à tirer parti de cette faille pour concevoir une méthode permettant de récupérer de manière fiable plus de 95 % des clés utilisées lors du processus de chiffrement.

Une nouvelle analyse réalisée par Chainalysis suggère que **74% des revenus générés** en 2021 par des **attaques de type rançongiciel** sont allés à des groupes « hautement susceptibles d'être affiliés à la Russie ». Selon les chercheurs, cela représente plus de 400 millions de dollars de paiements en crypto-monnaies.

La Commission nationale de l'informatique et des libertés (CNIL) annonce la mise en demeure d'un éditeur de site web utilisant l'outil **Google Analytics**. Dans son communiqué, la CNIL qualifie d'« illégaux » ces transferts de données vers les Etats-Unis. Source : CNIL

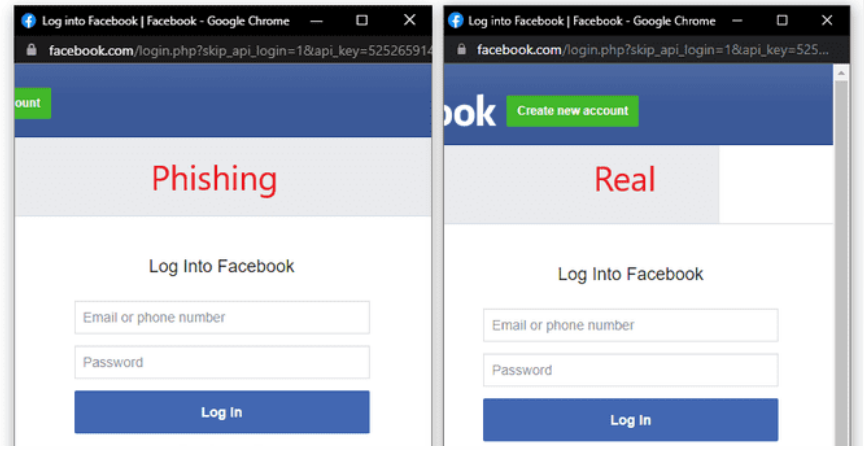
Roblox est une plateforme permettant aux utilisateurs de créer et de jouer ensemble à des jeux. C'est un moyen de se connecter, en temps réel, avec d'autres personnes dans un monde numérique. Cette plateforme est largement utilisée par des enfants (deux tiers des enfants entre 9 et 12 ans aux Etats-unis utiliseraient cette plateforme).
Quel est le risque ? Des utilisateurs détournent régulièrement le jeu (et transgressent les règles d'utilisation) pour se livrer à des jeux mimant virtuellement des actes sexuels incluant des discussions explicites. S'agissant d'un jeu, des mineurs peuvent ainsi facilement se trouver confrontés à ces pratiques sans présence d'adulte pour en contrôler l'usage. Source : BBC

Attention aux **licences Windows ou office vendues à bas prix** : Les Numériques a mené l'enquête sur les clés d'activation à bas coût et leur légalité.

Europol alerte sur le commerce de **fausses puces informatiques** dans son dernier rapport sur les crimes contre la propriété intellectuelle. Les téléphones mobiles et leurs accessoires font partie des équipements les plus touchés.

Nouvelles techniques d'attaque

Nouvelle attaque « Browser In The Browser » (BITB) : un chercheur a publié une nouvelle technique pour créer de faux formulaires de connexion. Le principe consiste à recréer la barre d'adresse du navigateur en plus du formulaire ce qui permet d'afficher une adresse licite et éviter toute suspicion de l'utilisateur qui pensera être sur le site légitime. Ceci pourrait être utilisé par des personnes malveillantes pour conduire de nouvelles attaques d'hameçonnage.



Exemple du « BITB » avec la page de connexion de Facebook : à gauche le site contrefait, à droite le site officiel.

Les deux affichent bien l'adresse « facebook.com »

Principales cyberattaques

- Informations sur les tensions internationales : l'ANSSI a édité une page spécifique mise à jour régulièrement sur l'état de la menace ainsi que sur des recommandations.
- **Serpent**, une nouvelle attaque ciblant des entreprises françaises : l'éditeur Proofpoint a découvert une nouvelle attaque ciblant des entreprises françaises dans le bâtiment et l'immobilier ainsi que dans le secteur public. Cette attaque prend la forme d'un document Microsoft Word en lien avec le règlement général sur la protection des données (RGPD) contenant une *macro* malveillante. Cette dernière va utiliser le composant *OpenSource* nommé « Chocolatey » permettant de déployer des paquets d'installation afin d'exécuter une porte dérobée nommée **Serpent**. L'objectif final de ce logiciel malveillant est encore inconnu.
- Le groupe Cybercriminel **Lapsus$** a fait de nouvelles victimes ce mois-ci. Après NVIDIA, Samsung, Ubisoft et Okta, c'est une partie du code source du moteur de recherche Bing de Microsoft ainsi que Maps et Cortana qui aurait été dérobé.

Le fait marquant : l'escroquerie au président (1/3)

Parmi les cybermenaces qui pèsent sur les entreprises, l'« **escroquerie au président** » figure parmi les **plus importantes en terme d'impact humain et financier**. A titre d'exemple, Le Parisien présentait en décembre dernier ce type de fraude subi par le promoteur immobilier Sefri-Cime qui a perdu pas moins de 33 millions d'euros.

Également appelé FOVI pour « faux ordre de virement international », l'escroquerie au président pourrait être la quintessence d'une habile manœuvre usant avec finesse de la confluence des technologies numériques et de l'ingénierie sociale.
Cette forme d'escroquerie, toujours préparée en amont, suit un schéma désormais éprouvé et parfaitement maîtrisé par les auteurs.

La première phase consiste à cibler une entreprise et rassembler des éléments sur celle-ci. L'auteur va alors rechercher les éléments disponibles en sources ouvertes, depuis son ordinateur et sans jamais bouger de son fauteuil. Après une phase initiale qui consiste à rechercher les éléments disponibles sur l'entreprise en regardant les éléments en ligne du registre du commerce, il va collecter les éléments sur le président (ou directeur), des données le concernant collectées sur des réseaux professionnels comme *LinkedIn* et des éléments plus personnels sur les réseaux sociaux. Les liens faits naturellement par les algorithmes de ces réseaux permettent assez facilement d'identifier tout ou partie des collaborateurs et ainsi cibler celui qui sera, au final, le vecteur (bien involontaire) de la fraude.

S'ajoute parfois dans ces recherches des « pêches miraculeuses » permettant de trouver sur internet des fac-similé de factures, des courriers et des signatures de cadres, voire du directeur lui-même.

A suivre...