Revue de presse des Cybermenaces

ComCyberGend

#6 – Juin 2022

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

A retenir

Ce mois de Juin signe le **retour en force de grands groupes Cybercriminels** : Emotet ou encore REvil. Plus de détails à ce sujet dans nos « *Informations sur la menace* ».

Nous vous parlions dans « *Le fait marquant* » de février de la probable poursuite et intensification de la vente d'outils offensifs. Cela semble se confirmer avec l'**augmentation du nombre de « *Zero day* »**, à lire dans notre rubrique « *Informations générales* ».

Le chiffre du mois

214 millions d'euros

Il s'agit du **montant cumulé d'amendes** jamais atteint **prononcé par la CNIL en 2021**. On notera également que 89 des 135 mises en demeure ont porté sur les *cookies*, l'une des thématiques prioritaires fixées par la CNIL pour cette année. Enfin, on retiendra la réception en 2021 de plus de 5000 notifications de violations de données (+79 %). Plus d'informations dans le rapport d'activité 2021 de la CNIL.

Informations générales

Vers une augmentation des « ***zero day*** » ? Le nombre de vulnérabilités non connues et exploitées avant leurs publications (et donc sans correctif) continue de croître. Même s'il est difficile d'estimer le nombre réel de ces vulnérabilités, cette hausse fait consensus dans la communauté de la sécurité informatique. Les **principaux utilisateurs** de ces « *zero days* » seraient **les Etats**, dans un but d'espionnage, suivis de près par **les cybercriminels** attirés par le gain financier. Les principales solutions ciblées sont, sans surprise, celles qui sont les plus répandues : Microsoft, Apple ou encore Google. Les organisations doivent **anticiper** ce type de menace et **se préparer** à y faire face. Plusieurs pistes : se mettre en capacité de lancer des mesures d'atténuation du risque (filtrage sur une liste noire de *pattern* d'attaque) ; se tenir informé au plus tôt des dernières vulnérabilités ; disposer d'un référentiel à jour de ses composants informatiques afin de pouvoir rapidement identifier les systèmes impactés par une vulnérabilité ; savoir définir ses priorités pour appliquer les correctifs (en tenant compte notamment de l'exposition, de l'existence de code d'exploitation public, de la présence de système critique) ; industrialiser au maximum le déploiement de correctifs.

Informations sur la menace

Face à la hausse du volume de **données pédopornographiques** sur Internet, l'**Union européenne** se dote de règles temporaires pour tenter d'endiguer le phénomène quitte à ce qu'il y ait des conséquences sur le respect de la vie privée. « Cet accord est un compromis » estime le rapporteur de cette législation. Source : Clubic.

Emotet est de retour après une pause de près de 10 mois. Cette interruption a permis l'intégration d'une nouvelle méthode de déploiement suite au blocage par défaut des macros VBA par Microsoft. De même pour **REvil** dont les activités avait été stoppées suite à des arrestations opérées en Octobre 2021 par le FSB (Federal Security Service). Une nouvelle infrastructure a été mise en place et des victimes ont déjà été annoncées.

Bonne nouvelle pour nos **données personnelles**, à partir du 20 juillet, les applications proposées dans la boutique **Android** (*Google Play Store*) devront fournir plus d'informations sur la manière dont elles collectent, partagent et protègent les données des utilisateurs. Source : Blog Google.

Des chercheurs ont réalisé une étude sur plusieurs **applications de viso-conférence** et plus particulièrement sur l'utilisation du bouton « mute » permettant de couper le micro. Surprise, même avec le micro coupé, plusieurs outils envoient des informations statistiques et de télémétrie (volume audio,...).

Connaissez-vous **Frappo** ? Il s'agit d'une plateforme malveillante d'hameçonnage à la demande. Des chercheurs en sécurité ont investigué sur ce nouveau produit. Vidéo de promotion, support et même extension pour les navigateurs internet, tout y est, à l'image d'un service professionnel !

Le président des États-Unis a signé en mai un mémorandum de sécurité nationale (NSM) demandant aux agences gouvernementales d'anticiper les risques posés par l'**informatique quantique** pour la sécurité nationale. L'objectif est de produire de nouveaux algorithmes de chiffrement résistant aux attaques d'ordinateurs quantiques d'ici 2035.

Nouvelles vulnérabilités critiques

Vulnérabilité dans F5 BIG-IP *[CERTFR-2022-ALE-004] - score CVSS : 9.8*

Cette vulnérabilité affecte les équipements réseau *BIG-IP* de l'éditeur *F5 Networks*. Elle permet de contourner le mécanisme d'authentification et de prendre le contrôle de l'équipement à travers l'interface de programmation (API) *iControl*. Les analyses techniques publiées récemment **confirment la facilité d'exploitation de cette vulnérabilité** et des **codes d'exploitation sont désormais disponibles**. Des **correctifs ont été publiés** par l'éditeur.

Vulnérabilité dans Microsoft Office *[CERTFR-2022-ALE-005]*

Cette vulnérabilité est **critique** car relativement **facile à exploiter** et permettant une exécution de code à distance. Elle cible le binaire légitime Microsoft Support Diagnostic Tool (MSDT). Des **codes d'exploitation existent.** En attendant un correctif, des contournements ont été publiés par Microsoft.

Principales cyberattaques

- 19 Avril, GHT Cœur Grand Est : le système informatique des établissements de l'ensemble du Groupement Hospitalier de Territoire (GHT) du Cœur Grand Est a été visé par une cyberattaque entraînant une fuite de données concernant les centres hospitaliers de Vitry-le-François et de Saint-Dizier. Le groupement hospitalier appelle à la vigilance par crainte d'hameçonnage.
- 4 mai, opération « Cuckoobees » : la société Cybereason a investigué sur plusieurs entreprises victimes d'une vaste opération qui semble avoir pour objectif l'espionnage industriel. Plusieurs entreprises d'Amérique du Nord, d'Europe et d'Asie sont impactées. Ces dernières souhaitent rester anonymes. Plusieurs centaines de Giga octets de secrets industriels ont été exfiltrés. Les chercheurs informatiques attribuent cette opération qui dure depuis 2019 a minima au groupe Winnti qui serait proche du gouvernement chinois avec un degré de confiance évalué à « modéré - élevé ». Une étude détaillée du logiciel malveillant ainsi qu'une seconde sur le mode opératoire ont été produites par cette société de cybersécurité.
- 10 mai, nouvelle arnaque au partage d'écran : la FCA (autorité de régulation financière britannique) alerte les internautes du monde entier d'une arnaque au « partage d'écran » en forte augmentation. Sous couvert de répondre à une question ou à une demande financière, le cybercriminel va essayer de convaincre son interlocuteur de participer à une visioconférence sur la base d'un outil légitime qu'il invite à installer afin de prendre le contrôle de l'ordinateur. Son objectif est d'avoir accès aux comptes bancaires de la victime.
- 10 mai, l'Union Européenne, dans un communiqué de presse, « condamne fermement les actes de cybermalveillance commis par la Fédération de Russie à l'encontre de l'Ukraine, qui ciblaient le réseau satellitaire KA-SAT, exploité par Viasat » officialisant ainsi l'attribution de l'attaque du 24 février.

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

La description de l'escroquerie au président réalisée ces deux derniers mois n'est pas exhaustive des différents stratagèmes et arguties utilisés. Néanmoins, les recommandations suivantes pourraient constituer un moyen de faire face au plus grand nombre :

- **Éviter d'exposer des informations internes** à l'entreprise et à ses dirigeants dès lors que cela ne s'avère pas nécessaire (notamment sur le site de l'entreprise elle même).
- **Sensibiliser les salariés** sur ce type d'escroquerie ainsi que sur les risques potentiels à dévoiler leur vie professionnelle sur les réseaux.
- Déployer un système permettant d'**alerter les utilisateurs en cas de réception de courriel a priori interne mais provenant en réalité de l'extérieur de l'entreprise** (technique dite de « Email *spoofing* » consistant à modifier les en-têtes des messages).
- Plus globalement, installer un outil permettant de **filtrer les courriels suspects.**
- Mettre en place une procédure stricte instaurant une **double validation des opérations sensibles**. Un collaborateur ne doit jamais être isolé lors d'une prise de décision ayant un impact fort sur l'entreprise. Il convient de faire en sorte que la demande soit confirmée par un second intervenant qui la validera de manière physique ou par un moyen d'authentification irréfutable.