Revue de presse des cybermenaces

Com CyberGend

#13 – Février 2023

Centre d'analyse et de regroupement des cybermenaces
revue-presse-comcybergend@gendarmerie.interieur.gouv.fr

A retenir

A l'image de la fin d'année, ce mois a de nouveau été marqué par une forte **coopération internationale** dans la lutte contre les cybermenaces. Le travail conjoint d'États européens a permis de démanteler dans les Balkans un réseau criminel proposant de **faux investissements en cryptomonnaies**. Le groupe **Hive** a été infiltré dans le cadre d'une opération internationale et plus de **300 clés de déchiffrement pour rançongiciel** ont été communiquées aux victimes. Toutefois, les cybercriminels restent actifs et créatifs puisque certains cherchent à détourner l'usage de **ChatGPT** afin de **développer des logiciels malveillants.**
Enfin, un effort significatif est mené à l'international afin de lutter contre les défauts de **sécurisation des données personnelles et le non-respect du RGPD** par certaines organisations.

Les chiffres du mois

3,7 milliards de dollars. C'est le montant total estimé des vols liées à des piratages de crypto-actifs en 2022, **soit une hausse de 58 % depuis 2021.** Zataz

16 millions d'euros. C'est le montant saisi en crypto-actifs à la suite d'une enquête judiciaire menée par plusieurs forces de police internationales, dont **Europol,** le **ComCyberGend** et le **FBI,** visant une **plateforme russophone d'échanges de crypto-actifs** soupçonnée de blanchir des millions de dollars. Gendarmerie

Informations sur la menace

Amazon S3 (Simple Storage Service), un service de stockage de données d'**AWS** (Amazon Web Services), va désormais **chiffrer par défaut en AES-256 toutes les nouvelles données sauvegardées**. Cette option était précédemment disponible mais nécessitait une action de l'administrateur. Ce changement, qui n'empêchera pas un attaquant disposant des droits suffisants d'accéder aux **données de l'utilisateur** participe toutefois à **élever la sécurité** du service de stockage. Bleeping Computer

Une action coordonnée d'États européens, avec le soutien d'**Europol**, a permis de démanteler un réseau criminel d'**arnaques aux cryptomonnaies par téléphone.** Les escrocs contactaient les victimes, principalement allemandes, pour leur proposer de faux investissements. **Plusieurs millions d'euros** auraient ainsi été dérobés aux victimes depuis des **centres d'appel** situés en Serbie. L'opération judiciaire menée ce 11 janvier a permis d'arrêter **15 suspects.** Des perquisitions ont eu lieu en **Serbie,** en **Bulgarie** et à **Chypre**. Europol

Il a été démontré qu'il était possible de transformer **l'enceinte connectée Google Home** en véritable **appareil d'espionnage** en ajoutant un nouveau compte utilisateur via une **faille de sécurité corrigée depuis par Google**. Il était alors envisageable d'effectuer de nombreuses commandes : **contrôler la maison connectée, activer le micro** et **surveiller l'activité ambiante**. Bleeping Computer

Le **malware Android** baptisé **Godfather**, distribué via des applications disponibles sur **Google Play** en vue de dérober des fonds, permet à l'attaquant de **voler les identifiants** d'au moins **215 applications bancaires** et de **110 plateformes d'échanges de cryptomonnaies**. En outre, le malware rend aussi possible l'accès aux SMS, aux contacts, au journal d'appels, etc. RedPacketSecurity

Les opérateurs du rançongiciel **ALPHV** (ou BlackCat) **ont innové dans leur tactique d'extorsion.** Ils ont créé une **réplique du site de l'entreprise victime**, avec un nom de domaine quasi similaire, pour y publier les **données volées** : informations sur les employés, données financières et **copies de passeports**. Cette nouvelle méthode d'extorsion accroît davantage la **pression sur l'entreprise** puisque les données sont désormais accessibles facilement et sans restriction sur le ***clearweb***. Bleeping Computer

Pour aller plus loin…

Cette rubrique vous propose une sélection de rapports d'analyse qu'il paraît pertinent de consulter pour approfondir un sujet.

- [**Recorded Future**] Season of Giving, Season of Taking: Heightened Fraud During Holiday Shopping
  Ce rapport traite de l'activité cybercriminelle autour des soldes de fin d'année, notamment des campagnes de phishing et d'escroqueries.
- [**Sophos**] Security threats report 2023 Retour sur l'industrie des logiciels malveillants « *as a service* » en 2022, prenant en compte les aspects géopolitiques de la menace cyber.
- [**Fortinet**] Cyber Threat Prediction Prospective sur l'évolution des menaces en 2023, et conseils de protection d'un système d'information.

Les faits marquants

L'agent conversationnel **d'OpenAI nommé ChatGPT**, qui suscite actuellement l'effervescence, aurait été détourné pour générer du **code malveillant**. Plusieurs utilisateurs auraient révélé sur des forums avoir utilisé l'outil de conversation basé sur **l'intelligence artificielle** (IA) afin de créer un **malware voleur de données** (*stealer)* en script Python ou encore un malware en langage Java permettant de déployer d'autres logiciels malveillants sur des **systèmes infectés**.

ChatGPT aurait également été utilisé pour **développer un script Python permettant de chiffrer des données**, lequel pourrait être transformé en **rançongiciel** à terme. Il n'est pas à exclure que ce nouvel outil soit utilisé pour faciliter **les cyberattaques et les rendre accessibles à des utilisateurs peu expérimentés**. Zdnet

Microsoft a, quant à lui, développé un outil de conversion texte-voix nommé **VALL-E** capable d'imiter la voix d'une personne, ce qui **soulève des questions de sécurité**. Si l'outil qui n'est actuellement pas disponible au public se démocratise, son usage pourrait être **détourné à des fins malveillantes pour faciliter les escroqueries et les usurpations d'identité**. Euronews

Principales cyberattaques

1er janvier, le cabinet d'experts comptables français **CDER** a été victime du groupe cybercriminiel **PLAY**. Les données publiées contiennent notamment des **passeports** et des **cartes d'identité** de clients. Ce secteur d'activité possédant des données particulièrement sensibles est une cible de choix pour des cybercriminels qui peuvent les revendre au prix fort à des fins **d'usurpation d'identité**. Zataz

31 décembre, après une attaque par **rançongiciel** d'un **hôpital pour enfant** situé au Canada, le **groupe Lockbit** s'est excusé publiquement et a publié la clé de déchiffrement. L'affilié ayant mené l'attaque a été exclu pour avoir violé les règles du groupe interdisant de mener des **actions susceptibles d'entraîner la mort.** Cela n'avait pas empêché Lockbit d'attaquer le **Centre Hospitalier Sud Francilien** (CHSF) ou encore celui de **Versailles**, obligeant le personnel à transférer les patients et à reporter des opérations. Le groupe reste actif ; il s'est attaqué le 12 janvier au géant français des cosmétiques **Nuxe** et réclame une **rançon de 300 000 euros**. BleepingComputer, SecurityAffairs,Numerama

4 janvier, un attaquant serait parvenu à récupérer les données de plus de **200 000 « clients »** de l'hebdomadaire **Charlie Hebdo** ainsi que des données internes. Celles-ci seraient proposées à la vente sur au moins un forum et **une enquête a été ouverte**. Cette attaque intervient alors qu'une **édition dédiée à l'Iran** était diffusée presque **8 ans jour pour jour après l'attentat contre le journal**. Les motivations de l'attaquant sont troubles. Ce dernier, qui pourrait être un **hacktiviste iranien, réclame 20BTC** en échange des **données exfiltrées**. Zataz, Lemonde

Réglementation

Avec le **Digital Market Act**, règlement de l'Union Européenne qui régit le marché du numérique, les gros éditeurs de la tech devront permettre aux utilisateurs de pouvoir **installer des applications sans passer par la boutique officielle** de la marque, notamment via des **boutiques alternatives**. L'entrée en vigueur est prévue le 2 mai 2023, mais les sanctions ne pourront être infligées qu'après 2024. Cette nouveauté soulève un débat autour de la sécurité et les risques de **déploiement de logiciels malveillants**. Bitdefender Commission Européenne

Ces deux derniers mois, les **autorités françaises et internationales** ont infligé **plusieurs amendes importantes** aux grandes entreprises du numérique auxquelles sont reprochées des violations **de la réglementation en matière de protection des données personnelles** de leurs clients :

- **60 millions d'euros** pour **Bing**, moteur de recherche de Microsoft, et **5 millions d'euros** pour **TikTok**, deux amendes infligées par la **CNIL**. La raison : il était plus facile, en un seul clic, d'accepter les cookies, que de les refuser. En effet, cette dernière opération nécessitait de valider plusieurs étapes ; BitDefender Numerama
- **520 millions de dollars** en deux amendes pour **Epic Games**. L'entreprise derrière **Fortnite** a été condamnée par un tribunal américain pour **violation de la loi sur la protection de la vie privée des enfants** et à **rembourser les familles**. Le jeu permettait aux enfants d'**effectuer des achats sans le consentement des parents** et, en appuyant sur un seul bouton, amenait à des **achats non désirés ;** Zataz, CNBC
- **390 millions d'euros pour Meta et 5,5 millions pour WhatsApp**. Ces amendes ont été décidées par la **Commission Irlandaise de Protection des Données**, pour avoir incité les utilisateurs à accepter les publicités personnalisées, en violation du **RGPD**. La condamnation de WhatsApp fait suite à **une modification des conditions d'utilisation** imposée aux utilisateurs, qui ne pouvaient plus accéder à l'application sans consentir au traitement de leurs données personnelles. Forbes, RedPacketSecurity