MINISTÈRE
DE L'INTÉRIEUR
ET DES OUTRE-MER
Liberté
Égalité
Fraternité

COMCYBER-MI

Commandement du ministère de l'Intérieur dans le cyberespace

Revue de presse des cybermenaces

Centre d'analyse et de regroupement des cybermenaces

#02 – FÉVRIER 2024

A retenir

Une **campagne d'hameçonnage** débutée fin 2023 relative à de faux avis de contravention pour stationnement usurpe les services des finances publiques. Elle est toujours en cours début 2024.
Des **mesures de sécurité** seront ajoutées à la solution d'IA **OpenAI** en prévision des élections en 2024 qui concerneront 50 pays, afin de prévenir toute opération de déstabilisation ou désinformation via les *deep fakes*.
Près d'une trentaine de **collectivités territoriales** et neuf **hôpitaux** ont été touchés par des **cyberattaques** en 2023. La tendance se poursuit en 2024, les rançongiciels restant la menace la plus redoutée.

Chiffres du mois

94% des entreprises ont subi une **attaque par hameçonnage** en 2023 soit une augmentation de 2% par rapport à l'année précédente. Les techniques les plus courantes sont les URL trompeuses, les pièces jointes corrompues et la réutilisation de comptes mail compromis.

L'enquête a été menée auprès de 500 RSSI aux États-Unis, en Grande-Bretagne et en Australie dans les secteurs financier, sanitaire, juridique et des ONG. InfoSecurity Magazine

Informations sur la menace

Un nouveau groupe spécialisé dans les attaques par **rançongiciel** appelé **Werewolves** connaît une notoriété croissante depuis fin 2023, période à laquelle il a multiplié les attaques. Ce groupe aurait été créé en mai 2023 et serait composé de membres russophones. Contrairement à d'autres groupes similaires, Werewolves attaque également des organisations implantées en Russie. En outre, il mettrait en œuvre le rançongiciel **LockBit 3.0** pour ses attaques, et exigerait le dépôt de garantie de 1 Bitcoin de la part de tout candidat-affilié afin d'éviter les tentatives d'infiltrations par les journalistes ou les forces de sécurité. SocRadar

Deux entreprises, attaquées par les groupes de **rançongiciels Royal** et **Akira** en octobre et novembre 2023, ont été les cibles de nouvelles tentatives d'extorsion après avoir payé la rançon. Des **escrocs** se présentant comme des **chercheurs** ou des **hackers éthiques** les ont contactées et ont affirmé avoir accès aux serveurs des attaquants. Ils ont indiqué être en mesure de supprimer définitivement les données exfiltrées lors de la première attaque, contre une somme de 5 Bitcoins. Bleeping Computer

Sur Telegram, un cyberdélinquant propose à la location mensuelle un service d'**hameçonnage vocal**. L'utilisateur du service renseigne le numéro de sa cible sur un robot Telegram. Puis, ce robot utilise des **fichiers audio pré-enregistrés** qu'il retransmet lorsque la victime décroche. Ce service « clé-en-main » peut permettre aux individus malveillants de passer des appels en prétendant représenter le service anti-fraude de la banque de la victime par exemple, pour ensuite récupérer des **codes d'authentification**. ZDNet

Une campagne d'**hameçonnage** observée depuis fin 2023 usurpe les services des **finances publiques**. Un **courriel frauduleux** informe le destinataire qu'une contravention pour stationnement interdit lui a été adressée. Le règlement d'une amende de 35 euros est exigé depuis une page *web* en apparence légitime. Les acteurs malveillants ont profité des nombreux déplacements en véhicule pour les réunions en famille ou entre amis lors des **fêtes de fin d'année** pour tenter de tromper les destinataires de ces courriels. Numerama

Pour aller plus loin…

[LIBÉRATION] Interview de Johanna Brousse, vice-procureure près la section J3 du Parquet de Paris. La magistrate s'exprime sur la criminalité liée aux escroqueries par SMS, le profil des délinquants et l'organisation des réseaux.

[ANSSI] Cyberattaques et remédiation, les clés de décision. Guide donnant les clés stratégiques de la remédiation face aux cyberattaques, offrant des orientations cruciales pour la prise de décision à la suite d'un incident de sécurité informatique.

[SEKOIA] Securing Gold: Assessing Cyber Threats on Paris 2024. Étude portant sur les potentielles cybermenaces autour des JOP en France, retour sur les précédentes éditions et état de la menace actuelle.

[CLUSIF] Panorama de la cybercriminalité du CLUSIF : Florilège d'attaques en 2023 – Compte rendu de la 24ème édition du Panorama de la cybercriminalité organisé par le CLUSIF

[ESET] Say what you will? Your favorite speech-to-text app may be a privacy risk. Article portant sur les applications de transcription audio, représentant un risque pour la vie privée (collecte, stockage, utilisation malveillante…).

Faits marquants

50 pays seront concernés par des **élections en 2024**. Des opérations de déstabilisation ou de désinformation mettant en œuvre des technologies associées à l'Intelligence Artificielle sont susceptibles d'être observées. Dès lors, **OpenAI**, développeur de **ChatGPT** et **DALL-E** a annoncé des **mesures de sécurité** afin de prévenir les *deep fakes*. Parmi celles-ci, des certificats d'authentification numérique **C2PA** (*Coalition for Content Provenance and Authenticity*) seront intégrés dans les images produites par les solutions d'OpenAI. InfoSecurity Magazine

Sébastien Raoult, hacker français de 23 ans, est accusé par les autorités américaines de faire partie du groupe de pirates **ShinyHunter**, spécialisé dans le **vol et la revente de données** sur le *dark web*. Il a été jugé aux États-Unis ce mois de janvier et condamné à une **peine de 3 ans d'emprisonnement**, après avoir plaidé coupable du vol de données, évitant ainsi une peine beaucoup plus lourde. Il avait été interpellé par le FBI au Maroc en mai 2022 et devrait être libéré fin 2024. 20 Minutes

Principales cyberattaques

Fin décembre 2023, le média Numerama a publié une **cartographie des villes, départements et hôpitaux victimes de cyberattaques sur l'ensemble de l'année écoulée**. En 2023, près d'une trentaine de collectivités territoriales, dont des communes et départements, ainsi que neuf hôpitaux, ont été touchés en France. L'**ANSSI** a également recensé **187 incidents cyber affectant les collectivités territoriales** entre janvier 2022 et juin 2023, avec une moyenne de 10 incidents par mois. Parmi les attaques dénombrées par l'ANSSI, 40 ont pour cause des rançongiciels, représentant la principale menace en raison des préjudices élevés. Numerama

Le 29 décembre 2023, la ville de **Fouesnant**, ainsi que la **Communauté de communes du Pays Fouesnantais**, ont été victimes d'une cyberattaque qualifiée de majeure. Les pirates ont provoqué une intrusion sur les serveurs informatiques, entraînant une paralysie des services municipaux. Seul le service de l'état-civil est resté opérationnel, car relié par une connexion plus sécurisée. Les équipes techniques et les autorités compétentes ont été mobilisées. Ces collectivités ont été assistées par un prestataire de réponse aux incidents de sécurité. ZDNet

Le 1er janvier 2024, la **mairie de Saint-Philippe (974)** a subi une cyberattaque par rançongiciel, privant les services municipaux de connexion à Internet et d'accès aux applications métier. Les ordinateurs ont été déconnectés d'internet, perturbant le traitement des demandes administratives. Les employés ont dû retourner à des méthodes manuscrites pour les actes officiels. Une plainte a été déposée, et la municipalité a été assistée par des experts en cybersécurité. France TV info

Le 15 janvier 2024, le **centre hospitalier universitaire de Nantes** a été victime d'une attaque par déni de service distribué. Si les logiciels de soins fonctionnaient, le réseau Internet de l'établissement, l'envoi et la réception de courriels, ainsi que l'accès à certains outils du CHU depuis l'extérieur ont été bloqués. Aucune intrusion ou compromission de données n'a été constatée. IT Connect

Le 23 janvier 2024, le site du **Département de la Sarthe** a été victime d'une cyberattaque. Les identifiants et mots de passe des agents du département auraient été dérobés et mis en ligne sur le *dark web*. Le site a été mis hors ligne pour bloquer la propagation de l'attaque. FranceBleu

Anticipation / Réglementation

L'U.S. Federal Trade Commission a lancé une compétition pour recueillir des idées permettant de **prévenir les dangers du clonage vocal par Intelligence Artificielle dans le cadre d'activités frauduleuses**. Le clonage vocal consiste à analyser un extrait audio afin d'en extraire les caractéristiques uniques de l'interlocuteur, puis de générer un nouveau discours par des outils *text-to-speech*. Le gagnant de cette compétition se verra offrir un prix de 25 000 dollars. Bleeping Computer

La **Commission Nationale Informatique et Libertés** (CNIL) a adressé une **amende** de 32 millions d'euros à Amazon France Logistique pour avoir mis en place un système de mesure de l'activité et de vidéosurveillance des employés jugé excessivement intrusif. CNIL