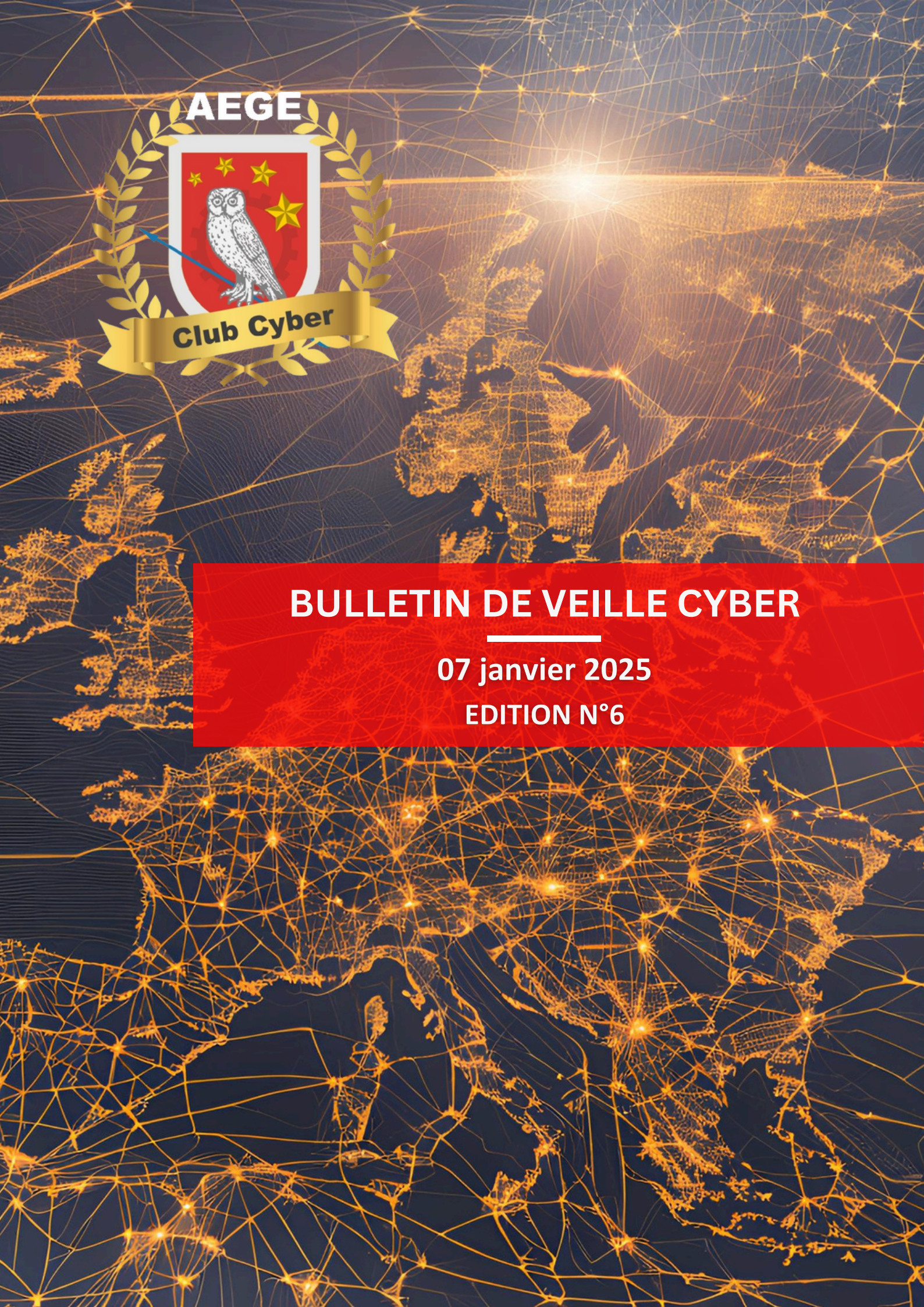


BULLETIN DE VEILLE CYBER

07 janvier 2025

EDITION N°6

ATOS DÉMENT LES ALLÉGATIONS D'ATTAQUE RANSOMWARES PAR LE GROUPE SPACE BEARS

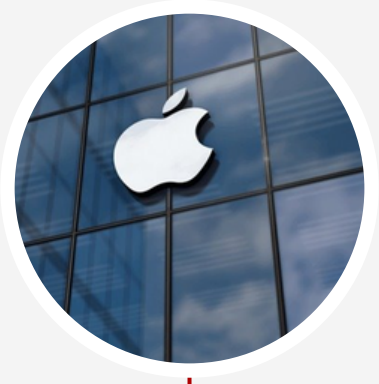
[03 JANVIER 2025] - Atos, géant français des technologies de l'information a nié les affirmations du groupe de ransomware Space Bears, qui prétend avoir compromis une de ses bases de données. Le groupe cybercriminel, apparu en avril 2024, avait annoncé le 28 décembre qu'il publierait les données volées sur son site du dark web.

Atos a attribué l'incident à une « *infrastructure externe tierce non connectée* » contenant des données mentionnant son nom, mais qui n'était ni gérée ni sécurisée par la société.

Space Bears, connu pour ses tactiques de double extorsion, a déjà revendiqué 45 attaques depuis son émergence, ciblant divers secteurs industriels à travers le monde. Atos maintient que sa sécurité n'a pas été compromise.

Source : https://atos.net/en/2025/press-release_2025_01_03/atos-confirms-not-being-compromised-by-the-ransomware-group-space-bears

95 MILLIONS DE DOLLARS POUR APAISER UNE CONTROVERSE SUR LA VIE PRIVÉE CHEZ APPLE



[2 JANVIER 2025] - Apple a accepté de verser 95 millions de dollars pour régler une action collective l'accusant d'avoir violé la vie privée de ses utilisateurs. Selon la plainte, Siri aurait enregistré des conversations, parfois sans avoir été activé, et partagé ces données sensibles avec des tiers, notamment des sous-traitants et des annonceurs.

L'affaire a éclaté après un rapport de The Guardian en 2019, révélant que des enregistrements incluaient des discussions confidentielles et étaient accompagnés de données personnelles comme la localisation et les informations d'applications.

Apple, tout en niant toute faute, a conclu l'accord sans commentaire public. L'entreprise se targue pourtant souvent d'être impliquée dans la protection de la vie privée de ses utilisateurs.

Source : https://therecord.media/apple-to-pay-95-million-siri-lawsuit

LES HACKERS PRORUSSES « NONAME » CIBLENT 23 SITES DE COLLECTIVITÉS FRANÇAISES POUR LE NOUVEL AN

[31 DECEMBRE 2024] - Le groupe de hackers prorusses NoName057(16) a revendiqué une série d'attaques par déni de service (DDoS) les 31 décembre 2024 et 1er janvier 2025, perturbant les sites internet de 23 collectivités, entreprises et institutions françaises. Parmi les cibles figurent des grandes villes comme Marseille, Bordeaux, ainsi que des départements et des territoires d'outre-mer. Les attaques sont justifiées par le groupe comme une réponse au soutien militaire de la France à l'Ukraine.

Le parquet de Paris a ouvert une enquête pour "entrave à un système de traitement automatisé des données en bande organisée", confiée à la DGSI. Spécialisé dans les attaques DDoS, le collectif est connu pour avoir mené des actions similaires contre d'autres institutions, notamment le Sénat, l'Assemblée nationale et le Parlement européen.

Source : https://www.lefigaro.fr/conjoncture/qui-sont-les-noname-ces-hackers-prorusses-qui-s-attaquent-a-plusieurs-villes-francaises-ce-mardi-20241231

Yunès-Louis Amadid

UNE CAMPAGNE DE PHISHING COMPROMET 35 EXTENSIONS CHROME UTILISÉES PAR 2,6 MILLIONS D'UTILISATEURS

[31 DECEMBRE 2024] - Une campagne de phishing ciblant les développeurs d'extensions Chrome a permis à des pirates de compromettre 35 extensions utilisées par environ 2,6 millions de personnes.

En exploitant des emails frauduleux imitant des notifications officielles de Google, les attaquants redirigeaient les victimes vers une fausse autorisation OAuth (protocole de délégation d'autorisation) pour prendre le contrôle des extensions.

Les attaquants ciblaient également les mécanismes de double authentification pour contourner les protections et exploiter les comptes à des fins financières. Bien que les activités récentes aient débuté en décembre 2024, les premières traces de cette attaque remontent à mars 2024.

Source : https://www.proofpoint.com/fr/threat-reference/oauth

LE TRÉSOR AMÉRICAIN VICTIME D'UNE INTRUSION PAR VOL DE CLÉ API

[31 DECEMBRE 2024] - Le département du Trésor des États-Unis a annoncé un « incident majeur de cybersécurité » survenu le 8 décembre 2024, permettant à des acteurs malveillants présumés d'origine chinoise d'accéder à distance à certains ordinateurs et documents non classifiés. L'intrusion a été facilitée par le vol d'une clé API de BeyondTrust, un fournisseur de services tiers.

En réponse, le Trésor américain collabore avec l'Agence de cybersécurité et de sécurité des infrastructures (CISA) ainsi que le FBI pour enquêter sur l'incident.

Les preuves suggèrent l'implication d'un acteur lié à l'État chinois. Le ministère chinois des Affaires étrangères a nié toute implication. Une mise à jour du Washington Post a révélé que l'attaque a également ciblé l'Office de contrôle des actifs étrangers (OFAC) et le bureau du secrétaire au Trésor.

Source : https://thehackernews.com/2024/12/chinese-apt-exploits-beyondtrust-api.html

DE NOUVELLES ENTREPRISES AMÉRICAINES VICTIME DU GROUPE DE HACKERS SALT TYPHOON

[6 JANVIER 2025] - Des entreprises américaines de télécommunication ont été victimes du groupes de hacker Salt Typhoon, affilié à l'Etat chinois.

Le Wall Street journal a été contacté par des sources confirmant que les systèmes des entreprises Charter Communications, Consolidated Communications et Windstream avaient été victimes d'une intrusion.

Cette intrusion fait suite à plusieurs intrusions du fait du groupe Salt Typhoon. Ils s'étaient précédemment introduits dans les sytèmes de plusieurs entreprises américaines pendant le mois d'octobre 2024, comme AT&T, Verizon et T-Mobile. Ils avaient aussi tenté de s'introduire dans les mails et les téléphones de l'équipe de campagne de Kamala Harris, Donald Trump et JD Vance.

Source : https://www.bleepingcomputer.com/news/security/charter-and-windstream-among-nine-us-telecoms-hacked-by-china/

Yunès-Louis Amadid