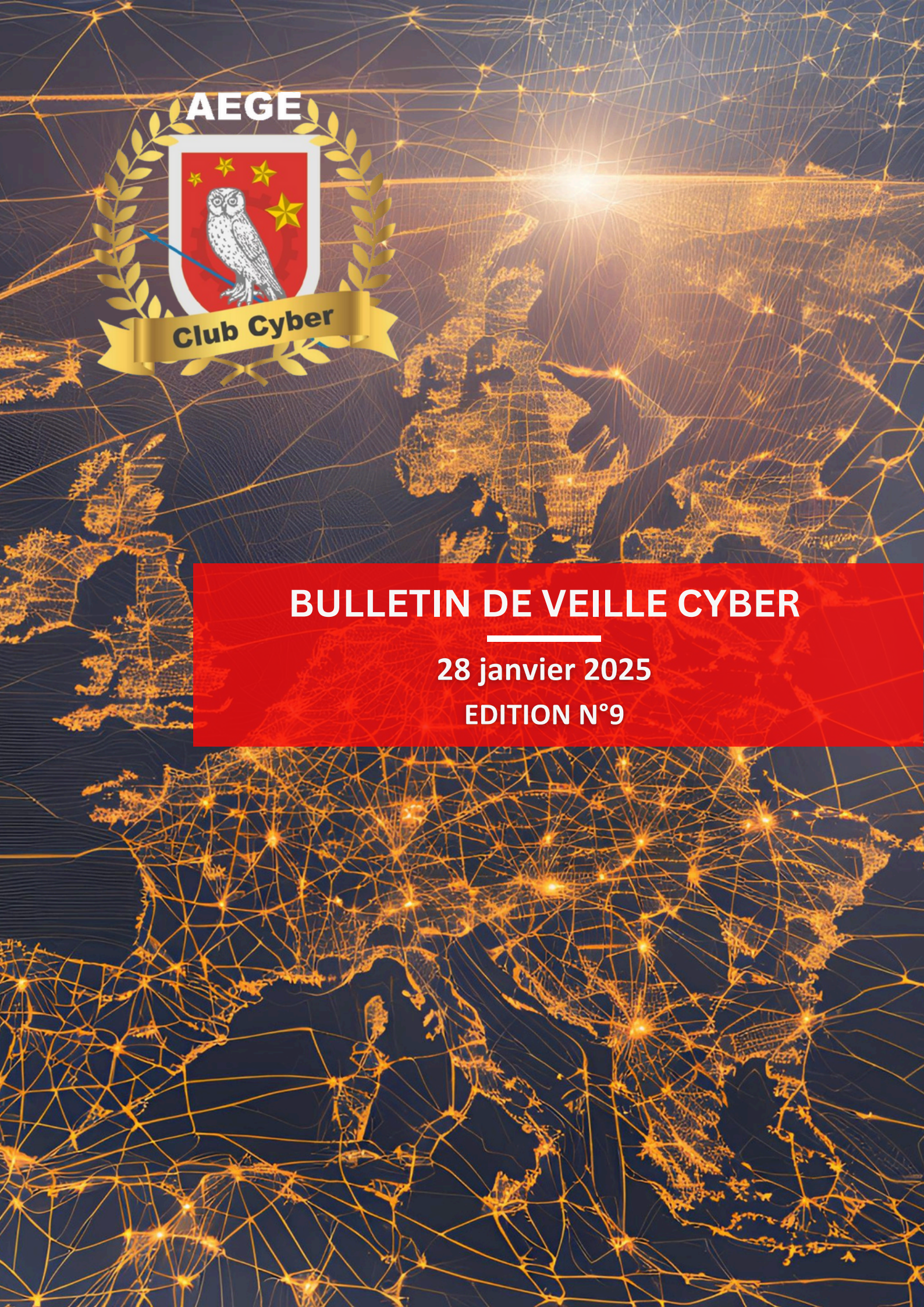


BULLETIN DE VEILLE CYBER

28 janvier 2025

EDITION N°9

DATA PRIVACY WEEK 2025

[27 JANVIER 2025] - La Semaine de la confidentialité des données, célébrée du 27 au 31 janvier 2025, met en avant le thème « Prenez le contrôle de vos données ».
Cette initiative vise à sensibiliser les individus à la gestion proactive de leurs informations en ligne et à encourager les entreprises à respecter la vie privée des utilisateurs, protéger les données et instaurer la confiance.

Des ressources sont mises à disposition pour aider les utilisateurs à prendre des décisions éclairées sur le partage de données et soutenir les organisations dans la mise en œuvre de pratiques respectueuses de la vie privée. Cet événement est porté par l'Alliance nationale pour la cybersécurité (National Cybersecurity Alliance).

Source : https://www.staysafeonline.org/fr/data-privacy-week

DES HACKERS RUSSES SE FONT PASSER POUR DES TECHNICIENS IT SUR MICROSOFT TEAMS

[23 JANVIER 2025] - Des cybercriminels russes ont usurpé l'identité de techniciens IT externes sur Microsoft Teams afin de pénétrer des réseaux et déployer des rançongiciels. Leur stratégie consiste à inonder les cibles de courriels de spam avant de les contacter via Teams, prétendant fournir une assistance technique.

Une fois qu'ils obtiennent un accès à distance, ils installent des rançongiciels, paralysant les systèmes et exfiltrant des données. La société britannique de cybersécurité Sophos a signalé 15 incidents similaires au cours des trois derniers mois, attribuant ces attaques aux groupes russes Fin7 et Storm-1811.

Cette tactique exploite les paramètres par défaut de Teams qui permettent les communications externes, soulignant l'importance pour les organisations de renforcer leurs défenses numériques.

Source : https://www.thetimes.com/uk/technology-uk/article/russian-hackers-pose-as-remote-it-staff-on-microsoft-teams-vhpx6ww7m?region=global

UN DIRIGEANT DE CRYPTOMONNAIES KIDNAPPÉ DANS UNE TENTATIVE D'EXTORSION VIOLENTE

[23 JANVIER 2025] - Monsieur Balland, le cofondateur français de l'entreprise de cryptomonnaies Ledger, âgé de 36 ans, a été enlevé par un gang armé réclamant une rançon de 10 millions d'euros. Pendant les 24 heures de captivité, Balland a subi des violences, dont la mutilation d'un doigt. L'intervention de l'unité d'élite GIGN a permis de sauver Balland ainsi que d'arrêter dix suspects. Cependant, les chefs du gang restent en fuite.

Une partie de la rançon, payée en cryptomonnaies, a pu être gelée. Cet incident met en lumière une tendance inquiétante d'attaques ciblant les acteurs de l'industrie des cryptomonnaies en France et en Belgique. Les experts conseillent désormais de faire preuve de discrétion quant à l'affichage de sa richesse personnelle.

Source : https://www.20minutes.fr/faits_divers/4135245-20250123-interpellations-circonstances-point-enlevement-contre-rancon-prodige-cryptomonnaie

Mehdi Medjou

AMENDE INFLIGÉE À PAYPAL POUR MANQUEMENTS À LA CYBERSÉCURITÉ

[23 JANVIER 2025] - PayPal a été condamné à une amende de 2 millions de dollars par le Department of Financial Services de New York pour des failles en matière de cybersécurité ayant entraîné l'exposition des numéros de sécurité sociale de ses clients fin 2022.

Ces problèmes découlaient d'un manque de personnel et de formation dans des rôles clés de cybersécurité, ce qui a permis à des cybercriminels d'accéder à des données sensibles pendant environ sept semaines.

Depuis cet incident, PayPal a mis en place des mesures telles que l'authentification multifactorielle sur tous les comptes américains, des réinitialisations forcées de mots de passe et l'ajout de CAPTCHA pour renforcer la sécurité.

Source : https://www.dfs.ny.gov/reports_and_publications/press_releases/pr20250123

https://www.reuters.com/technology/paypal-fined-by-new-york-cybersecurity-failures-2025-01-23/

LA DIRECTRICE SORTANTE DE LA CISA FAIT LE BILAN DE SON MANDAT DANS UN CONTEXTE INCERTAIN

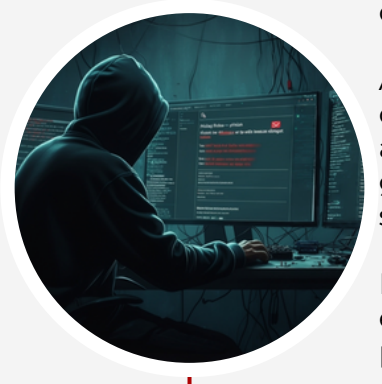
[23 JANVIER 2025] - Jen Easterly, directrice sortante de l'Agence de cybersécurité et de sécurité des infrastructures (CISA), a évoqué les réussites et les défis de son mandat, lors d'une interview. Depuis 2021, elle a piloté des réponses à des cybermenaces majeures, notamment la campagne d'espionnage Salt Typhoon liée à la Chine.

Malgré ces efforts, l'avenir de l'agence reste incertain alors que l'administration Trump prévoit de réduire ses moyens, avec des actions comme la nomination de Kristi Noem au poste de secrétaire à la Sécurité intérieure et la dissolution du Cyber Safety Review Board. Easterly a souligné l'importance d'une collaboration non partisane pour protéger les infrastructures nationales contre les cybermenaces.

Source : https://www.wired.com/story/big-interview-jen-easterly-cisa-cybersecurity/

SPEARPHISHING : UNE MENACE EN FORTE AUGMENTATION ALIMENTÉE PAR L'IA

[22 JANVIER 2025] - Les attaques de spearphishing, qui ciblent des individus ou des organisations spécifiques avec des emails personnalisés, sont en forte augmentation. Contrairement au phishing traditionnel, les attaquants collectent des informations détaillées pour rédiger des messages convaincants, souvent en usurpant l'identité de contacts de confiance. Les conséquences incluent le vol de données, des pertes financières.



Alors qu'elles ne représentaient que 2,39 % des cyberattaques en 2023, elles ont plus que triplé en 2024 pour atteindre 7,92 % selon Mailinblack. Cette augmentation est en grande partie due à l'essor de l'intelligence artificielle générative, qui permet aux hackers de concevoir des attaques plus sophistiquées, crédibles et difficiles à détecter.

Pour y faire face, les organisations doivent prioriser la formation des employés, l'utilisation d'outils de sécurité avancés et la mise en œuvre de politiques strictes en matière de cybersécurité.

Source : https://itrnews.com/articles/204897/le-spearphishing-une-menace-en-pleine-expansion.html

Mehdi Medjou