11 mars 2025 - EDITION N°15

LES ACTUS CYBER DE LA SEMAINE

SWIPE A DROITE POUR EN SAVOIR PLUS →

LE PENTAGONE NIE L'ARRÊT DES OPÉRATIONS OFFENSIVES CYBER CONTRE LA RUSSIE

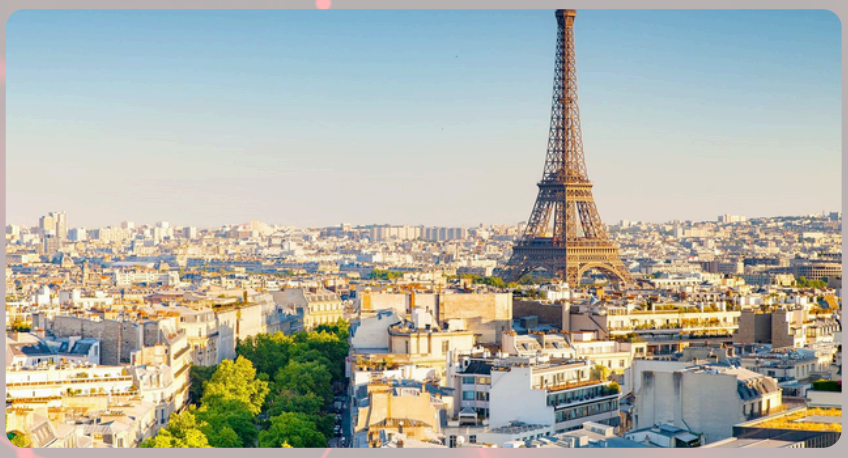
Du 4 mars 2025

Le 28 février 2025, un article de *The Record* annonçait que des sources internes du Pentagone faisaient écho d'une volonté de la part du secrétaire d'état à la défense, Pete Hegeth, d'arrêter les opérations offensives cyber contre la Russie.

Cependant, le 4 mars, le Pentagone a officiellement nié ces rumeurs en affirmant que le secrétaire d'état n'avait ni arrêté ni retardé les opérations cyber contre les cibles russes, et qu'aucun ordre n'avait été donné sur le sujet. Cette nouvelle avait à l'origine suscité de vives réactions du camp démocrate, dénonçant un « passe-droit » donné à la Russie par le Pentagone.

Source : https://www.bloomberg.com/news/articles/2025-03-04/pentagon-denies-report-of-halt-in-cyber-operations-versus-russia

LA MÉTROPOLE DU GRAND PARIS VICTIME D'UNE FUITE DE DONNÉES PERSONNELLES



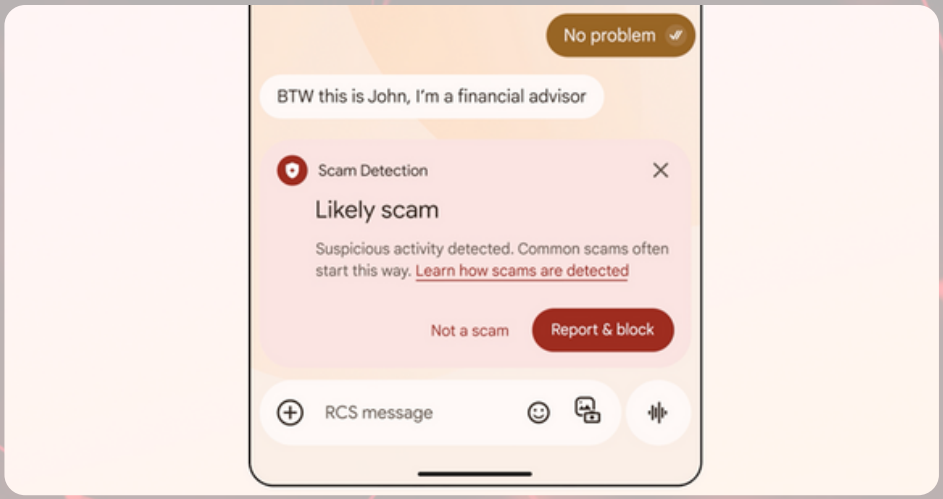
Du 6 mars 2025

Dans une plainte déposée jeudi, la Métropole du Grand Paris affirme avoir été victime d'une cyberattaque en février 2025, entraînant l'extraction de données personnelles de ses serveurs. Environ 5000 personnes, dont 250 agents et 208 élus, sont concernées, avec des informations telles que noms, prénoms, numéros de téléphone et adresses e-mail.

L'alerte a été donnée après des appels suspects reçus par certains agents. Une plainte contre X a été déposée pour collecte frauduleuse et abus de confiance. Cet incident s'inscrit dans une série d'attaques ciblant les collectivités (Nantes, Angers, Aix-Marseille-Provence).

Source : https://www.usine-digitale.fr/article/cybersecurite-la-metropole-du-grand-paris-victime-d-une-fuite-de-donnees-personnelles.N2228529

GOOGLE DÉPLOIE UNE IA ANTI-ARNAQUE SUR ANDROID



Du 5 mars 2025

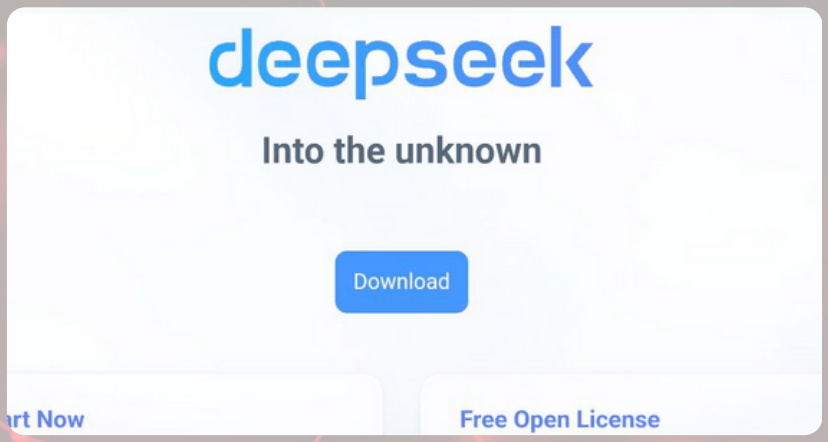
Google déploie une IA anti-arnaque sur Android pour détecter les fraudes conversationnelles en temps réel, en partenariat avec des institutions financières. Elle alerte les utilisateurs en cas de suspicion et permet de signaler ou bloquer l'expéditeur.

Cette fonctionnalité analyse les conversations textuelles et fonctionne entièrement sur l'appareil, selon Google. Désactivée par défaut, elle traite aussi l'audio sans l'enregistrer et signale les appels suspects. Les utilisateurs peuvent activer ou désactiver la fonction à tout moment.

Cependant, la fonctionnalité n'est disponible pour l'instant qu'aux Etats-Unis, Royaume-Uni et Canada.

Source : https://thehackernews.com/2025/03/google-rolls-out-ai-scam-detection-for.html

DES CYBERCRIMINELS EXPLOITENT LA POPULARITÉ DE DEEPSEEK SUR DES FAUX SITES



Du 6 mars 2025

Des cybercriminels exploitent la popularité de DeepSeek-R1 en diffusant de faux sites proposant un client téléchargeable. Ce logiciel malveillant vole des données sensibles (identifiants, cookies, portefeuilles crypto) et les envoie aux attaquants via Telegram ou un autre service de messagerie.

D'autres campagnes utilisent X (Twitter) pour propager des liens frauduleux. Les victimes téléchargent un installeur exécutant des commandes, donnant un accès à distance aux machines. Certaines de ces campagnes étaient destinées spécifiquement aux utilisateurs chinois.

Le véritable site de DeepSeek ne propose pas de client téléchargeable (à l'inverse de Chat GPT).

Source : https://securelist.com/backdoors-and-stealers-prey-on-deepseek-and-grok/115801/

LES ÉTATS-UNIS INCULPENT 12 HACKERS CHINOIS LIÉS AUX PIRATAGES D'INFRASTRUCTURES

Du 6 mars 2025

Le ministère américain de la Justice a inculpé 12 hackers chinois liés à Pékin et au groupe Silk Typhoon, accusés d'avoir piraté plus de 100 organisations à travers le monde, dont le Trésor américain. Parmi eux figurent des fonctionnaires chinois du ministère de la Sécurité Publique, des employés et dirigeants de l'entreprise i-Soon (spécialisée dans le cyberspionnage).

Ce groupe ciblait ministères, médias et institutions en exploitant des failles dans des logiciels tels que Citrix NetScaler ou Microsoft Exchange.

Les États-Unis offrent jusqu'à 10 millions de dollars de récompense pour toute information permettant d'arrêter les suspects, dont 2 millions spécifiquement pour l'un d'entre eux.

Source : https://www.usine-digitale.fr/article/les-etats-unis-inculpent-12-hackers-chinois-lies-au-piratage-d-infrastructures-critiques.N2228523

APPLE CONTESTE L'ORDRE DE "BACKDOOR" DU GOUVERNEMENT BRITANNIQUE

Du 4 mars 2025

Apple poursuit le gouvernement britannique devant le Investigatory Powers Tribunal pour contester un ordre du gouvernement exigeant un contournement du chiffrement iCloud. En réponse, Apple avait supprimé le chiffrement de bout en bout des sauvegardes iCloud au Royaume-Uni.

Aux États-Unis, l'administration Trump y voit une potentielle violation du Cloud Act protégeant les données américaines.

Cette affaire, une première au Royaume-Uni, pourrait créer un précédent légal. Apple affirme qu'il ne créera jamais de porte dérobée, tandis que le gouvernement britannique a discrètement supprimé ses anciennes recommandations, précédemment favorables au système de chiffrement d'Apple.

Source : https://www.reuters.com/technology/apple-appeals-overturn-uk-governments-back-door-order-financial-times-reports-2025-03-04/

L’ANSSI PUBLIE LE PANORAMA DE LA CYBERMENACE 2024

Du 11 mars 2025

L’ANSSI a publié son rapport “Panorama de la cybermenace 2024”. Elle identifie trois principales menaces cyber : les cybercriminels, ainsi que les attaquants liés à la Chine et à la Russie.

L’organisation des Jeux Olympiques de Paris a intensifié les risques, avec des attaques visant l’extorsion, l’espionnage et la déstabilisation, sans perturber l’événement.

L’année a aussi été marquée par une forte exploitation des vulnérabilités des équipements de sécurité en bordure des systèmes d’information, représentant plus de la moitié des opérations de cyberdéfense de l’ANSSI.

Source : https://cyber.gouv.fr/publications/panorama-de-la-cybermenace-2024

Le club cyber

elle

LE DÉBAT DE LA SEMAINE

Selon vous, faut-il interdire le paiement des rançongiciels ?

DONNE TON AVIS DANS LES COMMENTAIRES !