20 mai 2025 - EDITION N°25

LES ACTUS CYBER DE LA SEMAINE

SWIPE A DROITE POUR EN SAVOIR PLUS →

HTTPBOT CIBLE L'INDUSTRIE DES JEUX ET ENTREPRISES TECHNOLOGIQUES

Du 16 mai 2025

Des chercheurs en cybersécurité ont identifié un nouveau botnet nommé HTTPBot, actif depuis août 2024, ciblant principalement l'industrie du jeu, les entreprises technologiques et les établissements d'enseignement en Chine. Selon NSFOCUS, ce malware Windows écrit en Golang utilise des attaques DDoS via HTTP Flood sophistiquées, contournant les systèmes de détection classiques grâce à l'obscurcissement dynamique. Depuis avril 2025, il aurait lancé plus de 200 attaques, visant des interfaces critiques comme les systèmes de connexion et de paiement. HTTPBot marque un tournant vers des attaques DDoS plus précises et ciblées.

Source : https://thehackernews.com/2025/05/new-httpbot-botnet-launches-200.html

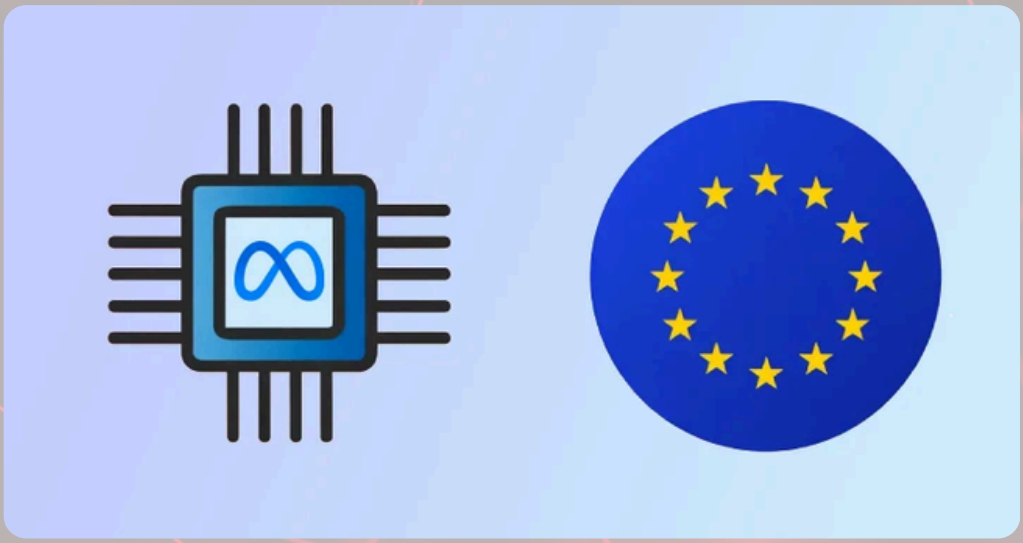
LES VULNÉRABILITÉS INTEL

Du 16 mai 2025

Des chercheurs de l'ETH Zurich ont identifié une nouvelle vulnérabilité, nommée Branch Privilege Injection (BPI), affectant tous les processeurs Intel modernes. Cette faille permettrait à des attaquants d'accéder à des données sensibles en exploitant la prédiction de branchement du CPU (unité centrale de traitement), rappelant les failles Spectre découvertes il y a plus de sept ans. Elle expose les contenus du cache et de la mémoire d'un autre utilisateur partageant le même processeur. Intel a publié des correctifs de microcode pour corriger la vulnérabilité avec une msie à jour.

Source : https://thehackernews.com/2025/05/researchers-expose-new-intel-cpu-flaws.html

META ACCUSÉE D'ENTRAÎNER SON IA SANS CONSENTEMENT



Du 15 mai 2025

L'association autrichienne de défense de la vie privée noyb a adressé une mise en demeure au siège irlandais de Meta, dénonçant l'intention de l'entreprise d'utiliser, dès le 27 mai 2025, les données publiques des utilisateurs européens de Facebook et Instagram pour entraîner ses modèles d'intelligence artificielle, sans consentement explicite. Meta invoque un « intérêt légitime » au lieu d'un véritable consentement, ce que noyb considère comme une violation flagrante du RGPD.
L'organisation souligne que l'entreprise limite également le droit de retrait, empêchant les utilisateurs de s'opposer facilement à l'usage de leurs données. Même si une minorité d'utilisateurs acceptait volontairement, cela suffirait à couvrir les langues et contextes culturels européens, selon noyb.

Source : https://thehackernews.com/2025/05/meta-to-train-ai-on-eu-user-data-from.html

COINBASE VICTIME D'UNE FUITE DE DONNÉES SUITE À UNE ATTAQUE INTERNE CIBLÉE

Du 15 mai 2025

Coinbase a annoncé qu'un groupe de cybercriminels a obtenu, via la corruption d'agents du service client basés en Inde, l'accès aux données personnelles d'une petite partie de ses utilisateurs actifs. Moins de 1 % des clients mensuels auraient été affectés. Les attaquants ont soudoyé des sous-traitants pour extraire des informations issues des outils de support client, incluant noms, coordonnées, documents d'identité, extraits de comptes et données bancaires partielles. Les données volées ont ensuite été utilisées dans des tentatives d'hameçonnage, où les victimes étaient contactées par de faux représentants Coinbase. Certains clients ont transféré des fonds à l'attaquant sous l'effet de cette fraude. Coinbase s'est engagé à indemniser les utilisateurs concernés.
Une tentative d'extorsion de 20 millions de dollars a également été signalée le 11 mai 2025, mais a échoué. L'entreprise précise que tous les agents impliqués ont été licenciés, et une enquête reste en cours.

Source : https://thehackernews.com/2025/05/coinbase-agents-bribed-data-of-1-users.html

LES AVIS DE SÉCURITÉ DU CERT-FR

Du 16 mai 2025

- Vulnérabilités dans IBM QRadar SIEM
- Vulnérabilités dans le noyau Linux de Red Hat
- Vulnérabilités dans les produits Nextcloud
- Vulnérabilité dans Microsoft Defender pour Endpoint
- Vulnérabilités dans Microsoft Edge
- Vulnérabilité dans Spring Framework
- Vulnérabilité dans Synacor Zimbra Collaboration
- Vulnérabilité dans Python
- Vulnérabilités dans Ivanti Endpoint Manager Mobile (EPMM)

Source : https://www.cert.ssi.gouv.fr/

Le club cyber

elle

LE DÉBAT DE LA SEMAINE

Peut-on encore dissocier cybersécurité et sécurité physique dans un secteur aussi exposé que celui des cryptomonnaies ?

DONNE TON AVIS DANS LES COMMENTAIRES !