27 mai 2025 - EDITION N°26

LES ACTUS CYBER DE LA SEMAINE

SWIPE A DROITE POUR EN SAVOIR PLUS →

DES HACKEURS RUSSES CIBLENT LA LOGISTIQUE UKRAINIENNE

Du 21 mai 2025

Des hackers russes liés au groupe APT28 (Fancy Bear), affilié aux services de renseignement militaire russes (GRU), mènent depuis 2022 une campagne de cyberespionnage visant à perturber l'aide internationale à l'Ukraine. Selon une alerte conjointe de 21 agences de renseignement et de cybersécurité, ils ont compromis des organisations dans les secteurs de la défense, du transport, de l'informatique et du trafic aérien dans 12 pays européens et aux États-Unis, utilisant diverses techniques d'intrusion comme le phishing, l'exploitation de vulnérabilités et le piratage de plus de 10 000 caméras de surveillance pour suivre les mouvements de matériel vers l'Ukraine, notamment aux frontières et sur les installations militaires.

Source : https://www.bleepingcomputer.com/news/security/russian-hackers-breach-orgs-to-track-aid-routes-to-ukraine/

UNE COMMISSION IRLANDAISE AUTORISE META À UTILISER LES DONNÉES DES EUROPÉNS POUR ENTRAINER SES MODÈLES D'IA

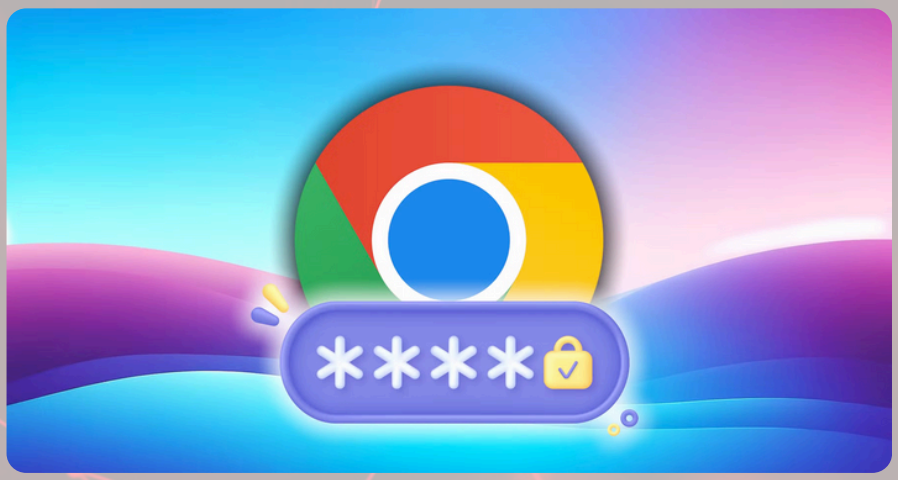
Du 22 mai 2025

La Commission irlandaise de protection des données (DPC) a autorisé Meta à commencer l'exploitation des publications publiques des citoyens européens pour entraîner son IA dès le 27 mai 2025, malgré les contestations juridiques en cours. Meta a apporté plusieurs améliorations à sa proposition, comme des notifications de transparence actualisées, un formulaire d'opposition plus accessible et une période de préavis prolongée, satisfaisant ainsi les préoccupations initiales de cette commission.

L'organisation de défense de la vie privée "noyb" et d'autres groupes contestent cette décision, affirmant que l'utilisation prévue viole le RGPD. Une décision judiciaire en Allemagne, attendue prochainement, pourrait potentiellement bloquer les plans de Meta.

Source : https://www.theregister.com/2025/05/22/irish_data_protection_commission_gives/

GOOGLE CHROME AUTOMATISERA BIENTÔT LE CHANGEMENT DE MOTS DE PASSE PIRATÉS



Du 22 mai 2025

Google Chrome va bientôt introduire une fonctionnalité permettant de changer automatiquement les mots de passe compromis. Lorsque Chrome détectera qu'un mot de passe a été volé ou est trop faible, il proposera non seulement de le modifier, mais pourra également effectuer ce changement automatiquement en arrière-plan avec l'autorisation de l'utilisateur. Cette nouvelle fonctionnalité a été présentée lors de la conférence “Google I/O”. Le déploiement sera progressif à partir de 2025, commençant par un nombre limité de sites web avant de s'étendre.

Source : https://siecledigital.fr/2025/05/22/mot-de-passe-pirate-google-chrome-sen-charge-bientot-pour-vous/

DES HACKERS UTILISENT TIKTOK POUR PIÉGER LES UTILISATEURS AVEC DE FAUX TUTORIELS

Du 23 mai 2025

Des cybercriminels utilisent des vidéos TikTok comme nouveau vecteur de distribution de logiciels malveillants Vidar et StealC via la technique ClickFix. Les cybercriminels créent des vidéos TikTok, possiblement générées par IA, prétendant enseigner comment activer gratuitement Windows, Office, Spotify ou CapCut, mais guidant en réalité les utilisateurs à exécuter des commandes PowerShell malveillantes dans leur système. Certaines vidéos ont atteint près de 500 000 vues avec plus de 20 000 likes avant la suppression des comptes.

Source : https://thehackernews.com/2025/05/hackers-use-tiktok-videos-to-distribute.html

DES HACKEURS RUSSES COMPROMETTENT PLUS D'UNE VINGTAINE D'ONG

Du 27 mai 2025

Des hackers russes affiliés au groupe Void Blizzard ont compromis plus de 20 ONG européennes et américaines en utilisant des techniques de phishing via de fausses pages Microsoft Entra. Active depuis avril 2024, cette campagne d'espionnage cible principalement des organisations stratégiques pour la Russie, notamment dans les secteurs gouvernemental, de la défense, des transports et des ONG soutenant l'Ukraine ou membres de l'OTAN. Les attaquants utilisent des emails de phishing contenant de fausses invitations à des sommets de défense européens, avec des codes QR malveillants redirigeant vers des sites de phishing basés sur le kit Evilginx pour voler les identifiants des victimes. Microsoft indique que le groupe utilise également des identifiants volés achetés sur des marchés cybercriminels et a été lié à la compromission d'une agence de police néerlandaise en septembre 2024, cherchant des informations sur les équipements militaires occidentaux et l'aide à l'Ukraine.

Source : https://thehackernews.com/2025/05/russian-hackers-breach-20-ngos-using.html

Le club cyber

elle

LE DÉBAT DE LA SEMAINE

META DEVRAIT-IL AVOIR LE DROIT D'ENTRAINER SES MODÈLES D'IA SUR LES DONNÉES DES EUROPÉENS ?

DONNE TON AVIS DANS LES COMMENTAIRES !