01 avril 2025 - EDITION N°18

LES ACTUS CYBER DE LA SEMAINE

SWIPE A DROITE POUR EN SAVOIR PLUS →

INTERSPORT VISÉ PAR UNE CYBERATTAQUE : LES DONNÉES DE 3 MILLIONS DE CLIENTS TOUCHÉES

Du 25 mars 2025

L'enseigne de sport a confirmé une intrusion informatique ayant entraîné le vol des données personnelles d'environ 3,4 millions de clients français. Les informations dérobées incluent noms et adresses, mais pas de données bancaires ni mots de passe. La base de données volée a été mise en vente sur un forum clandestin, faisant craindre des tentatives de phishing ciblées.

Source : https://www.rtl.fr/actu/sciences-tech/intersport-vise-par-une-cyberattaque-les-donnees-de-3-millions-de-clients-touches-7900487698

ESPIONNAGE DANS UNE TÉLÉCOM ASIATIQUE

Du 25 mars 2025

Selon un rapport de la société Sygnia, un groupe de hackers lié à la Chine, surnommé "Weaver Ant", a infiltré pendant plus de quatre ans le réseau d'un important opérateur télécom en Asie. Les pirates ont exploité des routeurs vulnérables pour installer des portes dérobées et maintenir un accès discret aux serveurs de l'entreprise, siphonnant des données sensibles tout en échappant à la détection.

Source : https://thehackernews.com/2025/03/chinese-hackers-breach-asian-telecom.html

CYBERATTAQUE : AUTOSUR VICTIME D'UNE FUITE DE DONNÉES DE MILLIONS DE CLIENTS

Du 28 mars 2025

Le réseau français de contrôle technique a annoncé une cyberattaque aboutissant à une fuite de données concernant jusqu'à 12 millions de clients. Les informations compromises comprennent noms, coordonnées, identifiants chiffrés et données techniques des véhicules. Environ 3 Go de données volées sont déjà en vente sur le darknet. Autosur a alerté la CNIL et contacté les clients concernés.

Source : https://www.bfmtv.com/tech/cybersecurite/cyberattaque-autosur-confirme-le-vol-de-4-millions-de-donnees-clients_AN-202503280307.html

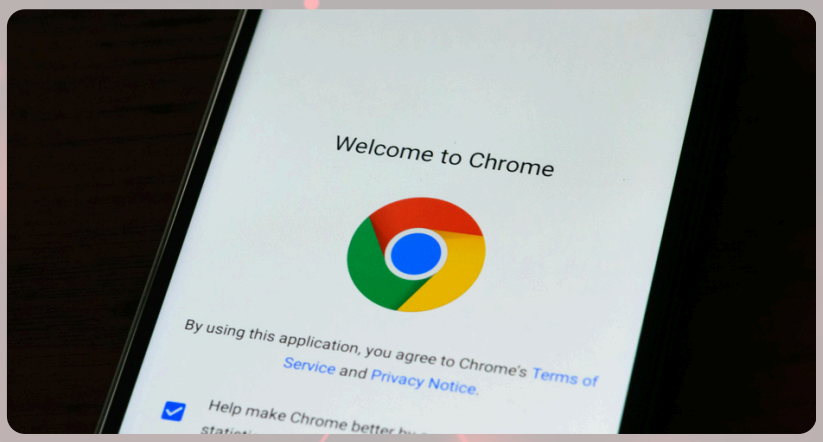
UNE MENACE DE CYBERSÉCURITÉ DÉTECTÉE À L'AÉROPORT DE KUALA LUMPUR

Du 26 mars 2025

Les autorités malaisiennes ont détecté une menace cyber sur les systèmes de l'aéroport international. Les pirates ont exigé une rançon de 10 millions de dollars. Le Premier ministre Anwar Ibrahim a publiquement refusé de payer, déclarant qu'il était hors de question de céder à un ultimatum criminel. Les opérations aériennes ont été maintenues grâce à des mesures d'urgence.

Source : https://www.bangkokpost.com/world/2987848/cyber-security-threat-detected-at-klia-according-to-malaysia-airports

GOOGLE CORRIGE UNE FAILLE ZERO DAY EXPLOITÉE DANS CHROME



Du 26 mars 2025

Une vulnérabilité critique, identifiée comme CVE-2025-2783, a été découverte dans Google Chrome, permettant aux attaquants de contourner les protections de la sandbox. Cette faille a été activement exploitée dans des attaques de cyberespionnage, notamment via des liens de phishing ciblant des professionnels des médias, des institutions éducatives et des agences gouvernementales. En réponse, Google a publié un correctif d'urgence et exhorte tous les utilisateurs à mettre à jour leur navigateur immédiatement pour se protéger contre cette menace.

Source : https://www.lemondeinformatique.fr/actualites/lire-google-corrige-une-faille-zero-day-exploitee-dans-chrome-96443.html

Le club cyber

elle

LE DÉBAT DE LA SEMAINE

Face à la recrudescence des fuites de données et des cybermenaces, quelle est selon vous la plus grande faiblesse actuelle en cybersécurité ?

DONNE TON AVIS DANS LES COMMENTAIRES !