18 mars 2025 - EDITION N°16

LES ACTUS CYBER DE LA SEMAINE

SWIPE A DROITE POUR EN SAVOIR PLUS →

RAPPORT ANSSI

Du 11 mars 2025

En 2024, l'ANSSI a traité 4 386 événements de sécurité, en hausse de 15 % par rapport à l'année précédente. Trois principales menaces ont marqué l'année : la cybercriminalité, avec une forte hausse des rançongiciels touchant entreprises et institutions ; les attaques de déstabilisation, notamment les DDoS qui ont doublé pendant les Jeux Olympiques ; et l'espionnage, porté par des acteurs liés à la Russie et à la Chine, ciblant les télécommunications et les secteurs stratégiques.

Grâce à une préparation efficace, les cyberattaques n'ont pas perturbé les Jeux Olympiques. L'ANSSI appelle à renforcer la sécurité des systèmes d'information, notamment en appliquant rapidement les correctifs aux vulnérabilités critiques. Elle poursuit également le développement des CSIRT et la mise en œuvre de la directive NIS 2 via le projet de loi Résilience. Enfin, la coopération nationale et internationale a permis plusieurs démantèlements de réseaux cybercriminels, soulignant l'importance d'une mobilisation continue pour renforcer la résilience cyber de la France.

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

RACHAT DE MANTRA

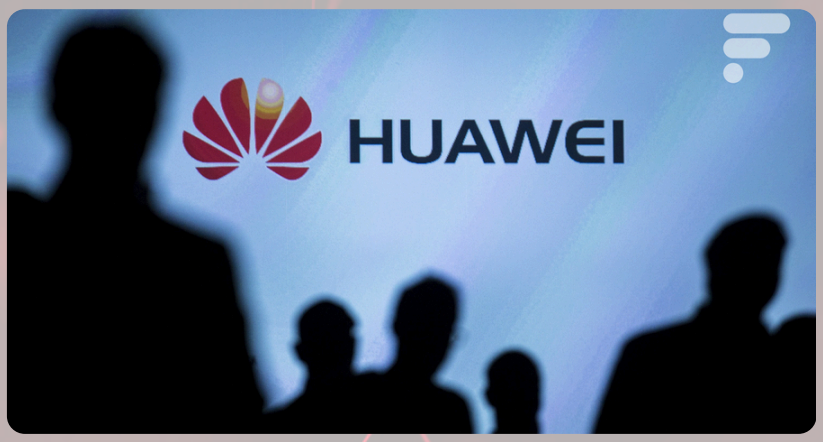
Du 13 mars 2025

Cyber Guru, qui développe un outil de sensibilisation en cybersécurité basé sur des modèles de machine learning, met la main sur Mantra, start-up française également à l'origine d'une plateforme de sensibilisation en entreprise. Cyber Guru devrait disposer d'une plateforme étendue et s'adresser à davantage d'entreprises, notamment les PME et ETI.

Cette acquisition renforcera la présence de Cyber Guru en France en intégrant les solutions de Mantra, lui permettant de mieux adresser les PME et ETI en plus de ses grands comptes.
Les rachats de start-ups françaises de cybersécurité par des acteurs étrangers restent rares. En janvier, Secure-IC a été acquis par Cadence Design Systems, mais en 2024, 11 start-ups sur 12 ont été rachetées par des entreprises françaises, selon Tikehau Capital.

Source : https://www.usine-digitale.fr/article/cybersecurite-l-italien-cyber-guru-s-empare-de-la-plateforme-francaise-de-sensibilisation-mantra.N2228911

CORRUPTION ET HUAWEI



Du 14 mars 2025

L'entreprise chinoise Huawei est soupçonnée d'avoir corrompu une quinzaine de députés européens. La police belge a mené des perquisitions à Bruxelles et arrêté plusieurs lobbyistes de Huawei pour corruption, blanchiment et organisation criminelle. Une perquisition a également eu lieu au Portugal, et une arrestation a été effectuée en France.

Les eurodéputés impliqués auraient reçu des avantages sous forme de rémunérations, de voyages ou d'invitations à des événements en échange de prises de position politiques et en violation des règles du Parlement. L'enquête découle d'une surveillance de longue date des services de renseignement belges sur les activités de Huawei en Europe.

Source : https://www.lemonde.fr/economie/article/2025/03/13/le-groupe-chinois-huawei-soupconne-d-avoir-corrompu-une-quinzaine-de-parlementaires-europeens_6580344_3234.html

LOGICIEL ESPION SUR ANDROID : KOSPY

Du 12 mars 2025

Une nouvelle menace de logiciel espion Android, nommée KoSpy, a été découverte par Lookout, une entreprise spécialisée dans la protection contre les cyberattaques mobiles et est attribuée au groupe nord-coréen APT37.
Ce logiciel malveillant se fait passer pour une application utilitaire, ciblant les utilisateurs coréens et anglophones depuis mars 2022.

KoSpy utilise une infrastructure de commande et de contrôle en deux étapes et peut exfiltrer diverses données sensibles, telles que les SMS, les journaux d'appels, la localisation et les fichiers. Des liens d'infrastructure ont été observés avec un autre groupe nord-coréen, APT43, suggérant des opérations chevauchantes.

Source : https://www.lookout.com/threat-intelligence/article/lookout-discovers-new-spyware-by-north-korean-apt37

ENQUÊTE DE LA CNIL SUR FREE

Du 13 mars 2025

À l'automne, Free a subi une cyberattaque exposant les données de 19 millions d'abonnés. En réponse, la CNIL a mené des inspections dans les locaux de Free pour s'assurer du respect des mesures de protection des données. Suite à ces contrôles, elle a engagé une procédure de sanctions contre l'opérateur, s'appuyant sur la loi de 1978 sur la protection des données personnelles.

Un rapporteur a été désigné pour instruire le dossier et déterminer si Free a enfreint le RGPD. En cas de manquements avérés, l'opérateur risque un rappel à l'ordre, une amende pouvant atteindre 20 millions d'euros ou 4 % de son chiffre d'affaires, ainsi qu'une obligation de mise en conformité sous peine de nouvelles sanctions.

Source : https://www.01net.com/actualites/cyberattaque-free-cnil-enquete-manquements-rgpd.html

Le club cyber

elle

LE DÉBAT DE LA SEMAINE

Cette acquisition de Mantra par Cyber Guru soulève-t-elle des questions sur la souveraineté des entreprises françaises en cybersécurité face à des acteurs étrangers ?

DONNE TON AVIS DANS LES COMMENTAIRES !