13 mai 2025 - EDITION N°24

LES ACTUS CYBER DE LA SEMAINE

SWIPE A DROITE POUR EN SAVOIR PLUS →

CONDAMNATION DE NSO GROUP DANS L'AFFAIRE JUDICIAIRE L'OPPOSANT À META

07 Mai 2025

En 2018 et 2019, Meta a accusé NSO d'avoir placé le logiciel espion Pegasus sur environ 1400 téléphones portables par la messagerie WhatsApp. L'entreprise israélienne a ainsi permis à l'un de ses clients d'espionner les échanges et données personnelles des propriétaires de ces smartphones.

Le jury fédéral a rendu la décision dans laquelle il condamne NSO Group à verser à Meta approximativement 168 millions de dollars américains (148 millions d'euros) au titre des dommages résultant de la compromission, en 2019, des serveurs de WhatsApp afin d'y déployer l'espiologiciel Pegasus. Ce dernier a visé plus de 1400 personnes.

Sources :

- **InCyber : https://incyber.org/article/logiciel-espion-pegasus-nso-group-condamne-verser-167-millions-dollars-meta/**
- **L'Usine Digitale : https://www.usine-digitale.fr/article/nso-group-condamne-malware-russe-contre-l-europe-les-5-actus-cyber-de-la-semaine.N2231804**
- **Le Monde : https://www.lemonde.fr/pixels/article/2025/05/07/logiciel-pegasus-la-societe-nso-group-condamnee-a-verser-168-millions-de-dollars-a-meta-pour-piratage-via-l-application-whatsapp_6603746_4408996.html**

UNE OPÉRATION INTERNATIONALE DE POLICE CONTRE PLUSIEURS LOUEURS DE SERVICES DDOS

7 mai 2025

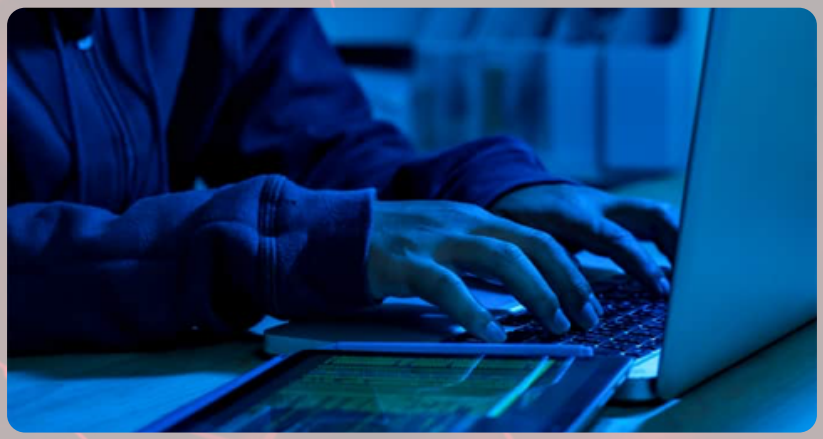
Le 7 mai 2025, Europol a mené une opération contre six structures proposant des outils pour mener des attaques par déni de service distribué (DDoS) contre des écoles, des services gouvernementaux, des entreprises et des plateformes de jeux-vidéos : cfxapi, cfxsecurity, neostress, jetstress, quickdown et zapcut.

Selon l'organisation de police européenne, ces infrastructures étaient louées à des opérateurs responsables d'attaques dans le monde entier et ce, pour la modique somme de dix euros. Dans le cadre de cette opération, les polices polonaises et américaines ont respectivement procédé à quatre arrestations et à la saisie de neuf domaines.

Sources :

- Europol: https://www.europol.europa.eu/media-press/newsroom/news/ddos-for-hire-empire-brought-down-poland-arrests-4-administrators-us-seizes-9-domains
- Clubs : https://www.clubic.com/actualite-564678-europol-demantele-un-empire-cybercriminel-qui-vendait-des-attaques-ddos-pour-seulement-10-euros.html

LOSTKEYS : LE MALWARE UTILISÉ PAR LES PIRATES RUSSES POUR VOLER DES FICHIERS AUX PAYS OCCIDENTAUX



9 mai 2025

L'équipe de renseignement sur les menaces de Google (GTIG) a publié un rapport dans lequel elle associe le malware "Lostkeys" au groupe de cybercriminels soutenu par le renseignement russe Cold River aussi connu sous les noms de Callisto, Star Blizzard et Seaborgium.

Le mode opératoire de ces cybercriminels est généralement de cibler des personnalités importantes via leurs adresses mail personnelles ou celles d'ONG. Tout commence par une fausse vérification Captcha en invitant à copier, coller et exécuter un script PowerShell malveillant.
Par ailleurs, le malware est aussi capable de voler les fichiers directement à partir d'une liste d'extensions et de répertoires codés en dur.

Source :

- L'Usine Digitale : https://www.usine-digitale.fr/article/lostkeys-le-malware-utilise-par-les-pirates-russes-pour-voler-des-fichiers-aux-pays-occidentaux.N2231803

L'ALLEMAGNE FERME EXCH POUR BLANCHIMENT DE 1,9 MILLIARD DE DOLLARS ET SAISIT 34 MILLIONS D'EUROS EN CRYPTO-MONNAIES

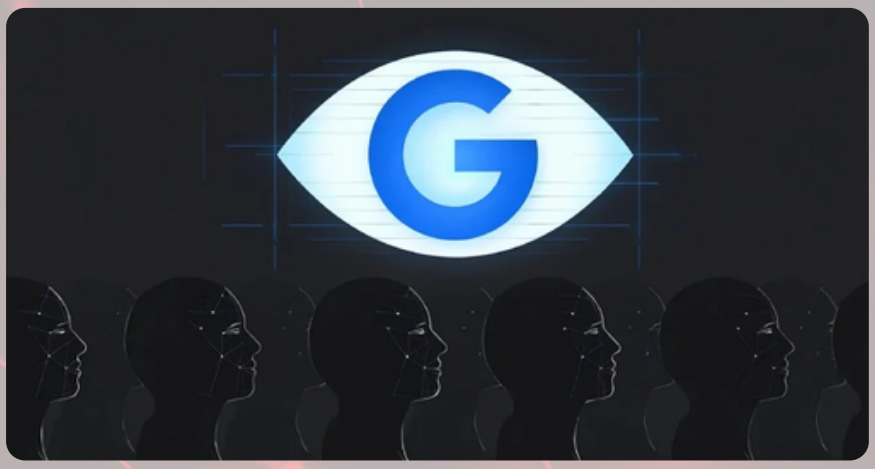
10 mai 2025

L'Office fédéral de la police criminelle allemande (BKA) a saisi et fermé la plateforme en ligne d'échanges de cryptomonnaies "eXch" pour blanchiment de capitaux. L'opération a permis la confiscation de 8 téraoctets de données et de 34 millions d'euros en Bitcoin, Ether, Litecoin et Dash.
Selon la BKA, eXch existe depuis 2014 et offrait des services d'échange de crypto-monnaie sur le clearnet mais aussi sur le darkweb, facilitant ainsi le blanchiment de fonds issus d'activités criminelles. Les actifs de crypto-monnaie sont estimés à 1,9 milliard de dollars et ont été transférés grâce au service depuis son lancement.

Sources :

- **The Hacker News : https://thehackernews.com/2025/05/germany-shuts-down-exch-over-19b.html**
- **Bitcoin.com News : https://news.bitcoin.com/fr/les-autorites-allemandes-ferment-le-service-de-crypto-exch-saisissent-34-millions-deuros-de-fonds-blanchis/#google_vignette**

GOOGLE VERSE 1,375 MILLIARD DE DOLLARS AU TEXAS POUR LE SUIVI NON AUTORISÉ ET LA COLLECTE DE DONNÉES BIOMÉTRIQUES



10 mai 2025

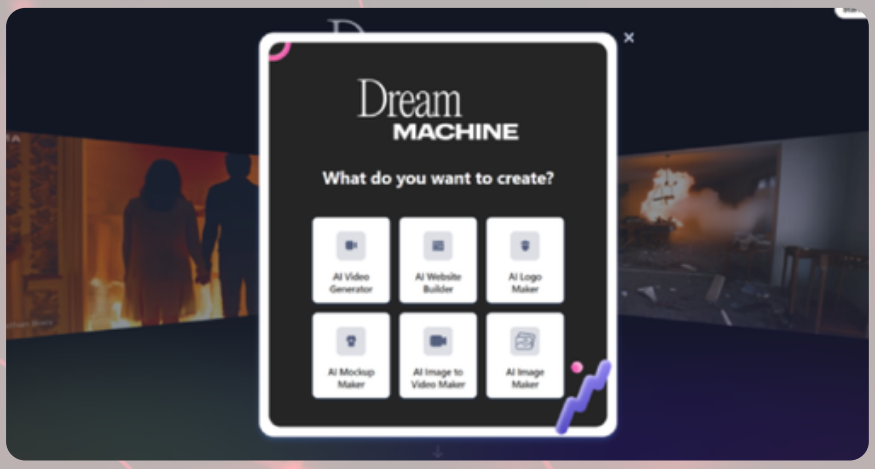
L'affaire datant de 2022, portait sur le suivi et la collecte illégaux des données des utilisateurs concernant la géolocalisation, les recherches incognito, les données biométriques, le suivi des trajets des utilisateurs même lorsque l'historique de localisation était désactivé.

Google a accepté de payer environ 1,4 milliard de dollars à l'Etat du Texas pour régler deux poursuites accusant l'entreprise de suivre l'emplacement personnel des utilisateurs et de conserver leurs données de reconnaissance faciale sans consentement.
En novembre 2022, Google avait déjà versé 391 millions de dollars à un groupe de 40 Etats, en janvier 2023 il a versé 29,5 millions de dollars à l'Indiana et Washington puis 93 millions de dollars supplémentaire en septembre pour régler avec la Californie.

Sources :

- **The Hacker News : https://thehackernews.com/2025/05/google-pays-1375-billion-to-texas-over.html**

L'INTELLIGENCE ARTIFICIELLE (IA) UTILISÉE POUR PROPAGER LE LOGICIEL MALVEILLANT NOODLOPHILE



12 mai 2025

Des acteurs malveillants exploitent de faux outils basés sur l'IA pour inciter les utilisateurs à télécharger un logiciel malveillant capable de voler leurs informations : Noodlophile.

Plutôt que de recourir à des techniques traditionnelles de phishing ou à des sites logiciels piratés, ces cybercriminels créent des plateformes attrayantes sur le thème de l'IA, souvent promues via des groupes Facebook semblant légitimes et des campagnes virales sur les réseaux sociaux selon le chercheur Morphisec Shmuel Uzan.

Les publications partagées sur ces pages ont attiré plus de 62 000 vues sur un unique post, indiquant ainsi que les cibles de campagne sont les personnes recherchant des outils d'IA pour l'édition d'images et de vidéos. Parmi les pages frauduleuses identifiées figurent Luma Dreammachine AI, Luma Dreammachine et gratistuslibros.

Source :

- **The Hacker News : https://thehackernews.com/2025/05/fake-ai-tools-used-to-spread.html**

Le club cyber

elle

LE DÉBAT DE LA SEMAINE

Selon vous, les amendes infligées aux géants de la tech permettent-elles réellement de prévenir les abus de ces derniers ?

DONNE TON AVIS DANS LES COMMENTAIRES !