08 avril 2025 - EDITION N°19

LES ACTUS CYBER DE LA SEMAINE

SWIPE A DROITE POUR EN SAVOIR PLUS →

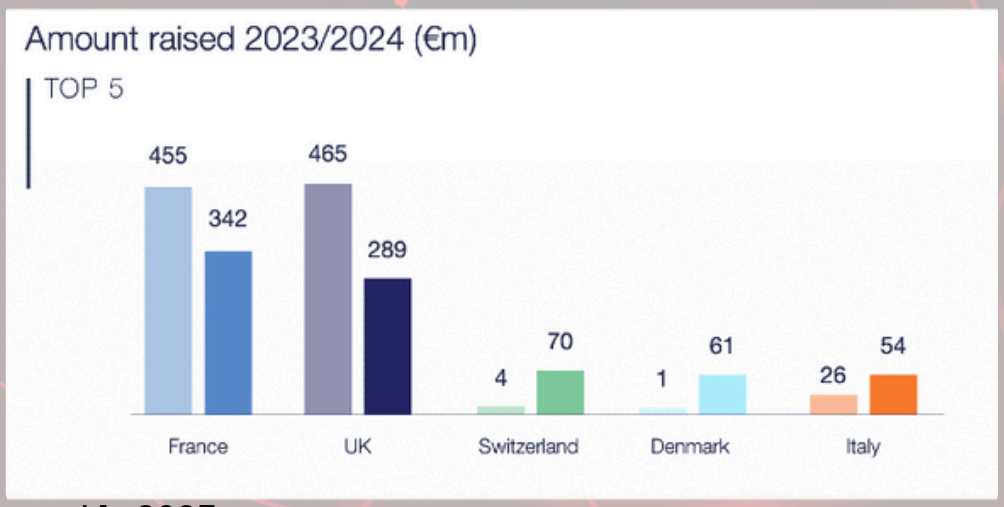
REBRANDING DU COLLECTIF CRIMINEL HUNTERS

Du 2 avril 2025

Les experts de Group-IB ont récemment publié une analyse concernant le groupe de ransomware Hunters International. Selon eux, il s'agirait d'un rebranding de ce collectif criminel, accompagné d'un changement stratégique visant à faciliter la continuité de leurs activités de rançonnage. Group-IB avance que la transition de Hunters International vers WorldLeaks pourrait être liée aux interventions des forces de l'ordre ciblant les opérateurs de BaaaS.
À partir de discussions internes interceptées, les chercheurs pensent que les opérateurs de Hunters cherchent à simplifier leurs attaques en se concentrant uniquement sur l'exfiltration de données.

Source : https://www.lemagit.fr/actualites/366621730/Ransomware-le-debut-de-la-fin-pour-Hunters-International

LA FRANCE EN TÊTE DES LEVÉES DE FONDS CYBER EN EUROPE



Du 7 avril 2025

L'étude de Tikehau Capital sur les investissements dans le secteur de la cybersécurité, révélè que la France est devenue le premier pays européen en termes de levées de fonds dans le secteur de la cybersécurité. En 2024, les start-ups françaises du domaine ont levé près de 620 millions d'euros, représentant plus de 30 % du total européen.
Ce classement place la France devant l'Allemagne et le Royaume-Uni, historiquement en tête sur ces questions. Les levées de fonds ont bénéficié à des acteurs comme HarfangLab, Filigran, ou encore CybelAngel, qui ont su convaincre investisseurs privés et publics de leur potentiel dans un contexte de forte croissance des cybermenaces.

Source : https://www.lemondeinformatique.fr/actualites/lire-la-france-en-tete-en-europe-des-levees-de-fonds-en-cybersecurite-96517.html

https://www.tikehaucapital.com/~/media/Files/T/Tikehau-Capital-V2/documents/news-and-views/en/2025/Tikehau-Capital-Barometre-2025-EN-AP.pdf

GCP CORRIGE UNE VULNÉRABILITÉ CRITIQUE

Du 03 avril 2025

Google Cloud a corrigé une vulnérabilité critique, nommée ImageRunner, découverte par la société de cybersécurité Tenable. Cette faille permettait à des attaquants d'accéder sans autorisation aux images de conteneurs privés sur Google Cloud Platform (GCP), en contournant les mécanismes d'authentification. Les conséquences potentielles incluaient une escalade de privilèges, le vol de données sensibles et des actes d'espionnage. Google a rapidement déployé un correctif pour remédier à cette vulnérabilité avant qu'elle ne soit exploitée

Source : https://www.lemondeinformatique.fr/actualites/lire-google-cloud-corrige-une-faille-exposant-des-images-de-conteneurs-prives-96519.html

PATRICK POUYANNÉ, DEMANDE LA CRÉATION D'UN CLOUD EUROPÉEN..

Du 03 avril 2025

Lors du Forum InCyber à Lille, Patrick Pouyanné, PDG de TotalEnergies, a exprimé son inquiétude face à la dépendance de son entreprise aux technologies cloud américaines, notamment celles d'Amazon, Microsoft et Google. Il a souligné son malaise à confier des données stratégiques, telles que celles issues des investissements sismiques et géophysiques annuels de près d'un milliard de dollars, à des clouds américains. Selon lui, cette situation illustre une "guerre économique" où les enjeux de souveraineté numérique sont cruciaux. l plaide pour la mise en place d'un cloud européen souverain, afin d'échapper au choix contraint entre les géants du cloud américains et chinois. Face à cette dépendance, l'industriel a opté pour une stratégie d'hébergement local (on-premise) pour ses données sensibles.

Source :https://www.usine-digitale.fr/article/fic-2025-patrick-pouyanne-pdg-de-totalenergies-appelle-a-la-creation-d-un-cloud-europeen.N2230104

GOOGLE CORRIGE UNE FAILLE ZERO DAY EXPLOITÉE DANS CHROME

Du 01 avril 2025

Aujourd'hui certains groupes cybercriminels revendiquent désormais des cyberattaques qu'ils n'ont pas réellement commises.
Le but ? Gagner en visibilité, semer la confusion, faire pression sur des victimes ou recycler d'anciennes fuites de données pour maximiser l'effet d'intimidation.
Ces « vraies-fausses attaques » peuvent consister à :

- Publier de fausses preuves d'intrusion,
- Revendiquer une attaque réelle commise par un autre groupe,
- Menacer des entreprises avec des données déjà compromises dans des incidents antérieurs.

Source :https://www.lemagit.fr/actualites/366621834/Ransomware-bienvenue-dans-lere-des-vraies-fausses-cyberattaques

Le club cyber

elle

LE DÉBAT DE LA SEMAINE

Investir dans un cloud souverain : une nécessité stratégique ou un gouffre financier ?

DONNE TON AVIS DANS LES COMMENTAIRES !