AEGE

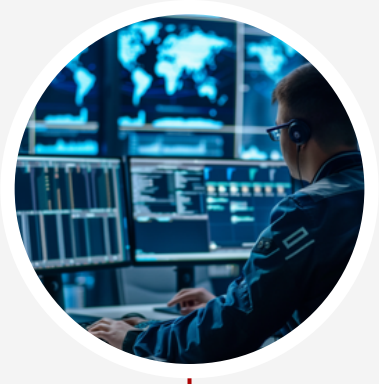
Club Cyber

BULLETIN DE VEILLE CYBER

10 décembre 2024

EDITION N°4

RAPPORT 2024 D'ELASTIC SUR LES MENACES MONDIALES



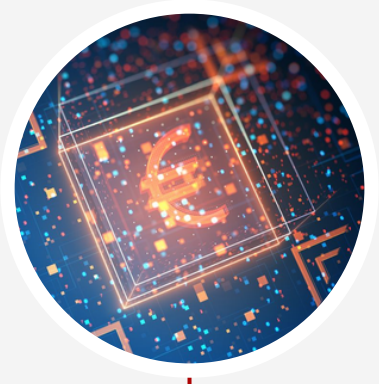
[7 DECEMBRE 2024] - Elastic et son laboratoire de recherche Elastic Security Labs partagent les grandes tendances en matière de cyberattaques par malware observées au cours des 12 derniers mois.

Les observations du laboratoire par système d'exploitation (OS) :

- Windows reste l'OS le plus ciblé par les malwares (66,12 %). Windows n'est pas plus vulnérable que les autres systèmes d'exploitation, il est juste plus ciblé par les cyberattaquants.
- MacOS ne représente que 1,68 % des attaques, le volume de données télémétriques le plus faible, mais le risque n'en est pas moins grand.
- Linux rassemble un tiers des attaques (32,20 %). Les packages pour les backdoors sont également une source d'intérêt pour les attaquants.

Source : https://www.elastic.co/fr/resources/security/report/global-threat-report

UN MALWARE CIBLE LES CLIENTS DES BANQUES FRANÇAISES



[6 ET 7 DECEMBRE 2024] - DroiBot, un cheval de Troie actif depuis juin 2024 et découvert fin octobre, cible les utilisateurs de 77 entités, dont des banques, des institutions financières et des plateformes d'échange de cryptomonnaies. En France, il s'attaque à des banques majeures telles que Boursorama, BNP Paribas, Crédit Agricole, Axa Banque, Caisse d'Épargne, Banque Populaire, ING et Société Générale.

La France figure parmi les cibles principales, particulièrement vulnérable dans un contexte de nombreuses fuites de données récentes, comme celle de Norauto ayant touché 80 000 clients.

Les entreprises concernées sont invitées à renforcer leur vigilance et leurs mesures de cybersécurité face à ce malware qui vise directement les finances des utilisateurs.

Source : https://www.clubic.com/actualite-546137-banques-francaises-sont-en-train-de-subir-une-cyberattaque-protegez-vous.html

LA SUPPLY CHAIN TOUJOURS À L'ÉPREUVE DES CYBERATTAQUES

[6 DECEMBRE 2024] - Avec l'essor de l'industrie 4.0, les attaques sur la chaîne d'approvisionnement exploitent les vulnérabilités des réseaux interconnectés pour compromettre la sécurité des systèmes.

Ces menaces incluent :

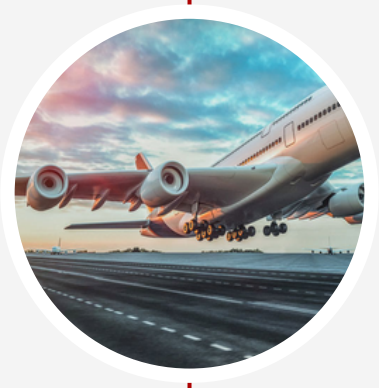
- Les attaques logicielles par la compromission de mises à jour ou d'applications ;
- Les attaques matérielles par la manipulation de composants physiques ;
- Les attaques par firmware, par injection de malwares dans le code de démarrage ;
- Les attaques via fournisseurs tiers par l'exploitation des relations de confiance.

Ces intrusions visent l'accès non autorisé à des données sensibles ou l'introduction de failles critiques, perturbant les opérations des entreprises.

Source : https://blog.economie-numerique.net/2024/12/06/la-chaine-dapprovisionnement-a-lepreuve-des-cyberattaques/

Chloé Quintas

TRANSPORT AÉRIEN : +20% DE CYBERATTAQUES EN 2024



[6 DECEMBRE 2024] - Le transport aérien est une cible de plus en plus populaire pour les pirates informatiques. La 130e Assemblée Générale de l'ATAF, qui s'est tenue du 22 au 24 novembre à Abidjan, a mis en exergue une hausse de 20% des cyberattaques cette année dans le secteur du transport aérien. L'Afrique est particulièrement touchée puisque ses infrastructures restent vulnérables après une cyberattaque.

Les compagnies aériennes, grandes et petites, subissent des intrusions régulières, parfois quotidiennes, pouvant aller jusqu'à perturber gravement les systèmes informatiques, voire paralyser les opérations.

L'IA a quant à elle été perçue comme une solution qui complète l'Homme plus qu'elle ne le remplacerait.

Source : https://www.linfodrome.com/economie/103977-transport-aerien-des-experts-revelent-une-augmentation-de-20-des-cyberattaques-en-2024

RAPPORT ANNUEL D'ORANGE CYBERDEFENSE SUR LES HACKTIVISTES

[5 DECEMBRE 2024] - Le menace s'intensifie en Europe selon le dernier rapport de recherche en sécurité annuel d'Orange Cyberdefense (Security Navigator 2025). Les hacktivistes – hackers et activistes – ciblent de plus en plus les entreprises européennes, leurs motivations sont d'ordre politique de manière criminelle.

Des groupes comme NoName, UserSec ou Anonymous Sudan, motivés par des causes politiques, poursuivront leurs cyberattaques en 2025. Actifs sur des forums et sur Telegram, ils utilisent des techniques rudimentaires mais symboliques pour paralyser des systèmes informatiques en protestation ou en soutien à des causes. Selon une analyse de 20 706 incidents en 2024, ces opérations, amplifiées par l'IA, figureront parmi les principales cybermenaces européennes.

Source : https://www.lefigaro.fr/secteur/high-tech/cybersecurite-les-entreprises-de-plus-en-plus-ciblees-par-les-hacktivistes-20241205

MICROSOFT EXIGE TPM 2.0 POUR L'UTILISATION DE WINDOWS 11

[4 DECEMBRE 2024] - Avec la fin du support de Windows 10 en octobre 2025, les utilisateurs de PC incompatibles avec Windows 11 devront envisager de remplacer leur appareil.

Microsoft exige, sans exception, un module TPM 2.0 pour installer Windows 11, excluant ainsi de nombreux ordinateurs encore performants. Le TPM permet de certifier la chaine de démarrage pour garantir son intégrité.

Le TPM, intégré à la carte mère ou sous forme de puce, renforce la sécurité en protégeant les clés de chiffrement, mots de passe et certificats. Après octobre 2025, les utilisateurs devront soit changer de matériel, soit continuer avec Windows 10 sans bénéficier des mises à jour de sécurité essentielles.

Source : https://www.justgeek.fr/windows11-tpm-non-negociable-132795/?utm_campaign=Cyber%2BLettre&utm_medium=web&utm_source=Cyber_Lettre_248

Chloé Quintas