25 mars 2025 - EDITION N°17

LES ACTUS CYBER DE LA SEMAINE

SWIPE A DROITE POUR EN SAVOIR PLUS →

VULNÉRABILITÉ 0-DAY PRÉSENTE DANS WINDOWS

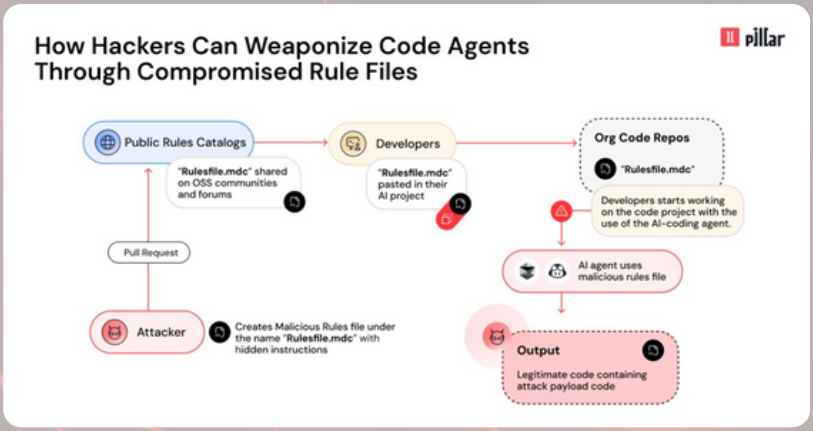
Du 18 mars 2025

The Hacker News rapporte l'analyse de deux chercheurs de Trend Micro sur une vulnérabilité nommée ZDI-CAN-25373. Par définition, le ZDI fait référence au Zero Day Initiative, un programme qui identifie, et publie des vulnérabilités de sécurité. Elles sont découvertes avant que les éditeurs de logiciels n'en soient informés pour les corriger.

Cette menace exposerait les organisations à des risques de vols de données et d'espionnage, notamment parce qu'elle est exploitée par des APT « *parrainés par des Etats de Corée du Nord, d'Iran, de Russie et de Chine. Des organisations des secteurs gouvernemental, financier, des télécommunications, militaire et de l'énergie ont été touchées en Amérique du Nord, en Europe, en Asie, en Amérique du Sud et en Australie* ».

Source : https://www.trendmicro.com/en_us/research/25/c/windows-shortcut-zero-day-exploit.html

NOUVELLE ATTAQUE À LA CHAÎNE D'APPROVISIONNEMENT POUR LES IA GÉNÉRÉES PAR DES ÉDITEURS DE CODE



Du 18 mars 2025

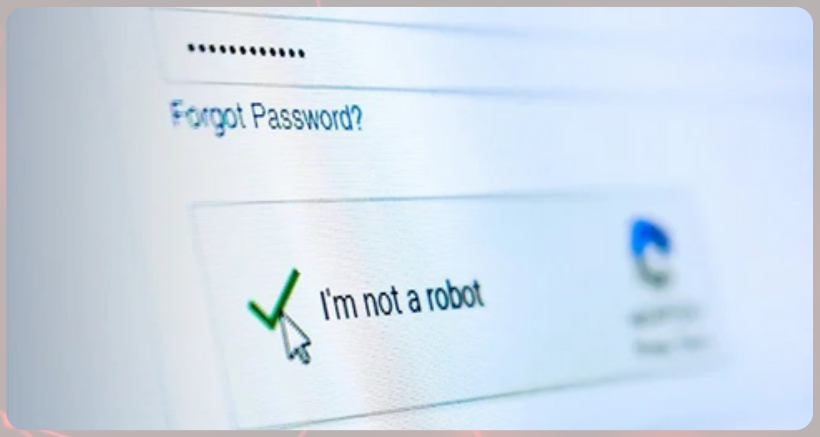
Des chercheurs de Pillar ont révélé des détails d'une nouvelle attaque par la chaîne d'approvisionnement appelée Rules File Backdoor. Cette porte dérobée concerne les intelligences artificielles générées par des éditeurs de code tels que GitHub Copilot et Cursor, les poussant à injecter du code malveillant.

Cela permet aux attaquants de compromettre ces systèmes en toute discrétion en injectant des commandes malveillantes dans des fichiers de configuration apparemment inoffensifs. De plus, cette technique a l'avantage de contourner les tests et revues de codes traditionnels.

Par ailleurs, la multiplicité des failles dans les logiciels open source et commerciaux tiers, ciblant les pipelines de développement de l'IA, exacerbent les problèmes de sécurité de la chaîne d'approvisionnement logicielle.

Source : https://thehackernews.com/2025/03/new-rules-file-backdoor-attack-lets.html

CAPTCHA : QUAND LA SÉCURITÉ DEVIENT UNE MENACE



Du 20 mars 2025

Une étude publiée par HP Wolf Security le 18 mars révèle que les CAPTCHA truqués deviennent une méthode privilégiée par les cybercriminels pour diffuser des logiciels malveillants, tels que Lumma Stealer, un cheval de Troie capable de compromettre discrètement les systèmes ciblés.

Les hackers exploitent la banalisation des CAPTCHA et de la vigilance réduite des utilisateurs. En effet, ce phénomène se nomme la « *tolérance aux clics* » qui pousse les internautes à cliquer mécaniquement sur des éléments d'apparence légitime sans vérifications approfondies.

Sous leur apparence crédible, ces faux CAPTCHA lancent secrètement des scripts dangereux à travers des outils systèmes tels que Microsoft PowerShell, contournant ainsi les antivirus les plus courants.

Source : https://siecledigital.fr/2025/03/20/les-captcha-detournes-par-les-hackers-quand-la-securite-devient-une-menace/

VPENTEST : 10 RÉSULTATS CRITIQUES DU TEST DE RÉSEAU « PENTEST » NÉGLIGÉS PAR LES ÉQUIPES IT

Du 21 mars 2025

Après avoir effectué plus de 10 000 tests automatisés de pénétration de réseau interne l'année dernière, vPenTest a découvert que de nombreuses entreprises ont encore des failles de sécurité critiques que les attaquants peuvent facilement exploiter. En ce sens, cette plate-forme aide les organisations à trouver des vulnérabilités exploitables avant que les cybercriminels ne le puissent.

Voici comment se décompensent les risques : 50% d'erreurs de configurations, 30% de correctifs manquants et 20% de mots de passe faibles.

L'article développe également les 10 risques les plus importants concernant la sécurité du réseau interne : que sont-ils, pourquoi sont-ils dangereux et des recommandations afin de mitiger au risque, même s'il est le moins courant.

Source : https://thehackernews.com/2025/03/10-critical-network-pentest-findings-it.html

L’AGENCE BRITANNIQUE DE CYBERSÉCURITÉ MET EN GARDE CONTRE LE RISQUE DE PIRATAGE QUANTIQUE

Du 20 mars 2025

L’agence britannique de cybersécurité, le National Cyber Security Center (NCSC), a publié de nouvelles directives pour inciter les organisations à se préparer contre les menaces posées par les ordinateurs quantiques d’ici à 2035. Le chiffrement serait le principal domaine concerné par cette menace, car il pourrait souffrir des avancées technologiques en matière de quantique.

En ce sens, le NCSC recommande aux grandes organisations, y compris les fournisseurs d’énergie et de transport, d’introduire le « *chiffrement post-quantique* » afin d’empêcher le déploiement de la technologie quantique pour s’introduire dans leurs systèmes.

Selon ces directives, les organisations devraient suivre ce calendrier : identifier les services nécessitant une mise à niveau d’ici 2028, réaliser les révisions les plus importantes d’ici 2031 et enfin, la migration vers un nouveau système de chiffrement d’ici 2035.

Source : https://www.theguardian.com/technology/2025/mar/20/uk-cybersecurity-agency-quantum-hackers

Le club cyber

elle

LE DÉBAT DE LA SEMAINE

Les entreprises prennent-elles pleinement conscience des opportunités et des risques que représente l'ordinateur quantique pour les années à venir ?

DONNE TON AVIS DANS LES COMMENTAIRES !