BULLETIN DE VEILLE CYBER

25 février 2025

EDITION N°13

ANSSI : LES CYBERATTAQUES EXPLOSENT SUR LES ENVIRONNEMENTS CLOUD

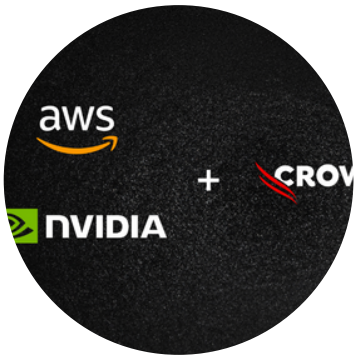
[24 février 2025] - L'Agence nationale de la sécurité des systèmes d'information (ANSSI) tire la sonnette d'alarme concernant l'augmentation des cyberattaques ciblant les environnements cloud. Les vulnérabilités des infrastructures hybrides sont aussi exploitées, élargissant la surface d'attaque pour les cybercriminels. Une fois qu'un cybercriminel a compromis une partie de l'infrastructure (qu'elle soit locale ou cloud), il peut essayer de se déplacer dans l'autre environnement, profitant de la communication entre les deux.

Les groupes tels que Mango Sandstorm et Scattered Spider mènent des campagnes sophistiquées combinant l'extorsion, l'espionnage et le sabotage. Ils pourraient héberger des logiciels malveillants, exfiltrer des données ou lancer des attaques via des serveurs compromis. Ce qui leur permettrait de masquer leurs activités dans un flux de trafic légitime, rendant ainsi leur détection difficile

Les fournisseurs devraient renforcer leur sécurité en proposant des outils de gestion des risques à leurs clients. Les entreprises utilisatrices doivent aussi adopter des pratiques rigoureuses en matière de cybersécurité.

Source : https://www.blogdigital.fr/cyberattaques-sur-cloud-explosent-anssi-tire-sonnette-alarme/

CROWDSTRIKE, AWS ET NVIDIA IMPULSENT L'INNOVATION DANS LE SECTEUR DE L'IA ET DE LA SÉCURITÉ DU CLOUD



[24 février 2025] - CrowdStrike et AWS deux géants du numérique et du Cloud ont sélectionné 36 startups pour un programme d'accélération en cybersécurité avec le soutien de NVIDIA. Pour cette édition 2025, les entreprises sélectionnées bénéficient de mentorat, d'expertise technique et d'opportunités de mise sur le marché pour stimuler l'innovation en IA et sécurité cloud.

Le programme culminera lors d'une journée de démonstration où un jury d'experts choisira un lauréat, pouvant recevoir un financement du CrowdStrike Falcon Fund.

Source : https://www.morningstar.com/news/business-wire/20250223217543/crowdstrike-and-aws-select-36-startups-for-2025-cybersecurity-accelerator-with-support-from-nvidia

ZERO DAY : ROBERT DE NIRO FACE AU CHAOS SUR NETFLIX

[23 février 2025] - La nouvelle série Netflix, Zero Day, mettant en scène Robert De Niro fait parler beaucoup d'acteur de la Cybersécurité. Cette série décrit l'intrigue de thriller politique centrée sur une cyberattaque et une conspiration gouvernementale.

Il s'agit de George Mullen, un ancien président américain contraint de reprendre du service après une cyberattaque dévastatrice, qui paralyse les infrastructures du pays. Une cyberattaque qui démontre plusieurs failles dans tous les systèmes d'exploitation, d'infrastructures critiques, notamment des réseaux électriques, des systèmes de communication et de transport, entraînant des milliers de victimes.

La série et la performance de De Niro, rencontrent un fort engouement tout en évoquant la possibilité d'une saison 2.

Source : https://pointgphone.com/zero-day-sur-netflix-robert-de-niro-saison-2-74751/

Siegfried M.

FAILLES DE L'IA : UNE FLAMBÉE D'INQUIÉTUDES

[23 février 2025] - D'après Sven Cattell foundateur "the AI Village" revient sur les difficultés à garantir la sécurité de l'IA. les approches de Red Team devraient être repensées pour répondre aux évolutions technologiques et aux nouvelles techniques d'attaque. Selon l'article, le fait de tester le potentiel de jailbreaks, de procéder par désinformation ou par hallucinations, et par injection de prompt, ne suffisent plus à garantir la sécurité d'une IA. Pour rappel, Le potentiel de jailbreaks se définit comme étant la facilité avec laquelle un appareil (comme un téléphone) peut être débloqué pour lever les restrictions du fabricant.

Ces inquiétudes sur la vulnérabilité des IA concernent la nouvelle forme d'attaque en passant par la manipulation des modèles, les fuites de données, les deepfakes et les cyberattaques.

La Corée du Sud de son coté à suspendu temporairement le chatbot DeepSeek afin de vérifier la conformité sur la protection des données. Ce qui interroge sur la fiabilité à long terme de l'IA dans le domaine médical et d'autres secteurs critiques.

Source : https://technplay.com/les-modeles-ia-en-danger-les-hackers-mettent-en-lumiere-des-failles/#google_vignette

LE PIRATAGE DE 1,5 MILLIARD DE DOLLARS DE CRYPTO-MONNAIES PAR BYBIT : LA CYBERATTAQUE DU SIÈCLE

[22 février 2025] - Linfodrome rapporte une cyberattaque massive contre la plateforme d'échange de cryptomonnaies Bybit. Les pirates ont dérobé 400.000 Ethereum, l'équivalent de 1,5 milliard de dollars.

Les Hackers ont exploité une faille dans un portefeuille hors ligne "cold wallet", en contournant ainsi le système de multi-signatures. Ce vol n'est pas un cas isolé, et ressemble à d'autres incidents majeurs dans le secteur des cryptomonnaies à l'exemple du le vol de 620 millions de dollars sur le réseau Ronin en 2022.

Les cyberattaques contre ces plateformes de cryptomonnaies mettent en lumière les vulnérabilités du secteur et la nécessité de renforcer leur sécurité.

Source : https://www.linfodrome.com/high-tech/106553-cyberattaque-du-siecle-1-5-milliard-de-cryptomonnaies-derobees-a-bybit

CÔTE D'IVOIRE: IA, DÉFENSE ET VISION D'ALASSANE OUATTARA

[22 février 2025] - Le Gouvernement de la Côte d'Ivoire a publié un communiqué de presse concernant le Salon International sur l'Intelligence Artificielle, de la Défense et de l'Espace (SIADE).

Le ministre de la Transition Numérique et de la Digitalisation Kalil Konaté a souligné l'importance de l'IA pour la croissance et le développement du pays, saluant la vision du Président Alassane Ouattara. Le ministre a aussi mis en évidence les investissements du gouvernement dans les infrastructures numériques, la cybersécurité et les technologies spatiales. Il a également encouragé les jeunes Ivoiriens à participer à la quatrième révolution industrielle et à adopter l'IA.

La Côte d'Ivoire a mis en place une stratégie nationales pour l'IA, avec l'implication de divers acteurs tels que les experts, les chercheurs, les secteurs publics et privés, et les académiciens.

Source : https://pointgphone.com/zero-day-sur-netflix-robert-de-niro-saison-2-74751/

DES HACKERS CHINOIS AU COEUR DES CYBER ATTAQUES DES ETABLISSEMENTS DE SANTÉ EUROPÉEN

[21 février 2025] - Une campagne de ransomware ciblant des établissements de santé européens a été détectée par Orange Cyberdefense. Des cyberattaquants possiblement liés à la Chine, ont exploité une faille de sécurité Check Point pour s'infiltrer dans les réseaux.

Les malwares tels que ShadowPad et PlugX, détectés par Orange Cyberdefense, sont souvent associés à des intrusions chinoises, pour déployer le ransomware "NailaoLocker". Un fichier DLL est téléchargé depuis un exécutable légitime (usysdiag.exe), permettant d'activer ce ransomware. Une fois activé, le ransomware chiffre les fichiers en ajoutant une extension ".locked", puis envoie une note de rançon au format HTML demandant aux victimes de les contacter via une adresse mail Proton. Ces tactiques employées ressembleraient à celles du groupe chinois "Bronze Starlight", soulevant des questions sur les motivations réelles de l'attaque.

Source : https://www.usine-digitale.fr/article/ransomware-plusieurs-etablissements-de-sante-europeens-cibles-par-des-pirates-chinois.N2227764