Veille Technologique

Outil utilisé :

- Feedly

Thème :

- CyberSécurité

Articles consultés :

https://krebsonsecurity.com/2023/04/fbi-seizes-bot-shop-genesis-market-amid-arrests-targeting-operators-suppliers/

Brian Krebs - FBI Seizes Bot Shop 'Genesis Market' Amid Arrests Targeting Operators, Suppliers - 04/04/2023

Le Genesis Market était un site de vente de bots, de systèmes infectés, de comptes volés etc… Ce site a récemment été fermé par le FBI et les administrateurs arrêtés.

https://grahamcluley.com/fake-gpt-chrome-extension-steals-facebook-session-cookies-breaks-into-accounts/

Graham Cluley - Fake GPT Chrome extension steals Facebook session cookies, breaks into accounts - 24/03/2023

Cet article nous apprend que de nombreux hackers ont profité de la popularité récente de ChatGPT pour en faire des faux clones à but malveillants.
En effet, on a pu retrouver sur le Chrome Web Store, des extensions pour navigateur se faisant passer pour ChatGPT.
Cependant, ces extensions étaient fausses et se contentaient de récupérer les cookies de session Facebook pour les envoyer aux hackers. Une fois en sa possession le cyber criminel pouvait s'en servir pour se connecter sur un compte et en faire ce qu'il voulait.

https://www.bbc.com/news/technology-65047304

Ben Derico - ChatGPT bug leaked users' conversation histories - 23/03/2023

Dans cet article, nous apprenons qu'un bug sur le site de ChatGPT a eu lieu et a permis à certains utilisateurs d'avoir accès aux conversations qui ne sont pas les leurs. La compagnie responsable de ChatGPT a vite pris les choses en main et a désactivé l'accès au site pendant un moment pour corriger cette erreur.

Cependant, la présence de ce bug a soulevé de nombreuses craintes auprès des utilisateurs pour leurs données, il semblerait que l'entreprise ait accès à toutes les conversations entre l'intelligence artificielle et eux. L'entreprise a répondu en indiquant que les conversations pouvaient être utilisées pour entraîner le modèle.

https://www.darkreading.com/attacks-breaches/zero-day-bug-crypto-hackers-bitcoin-atms

Dark Reading - Zero-Day Bug Allows Crypto Hackers to Drain $1.6M From Bitcoin ATMs - 21/03/2023

Nous pouvons lire dans cet article que des hackers ont eu accès à la base de données de certains distributeurs de Bitcoins, ils ont pu récupérer notamment les identifiants, les hashs de mots de passe ou les clés des APIs. Les hackers ont pu voler 1.6 million de dollars.

https://thehackernews.com/2023/03/new-shellbot-ddos-malware-targeting.html

Ravie Lakshmanan - New ShellBot DDoS Malware Variants Targeting Poorly Managed Linux Servers - 21/03/2023

Nous apprenons ici qu'un outil de DDOS appelé Shell Bot est également en train de cibler les différents serveurs Linux qui seraient mal protégés. En effet, ce bot prend avantage des nombreux serveurs Linux SSH ayant le port 22 ouvert. Par dessus, le programme utilise une attaque par dictionnaire pour récupérer les identifiants du serveur et se connecter. Ce serveur servira ensuite à attaquer d'autres serveurs.

https://www.usine-digitale.fr/article/ferrari-victime-d-une-cyberattaque.N2113091

Jérôme Marin - Ferrari victime d'une cyberattaque - 21/03/2023

Le constructeur automobile a annoncé le 21 Mars 2023 avoir été victime d'une cyberattaque par ransomware. Ces attaques sont un fléau pour toute entreprise car elle donne lieu au chiffrement de toutes les données de l'entreprise en échange d'une rançon. Le constructeur a cependant indiqué que les données des utilisateurs concernant leurs achats ou leurs informations bancaires n'ont pas été compromises.