Les extensions ChatGPT malveillantes prennent le contrôle de comptes Facebook

Titre HTML : Les cybercriminels profitent de ChatGPT pour pirater les comptes Facebook

Les utilisateurs de ChatGPT ciblés par des cybercriminels

Des cybercriminels ont créé des add-ons frauduleux pour Chrome afin de proposer aux utilisateurs d'ajouter le chatbot ChatGPT, qui s'avère en réalité être un stratagème pour pirater l'accès aux comptes Facebook des utilisateurs. Découverte par la société de sécurité Guardio Labs et signalée par BleepingComputer, la fausse extension se sert de l'API de Chrome Extension pour détecter les cookies actifs de Facebook et envoyer les données volées au serveur de l'attaquant. Les profils piratés sont convertis en celui d'une fausse personne nommée Lily Collins, et ces comptes zombies sont ensuite utilisés pour diffuser des publicités malveillantes et des contenus illicites.

Un stratagème détecté par Guardio Labs

La plupart des personnes exposées à cette fausse extension l'ont probablement téléchargée par le biais d'une publicité sponsorisée dans les recherches Google pour « Chat GPT 4 ». Ce stratagème reflète des attaques similaires sur les utilisateurs de Radeon et de Bitwarden plus tôt cette année. Les utilisateurs de ChatGPT ne remarqueraient pas nécessairement quelque chose d'anormal s'ils devenaient victimes de cette extension. D'après Guardio Labs, cette extension frauduleuse utilise en effet le code du véritable add-on, et l'intégration de ChatGPT dans les résultats de

recherche Google fonctionne toujours. Pour être exposés à la fausse extension, les utilisateurs auraient dû la télécharger à partir du Chrome Web Store entre le 14 février et le 22 mars.

Comment vérifier l'authenticité de ChatGPT

Si ChatGPT for Google est installé sur votre ordinateur et que vous souhaitez vérifier son authenticité, vous pouvez cliquer sur l'icône en forme de puzzle située à droite de la barre d'adresse de Chrome, puis sur Manage Extensions (Gérer les extensions). En cliquant sur le bouton Détails de l'extension, puis sur « Afficher dans Chrome Web Store », vous pouvez vérifier que l'extension appartient bien à « chatgpt4google.com ». De plus, plus d'un million d'utilisateurs ont validé l'extension. Toute autre mention est une contrefaçon.

Une extension frauduleuse qui n'est pas la première du genre

Malheureusement, cette extension frauduleuse n'est pas la première à cibler les personnes curieuses de ChatGPT. Au début du mois de mars, Guardio Labs avait déjà détecté une version antérieure de cette extension malveillante. Cette version utilisait le marketing de Facebook pour attirer les utilisateurs de Chrome. Avec le nombre grandissant d'utilisateurs de ChatGPT, il est probable que d'autres extensions du même type soient créées. Il est donc important d'être vigilant quant aux liens trouvés dans les résultats de recherche Google, d'installer un logiciel antivirus et éventuellement de s'équiper d'un bloqueur de publicités.

Conclusion

En conclusion, les cybercriminels profitent de l'engouement pour ChatGPT pour pirater les comptes Facebook des utilisateurs. Une extension frauduleuse a été découverte et signalée par Guardio Labs, qui affecte les utilisateurs qui ont téléchargé la fausse extension sur le Chrome Web Store

entre le 14 février et le 22 mars. Il est donc important de vérifier l’authenticité de l’extension en allant sur le Chrome Web Store. Les utilisateurs devraient également installer un logiciel antivirus et envisager d’installer un bloqueur de publicités pour éviter les arnaques et les attaques ciblées.

Source : www.lemondeinformatique.fr

→ Accéder à CHAT GPT en cliquant dessus