

La création d'un malware dangereux avec l'aide de ChatGPT

Un chercheur utilise ChatGPT pour créer un malware sophistiqué sur PC

Introduction

Un chercheur a réussi à utiliser ChatGPT pour créer un malware sophistiqué sur PC. Cette réalisation soulève des inquiétudes quant à l'utilisation mal intentionnée de l'intelligence artificielle.

L'utilisation de ChatGPT pour créer un malware

OpenAI a prévu des garde-fous pour éviter que ChatGPT ne soit utilisé à des fins malveillantes. Cependant, Aaron Mulgrew, chercheur de Forcepoint, a pu contourner ces protections afin de créer facilement un logiciel malveillant. Il a fait en sorte que l'IA écrive séparément des lignes de code qu'il a ensuite compilées pour concevoir un logiciel fonctionnel. Ce processus permet aux personnes mal intentionnées d'utiliser un stratagème similaire.

Description du malware créé par Aaron Mulgrew

Le malware créé par le chercheur se déguise sous les traits d'un économiseur d'écran qui s'exécute automatiquement sur Windows. Le logiciel malveillant peut extraire des données potentiellement sensibles de l'ordinateur pour être transférées dans un dossier Google Drive. Aaron Mulgrew explique qu'il a même pu affiner son logiciel à l'aide de ChatGPT pour rendre le code plus efficace encore. Au point de pouvoir soumettre le malware aux tests de VirusTotal sans être détecté.

Sensibiliser les acteurs du marché

Le chercheur a réalisé cette expérience pour sensibiliser les acteurs du marché à faire preuve de vigilance face à l'utilisation malveillante de l'intelligence artificielle. Il est important de rappeler que les systèmes de sécurité ne sont pas infaillibles et que les cybercriminels peuvent trouver des moyens de les contourner.

Conclusion

La création d'un malware sophistiqué à l'aide de ChatGPT soulève des inquiétudes quant à l'utilisation malveillante de l'intelligence artificielle. Les acteurs du marché doivent être vigilants et prendre les mesures nécessaires pour protéger les utilisateurs contre les cyberattaques.

Source : www.frandroid.com

→□ Accéder à CHAT GPT en cliquant dessus