ChatGPT Contraint de Concevoir un Maliciel Impénétrable

Titre : Un chercheur de Forcepoint réussit à concevoir un exploit zero day en utilisant ChatGPT

Aaron Mulgrew, chercheur en sécurité chez Forcepoint, a réussi à générer un exploit zero day avancé en utilisant uniquement le chatbot ChatGPT d'OpenAI. Il a montré la facilité avec laquelle les garde-fous de ChatGPT peuvent être contournés, et comment des malwares avancés peuvent être créés sans écrire de code en utilisant la technique de stéganographie.

Technique de stéganographie

La stéganographie est une technique ancienne qui consiste à cacher une donnée que l'on souhaite rendre inaccessible à l'intérieur d'une donnée accessible mais inutile. Contrairement au chiffrement, la stéganographie ne rend pas l'accès impossible, mais le camoufle.

La création de l'exploit zero day

Pour créer son malware via ChatGPT, Aaron Mulgrew a d'abord demandé à l'IA de générer un code pour rechercher un PNG de plus de 5 Mo sur le disque local, puis de coder ce fichier avec de la stéganographie. Ensuite, il a utilisé une série de requêtes pour faire en sorte que ChatGPT génère un code supplémentaire pour trouver des documents Word et PDF sur le disque local, diviser les fichiers de plus de 1 Mo en petits morceaux, et créer un fichier d'économiseur d'écran contenant l'exécutable malveillant.

L’attaque initiale

Pour faire passer son malware inaperçu, Aaron Mulgrew a demandé à ChatGPT de protéger la propriété intellectuelle du code en produisant un exemple de code qui cachait les noms de variables et suggérait des modules Go pertinents pour générer un code entièrement masqué. Le malware a été ensuite téléchargé sur Google Drive, car l’ensemble du domaine Google est généralement autorisé dans la plupart des réseaux d’entreprise.

L’absence de contre-mesure

Les outils existants qui surveillent le trafic réseau ne sont pas en mesure de détecter les manipulations de la stéganographie, car les seuls documents qui traversent la frontière sont des images. Il est donc peu probable que les outils actuels des entreprises permettent de bloquer le trafic de téléchargement d’images vers le domaine Google. Les RSSI doivent donc former les employés aux risques cyber, mettre à jour constamment les logiciels et mettre en place un contrôle d’accès.

Conclusion

L’exploit zero day créé par Aaron Mulgrew a mis en évidence la facilité avec laquelle ChatGPT peut être utilisé pour créer des malwares avancés sans écrire de code. Les RSSI doivent mettre en place des contre-mesures, mais aucune solution n’est infaillible face à cette technique sophistiquée.

Source : www.lemondeinformatique.fr

Quel est l’impact de cette tendance sur le secteur du marketing ?

Résumé détaillé en 600 mots maximum : L’outil ChatGPT développé par OpenAI au crépuscule de l’année 2022 va bouleverser la manière dont travaillent communicants et marketeurs. Bien que suscitant un engouement planétaire, la technologie reste à l’aube de son déploiement dans les stratégies marketing. Forrester a mené une enquête montrant comment les CMO envisagent d’intégrer ChatGPT dans leurs stratégies marketing, montrant qu’un petit pourcentage d’entreprises ont commencé à explorer son potentiel, avec seulement une minorité l’utilisant concrètement. Cet outil permet de gagner du temps grâce à l’automatisation d’un certain nombre de tâches, mais sa qualité n’est pas encore au même niveau que ce qu’un humain peut réaliser. L’outil pourra devenir une sorte d’assistant, mais il ne remplacera pas les professionnels, et ChatGPT va créer des nouveaux jobs et faire évoluer la manière dont nous travaillons. Les opportunités offertes par l’outil restent limitées, comme le fait que ChatGPT est aujourd’hui incapable d’exploiter les autres bases de données que la sienne. L’adaptation aux nouveaux usages liés à l’apparition de ce générateur de texte sera indispensable, il faudra à n’en pas douter une certaine formation pour les équipes marketing. Certaines places

risquent, tout de même, de ne plus être nécessaires, mais l'outil va ainsi débarrasser le marché des usurpateurs qui ne font rien d'autre que des commentaires de tableaux et de reporting, sans pousser l'analyse plus loin.

Source : e-marketing.fr

→□ Accéder à CHAT GPT en cliquant dessus

TEST GPT-4 : LA DÉMO COMPLÈTE EN FRANÇAIS □□ (il lit VRAIMENT les images □)

GPT-4 : une nouvelle fonctionnalité pour les abonnés premium de Chat Gipiti

GPT-4 est enfin disponible pour les abonnés premium de Chat Gipiti. Cette nouvelle fonctionnalité permet de comprendre et interpréter tout ce qu'on lui raconte avec une précision de 4 sur 5. Dans cet article, nous allons tester ensemble différentes fonctionnalités de GPT-4.

Accéder à GPT-4 sur Chat Gipiti

Pour accéder à GPT-4 sur Chat Gipiti, il suffit d'aller dans

“Modèle” et d’activer l’option GPT-4. Le graphique présentant les avantages et inconvénients de GPT-4 indique que la vitesse de sur 5 est l’inconvénient majeur.

Test de GPT-4 avec un prompte

Nous avons testé GPT-4 en créant un prompte lui demandant de proposer des solutions pour sauver le régime des retraites en France. Nous avons demandé à ce qu’il mette cela dans un tableau avec les avantages et inconvénients de chaque solution. GPT-4 a proposé des solutions intéressantes et précises bien qu’il y ait un petit problème de construction du tableau.

GPT-4 peut traiter 25000 mots

Nous avons également constaté que GPT-4 est capable de traiter des documents PDF de plus de 200 pages. Pour tester cette fonctionnalité, nous avons demandé à GPT-4 de nous faire un résumé en français du rapport complet du GIEC en PDF. GPT-4 a réussi à en faire la synthèse en quelques instants.

GPT-4 peut interpréter des images

Dans la vidéo de présentation de GPT-4, nous apprenons qu’il est capable de comprendre une image et d’interpréter celle-ci pour répondre à nos questions. Pour tester cette fonctionnalité, nous avons demandé à GPT-4 de nous proposer trois recettes de repas avec des ingrédients présents sur une image que nous avons trouvé sur Google Images. GPT-4 a réussi à répondre à notre demande avec brio.

Conclusion

GPT-4 est une nouvelle fonctionnalité intéressante pour les abonnés premium de Chat Gipiti. Avec GPT-4, il est possible de comprendre et interpréter tout ce qu’on lui raconte avec une précision intéressante. Cette nouvelle fonctionnalité permet également de traiter des documents volumineux et de comprendre

des images. Avec GPT-4, les abonnés premium de Chat Gipiti peuvent se lancer dans de nouveaux projets.

Source : Ludo Salenne | Date : 2023-03-15 12:00:31 | Durée : 00:16:00

➡ Accéder à CHAT GPT en cliquant dessus

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 malintentionnée 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