Est-il possible d’utiliser ChatGPT pour créer du code malveillant ?

ChatGPT n’est pas l’outil parfait pour écrire du code malveillant

Depuis son lancement cet hiver, ChatGPT, la formidable intelligence artificielle conversationnelle d’OpenAI, a suscité énormément d’enthousiasme. Cependant, cet enthousiasme était parfois trop grand, ce qui a conduit les chercheurs de Check Point à s’inquiéter des expérimentations de cybercriminels menées avec le chatbot. Leur crainte ? Que ChatGPT devienne l’outil qui permettrait d’ouvrir la programmation de logiciels malveillants à un public plus large et moins qualifié.

Heureusement, le célèbre chercheur en sécurité Marcus Hutchins a récemment démenti ses craintes dans un post de blog. Il a débuté dans la programmation de logiciels malveillants avant de revenir dans le droit chemin, et est devenu un héros mondial après avoir stoppé le terrible malware autorépliquant WannaCry.

ChatGPT est limité par le nombre de caractères

Selon Marcus Hutchins, ChatGPT est loin d’être capable de

créer un logiciel malveillant entièrement fonctionnel. Si vous lui demandez de générer un extrait de code Python pour charger une page web, il peut le faire. Mais plus vous ajoutez de paramètres, plus cela devient confus. La limitation du nombre de caractères dans la boîte de dialogue empêche de saisir suffisamment de données pour générer quelque chose qui irait au-delà d'extraits que l'on peut déjà trouver sur le moteur de recherche Google. Et un néophyte aurait dû mal à identifier les erreurs de code écrites par le chatbot. Ce qui veut dire qu'il ne sera vraisemblablement pas l'outil adéquat pour démocratiser la programmation de programmes malveillants.

La programmation informatique implique plus que de l'écriture de code

Selon Marcus Hutchins, ce malentendu à propos de la programmation informatique est nourri par un malentendu plus général. Il ne s'agit pas seulement d'écrire du code, mais d'abord de comprendre comment arriver à un but que l'on s'est fixé. Bref, ce ne sont pas seulement des lignes qui se succèdent, mais aussi une architecture à imaginer. De plus, à propos de la génération d'e-mails d'hameçonnage, le jeune anglais ironise en rappelant que Google a déjà lancé il y a sept ans un service d'intelligence artificielle sophistiqué avec son célèbre traducteur en ligne.

Ainsi, pour Marcus Hutchins, l'intelligence artificielle conversationnelle ne peut pas offrir de perspectives aux cybercriminels. Ecrire des e-mails de hameçonnage n'a jamais été difficile et ne nécessite pas d'intelligence artificielle. En effet, ces derniers peuvent être construits très simplement en copiant le code HTML d'un message authentique. Pas besoin d'un chatbot pour faire un copier-coller.

Ainsi, bien que ChatGPT soit une formidable intelligence

artificielle conversationnelle, elle n’est pas l’outil parfait pour écrire du code malveillant. Elle est limitée par le nombre de caractères et ne peut pas offrir de perspectives aux cybercriminels. La programmation informatique implique plus que de l’écriture de code et ne nécessite pas d’intelligence artificielle. Les e-mails de hameçonnage peuvent être construits très simplement en copiant le code HTML d’un message authentique.

Source : www.zdnet.fr

→ Accéder à CHAT GPT en cliquant dessus