Les implications potentielles de ChatGPT et GPT-4 dans la propagation de la cybercriminalité

Comment l'IA générative pourrait augmenter le nombre de cyberattaques

Selon les chercheurs de Nord VPN, le nombre de messages sur le dark web expliquant la manière de manipuler ChatGPT, l'un des grands modèles de langage d'intelligence artificielle d'OpenAI, est passé de 120 en janvier à 870 en février, soit une augmentation de 625%. Cette hausse montre l'intérêt grandissant de hackers pour ces nouveaux outils d'IA générative.

Les outils d'IA générative comme ChatGPT et GPT-4 permettent de démultiplier le nombre de cyberattaques, avertit Sam Altman, le PDG d'OpenAI sur la chaîne américaine ABC News. Les personnes mal intentionnées ayant acquis des connaissances approfondies de ces technologies pourraient les utiliser pour concevoir des codes informatiques pour des cyberattaques.

L'apprentissage automatique (Machine Learning ou ML) basé sur l'IA générative change le paysage de la cybersécurité. Il y a un potentiel de création tendancieux en utilisant des outils comme l'IAT de Tesla, qui peut apprendre à tromper des réseaux de surveillance en lignes droites.

Les entreprises doivent être conscientes des menaces potentielles des outils d'IA générative et des moyens de s'en protéger. Les planificateurs de cybersécurité peuvent s'attendre à ce que les attaquants utilisent des techniques de

ML pour cibler des victimes spécifiques et concevoir des attaques sophistiquées.

Les experts conseillent que pour contrer les futures attaques orientées vers l'IA, les entreprises doivent commencer à collecter autant de données qu'elles le peuvent sur les menaces, les échantillons de logiciels malveillants et les attaques connues. Les données volumineuses en temps réel peuvent également permettre de déduire les comportements malveillants.

Les analystes peuvent également utiliser les techniques d'apprentissage automatique pour analyser les tendances, notamment en fournissant des indicateurs de compromission en temps réel. Les systèmes d'apprentissage automatique peuvent offrir des résultats en temps réel qui peuvent garantir que les équipes de sécurité peuvent répondre rapidement aux menaces.

Enfin, les entreprises doivent investir dans des capacités de pivotement dynamique. Au lieu d'être contraintes par la sécurité statique, où les systèmes sont uniquement conçus pour attraper les menaces connues et identifiées, les entreprises doivent concevoir un cyberenvironnement capable de détecter et de répondre rapidement aux menaces inconnues.

En résumé, l'IA générative peut être utilisée pour augmenter le nombre de cyberattaques. Les entreprises doivent être conscientes de la menace et prendre des mesures préventives pour se protéger. Les outils d'apprentissage automatique peuvent aider à analyser les tendances et les comportements malveillants en temps réel pour garantir une réponse rapide aux menaces.

Source : www.lefigaro.fr

→ Accéder à CHAT GPT en cliquant dessus