

Les pirates de la Russie, la Chine, l'Iran et la Corée du Nord utilisent ChatGPT : le côté obscur de l'intelligence artificielle

Les pirates utilisent ChatGPT pour leurs attaques

Les pirates utilisent ChatGPT pour leurs attaques

Récemment, Microsoft a divulgué que différents groupes de pirates financés par des gouvernements russes, chinois, iraniens et nord-coréens exploitent l'intelligence artificielle pour mener des attaques à travers ChatGPT.

D'après les spécialistes de Microsoft Threat Intelligence, ces cybercriminels utilisent l'IA générative pour faciliter leurs activités depuis le début de l'année dernière. ChatGPT, un chatbot développé par OpenAI, est utilisé par ces pirates pour repérer les vulnérabilités d'un système, contourner les mécanismes de défense des antivirus et organiser des attaques de hameçonnage. Pour ces pirates, ChatGPT est un "outil de productivité" qui leur permet de perfectionner et d'améliorer leurs attaques.

Les pirates utilisent des modèles de langage pour collecter des informations sur leurs cibles, obtenir de l'assistance

dans la programmation de logiciels malveillants et surmonter la barrière de la langue lors de leurs communications avec des victimes dans une langue étrangère. Ils peuvent ainsi rédiger des messages persuasifs sans être trahis par une syntaxe ou une orthographe approximative.

Le rapport de Microsoft détaille quels groupes de pirates se servent de ChatGPT pour perfectionner leurs stratégies. Parmi eux, on retrouve Forest Blizzard, un groupe de pirates russes plus connu sous le nom de Fancy Bear, spécialisés dans l'espionnage et mandatés par le Kremlin. Ils ont notamment piraté le Comité National Démocrate (DNC) des États-Unis lors de l'élection présidentielle de 2016.

Les cybercriminels russes ont apparemment utilisé l'IA pour mener des recherches sur "diverses technologies de satellite et de radar". Ils ont également réclamé l'aide de ChatGPT pour rédiger des scripts et automatiser certaines opérations

Les pirates nord-coréens d'Emerald Sleet ont également été observés en train d'utiliser ChatGPT pour mieux comprendre les vulnérabilités signalées publiquement et pour composer des messages de hameçonnage. Les pirates iraniens de Crimson Sandstorm exploitent aussi ChatGPT pour générer des courriels d'hameçonnage conçus pour piéger les féministes, sur demande de l'Iran.

Les pirates chinois des groupes Charcoal Typhoon et Salmon Typhoon ont fait appel au chatbot pour comprendre des technologies, générer et affiner des scripts ainsi que pour obtenir des traductions.

Face à ces utilisations malveillantes, OpenAI a pris des mesures pour empêcher les cybercriminels de dialoguer avec ChatGPT. La start-up a désactivé les comptes ChatGPT utilisés par les groupes de pirates. Microsoft a également agi pour perturber les actifs associés aux pirates.

Pour rester informé des dernières actualités, suivez-nous sur

Google Actualités et WhatsApp.

Source : Microsoft