Les dessous inédits de WormGPT, la contre-attaque des cybercriminels contre ChatGPT

Intelligence artificielle : la menace des outils malveillants

Intelligence artificielle : la menace des outils malveillants

Le célèbre agent conversationnel d’intelligence artificielle ChatGPT a trouvé son imitation malveillante en WormGPT. Découvert et dévoilé par les chercheurs en cybersécurité de la société SlashNext, WormGPT est présentement disponible sur un forum de pirates informatiques. Présenté comme une “alternative” noire à ChatGPT, WormGPT est un outil basé sur le modèle de langage GPTJ. Il a été entraîné à l’aide de sources de données comprenant notamment des informations sur les logiciels malveillants.

Sans limites éthiques

WormGPT est décrit comme une version de ChatGPT sans aucune restriction éthique. Contrairement à ChatGPT, développé par OpenAI, WormGPT ne refuse pas la création de logiciels malveillants. Les chercheurs de SlashNext ont observé que ce nouvel outil était capable de générer un courrier électronique persuasif visant à tromper un gestionnaire de compte et le pousser à effectuer un paiement frauduleux. L'équipe a été impressionnée par l'efficacité et la stratégie du modèle de langage de WormGPT.

Un abonnement allant de 60 à 700 dollars pour les cybercriminels

Sur un canal Telegram dédié à la promotion de WormGPT, les messages consultés par ZDNet révèlent que le développeur prévoit de proposer un modèle d'abonnement avec un accès compris entre 60 et 700 dollars. Un membre du canal, "darkstux", affirme déjà compter plus de 1 500 utilisateurs de WormGPT.

Il est clair que WormGPT n'est que le premier d'une nouvelle génération d'outils malveillants. Là où l'argent peut être gagné, les cybercriminels s'empresseront de tirer parti de ces outils. Les modèles de langage naturel tels que WormGPT sont susceptibles de transformer les escroqueries d'hameçonnage, souvent faciles à repérer, en opérations sophistiquées et très réussies.

Un nouveau défi pour les forces de

police

Dans un rapport précédent, l’agence de police européenne Europol a souligné la nécessité de surveiller le développement de ces modèles de langage naturel. Europol estime en effet que ces outils constituent un nouveau défi pour les forces de l’ordre, car ils facilitent grandement les activités criminelles en permettant à des acteurs malveillants de les perpétrer sans nécessiter de connaissances préalables spécifiques. De plus, ChatGPT lui-même peut être détourné de son usage initial et utilisé à des fins illégales, notamment pour rédiger des courriers professionnels, des lettres de motivation ou des bons de commande, en éliminant les éléments typiques d’un courrier d’hameçonnage tels que les fautes d’orthographe et les problèmes de grammaire.

Source : “ZDNet.com”