WormGPT, nouvelle arme des cyberattaquants pour vous piéger

Dans le cadre de l'opération « Tribune d'été », organisée par la rédaction de Maddyness, nous nous sommes rapprochés de celles et ceux qui ouvrent une fenêtre sur le futur des entreprises et de la société. Tribune proposée par Achraf Hamid, Data Scientist chez Mailinblack, sur WormGPT.

Temps de lecture : minute

4 août 2023

Avec plus de 3,4 milliards de courriels indésirables envoyés quotidiennement dans le monde, le phishing est aujourd'hui la forme la plus courante de cybercriminalité. Cette technique, qui vise à obtenir des renseignements personnels dans le but de perpétrer une usurpation d'identité, pourrait bien devenir encore plus difficile à gérer pour les professionnels de la sécurité informatique.

En effet, quelques mois après la mise sur le marché d'intelligences artificielles génératives telles que ChatGPT ou Midjourney, une solution malveillante basée sur le même type de technologie a été découverte le 13 juillet 2023. Elle est capable de créer des campagnes de phishing à grande échelle en quelques minutes. Baptisée WormGPT, elle fait peser le risque d'un changement d'échelle à un type de cyberattaque déjà problématique.

IA générative : un potentiel exploité par des

développeurs malveillants

L'évolution rapide des cyberattaques nous amène à faire face à de nouvelles menaces dont l'une des plus inquiétantes est WormGPT. Développé récemment par des hackers et basé sur des pratiques de black-hat (hacker mal intentionné), ce nouvel outil excelle particulièrement dans les attaques d'ingénierie sociale sophistiquées à travers la rédaction de Business Email Compromise (BEC). Également connue sous le nom de fraude du président, cette arnaque vise les entreprises en se faisant passer pour des cadres supérieurs ou des partenaires de confiance pour les convaincre de dévoiler des informations confidentielles ou d'effectuer des paiements vers un compte bancaire (celui de l'usurpateur).

Selon des experts en sécurité numérique de Symantec, la fraude au président cible au minimum 400 entreprises par jour, et d'après Threat Intelligence, 22 % des PDG seraient visés par ces attaques.

WormGPT, en tant que puissant outil d'IA générative, pose des défis majeurs en matière de cybersécurité. Peu de temps après son lancement, il a déjà rassemblé une communauté de plus de 9.500 abonnés sur le réseau social Telegram, composée d'acteurs potentiellement menaçants qui utilisent cet outil pour des attaques réelles.

Cette IA fait le bonheur des hackeurs moins expérimentés qui peuvent désormais mener des attaques sophistiquées, élargissant ainsi la menace cybercriminelle. À peine une semaine après son lancement, les membres payants de WormGPT sont estimés à 1.500 membres.

Une technologie sans éthique ni frontière

WormGPT a été créé à partir d'une IA générative créée sans contraintes morales ni éthiques, dépourvue de barrières de sécurité, et capable de

répondre à toute demande malveillante. En effet, cette IA a été entraînée sur des logiciels malveillants et des emails de phishing, ce qui lui permet de créer des virus et d'écrire automatiquement des emails de phishing convaincants et personnalisés. Cette version fonctionne sur un modèle GPT-J, publié par EleutherAI en 2021, et possède une capacité de 6 milliards de paramètres et une taille de vocabulaire de 50.257 jetons, similaire à GPT-2 d'OpenAI.

La face cachée de l'iceberg : avant même l'apparition de cette dangereuse révolution, les cybercriminels utilisaient déjà de nombreux outils pour tromper les gens. Avec WormGPT cette menace atteint un niveau inédit jusqu'ici. Désormais, même un hacker débutant peut solliciter cette IA pour créer un logiciel malveillant capable de scanner le réseau d'une organisation à la recherche de vulnérabilités potentielles. Ensuite, il peut utiliser cet outil pour créer le code nécessaire pour exploiter les failles détectées. Une fois à l'intérieur du réseau, le hacker peut choisir d'espionner les échanges internes par email, en récupérant des messages rédigés par le PDG pour les soumettre à l'IA malveillante. Cette dernière serait alors capable de rédiger un email de fraude, imitant le style d'écriture du dirigeant propre (vocabulaire, syntaxe et structure des phrases, ponctuation, …), demandant au comptable d'effectuer un virement vers un fournisseur en utilisant un compte bancaire détourné.

Face à cette menace grandissante, la cybersécurité doit continuer à évoluer et à s'adapter rapidement. La vigilance et l'investissement dans des solutions de protection robustes et l’éducation aux bonnes pratiques cyber et aux risques encourus restent essentiels pour faire face à cette nouvelle ère de cybercriminalité alimentée par des outils d'IA générative tels que WormGPT. En restant informés sur ces développements et en agissant de manière proactive, nous pourrons mieux protéger nos entreprises et nos données sensibles des menaces cybercriminelles avancées de demain.

MADDYNEWS

La newsletter qu'il vous faut pour ne rien rater de l'actualité des startups françaises !

JE M’INSCRIS

Article écrit par Achraf Hamid