***ChatGPT : Un outil de cybercriminalitÃ©.?***
**Logiciel**
PostÃ© par : JulieM
PubliÃ©e le : 30/1/2023 13:00:00

Lâagent conversationnel ChatGPT dâOpenAI fait couler beaucoup dâencre depuis plusieurs semaines. Cet outil fascine autant quâil inquiÃ¨te, et pose des dÃ©fis susceptibles de rÃ©volutionner lâactivitÃ© cybercriminelle.

Dirk Schrader, Resident CISO (EMEA) and VP of Security Research chez Netwrix, fait le commentaire suivant :

Â« Les cybercriminels tireront certainement profit du ChatGPT d'OpenAI. Tout d'abord, l'utilisation de cet outil augmentera leur efficacitÃ© et leur crÃ©dibilitÃ© lors de l'exÃ©cution de campagnes de phishing ciblÃ©es ou vastes.

Ces activitÃ©s reposent en effet sur le langage. Jusqu'Ã aujourd'hui, la plupart des emails de phishing Ã©taient souvent mal traduits et maladroits sur le plan grammatical, et donc gÃ©nÃ©ralement faciles Ã repÃ©rer.

L'utilisation de ChatGPT va changer la situation car il est capable de crÃ©er des textes bien formulÃ©s et corrects dans de nombreuses langues. Il sera donc plus difficile pour l'utilisateur final de distinguer le phishing du message lÃ©gitime. Les formations de sensibilisation des employÃ©s devront par consÃ©quent Ãªtre modifiÃ©es pour tenir compte de cette menace.

Il existe Ã©galement un Ã©lÃ©ment spÃ©cifique aux campagnes de phishing, soit dâhameÃ§onnage ciblÃ©. Il sera ainsi plus facile pour les APT (Advanced Persistant Threat) de crÃ©er un Ã©cosystÃ¨me complet pour celles-ci.

Des emails et des pages de renvoi, crÃ©Ã©s dans la langue de la victime et avec un contenu de qualitÃ©, inciteront des cibles ayant accÃ¨s Ã des donnÃ©es sensibles Ã faire preuve dâune mauvaise cyber-hygiÃ¨ne : tÃ©lÃ©charger un fichier malveillant ou encore partager ses identifiants, par exemple.

Pour se prÃ©parer Ã ce type d'attaque assistÃ©e par l'IA, les organisations doivent accorder une plus grande attention Ã la sÃ©curisation des identitÃ©s de leurs utilisateurs.

Il est essentiel de renforcer la posture de chaque compte ordinaire et Ã privilÃ¨ges, en mettant en Åuvre une approche de zÃ©ro privilÃ¨ge permanent, les droits dâaccÃ¨s nâÃ©tant garanti que si et quand ils sont nÃ©cessaires.

DeuxiÃ¨mement, si nous examinons le fonctionnement interne d'un groupe APT typique, il est possible de supposer d'autres faÃ§ons dont ChatGPT peut influencer leurs opÃ©rations.

La crÃ©ation, la transformation et la variation du code sont certainement le domaine oÃ¹ ChatGPT est un outil bienvenu. Il peut Ãªtre utilisÃ© pour Ã©crire certains modules du code ou lorsquâune rÃ©Ã©criture est nÃ©cessaire ; par exemple, pour changer les valeurs de hachage, afin d'Ã©viter une dÃ©tection facile par des outils dÃ©fensifs comme Virustotal.

Une autre compÃ©tence notable est la capacitÃ© de ChatGPT Ã transformer un langage de programmation ou de script en un autre. Cela permet de raccourcir le cycle de dÃ©veloppement

pour les groupes spÃ©cialisÃ©s en ransomware, tout en augmentant  leur base de code et leur facilitÃ© d'utilisation sur plusieurs plateformes.

Les langages de script pourraient Ãªtre le premier point de mire ici, car les  attaques qui utilisent, par exemple, Powershell, nÃ©cessitent des connaissances  particuliÃ¨res et doivent Ãªtre rÃ©inventÃ©es frÃ©quemment pour Ã©viter d'Ãªtre  dÃ©tectÃ©es.

 De plus, ChatGPT va s'amÃ©liorer grÃ¢ce Ã  ses capacitÃ©s d'apprentissage. Il est potentiellement capable de crÃ©er des extraits de code de logiciels malveillants  et de ransomwares accessibles aux cybercriminels dotÃ©s dâ□□une expÃ©rience moindre.  C'est une menace Ã  venir Ã  prendre Ã©galement en compte. Â»