ChatGPT : le nouvel alliÃ© des cybercriminels dÃ©butants
SÃ©curitÃ©
PostÃ© par : JerryG
PubliÃ©e le : 18/1/2023 14:00:00

ChatGPT est rapidement devenu un outil incontournable, dÃ©passant la barre du million dâutilisateurs aprÃ¨s tout juste quelques semaines dâexistence. Mais il prÃ©sente Ã©galement certains risques pour les utilisateurs et les entreprises.

Il est en effet trÃ¨s facile de divulguer, de faÃ§on accidentelle, des informations personnelles ou professionnelles en rÃ©digeant des questions Ã lâattention de lâintelligence artificielle (IA), ce qui peut entraÃ®ner une fuite de donnÃ©es et un rÃ©el prÃ©judice pour les entreprises.

Selon Gustavo Palazolo, threat research engineer chez Netskope, ChatGPT faciliterait aussi la tÃ¢che des cybercriminels dans lâÃ©laboration de leurs attaques pour crÃ©er des logiciels malveillants ou des Ã©lÃ©ments de code nÃ©fastes :

Â« Cette IA pourrait en effet rÃ©diger des emails de phishing plus convaincants, mettre en Åuvre des attaques dâingÃ©nierie sociale davantage persuasives, dialoguer avec leurs victimes afin de les inciter Ã divulguer des informations sensibles, voire rÃ©diger du code malveillant sans disposer de compÃ©tences avancÃ©es. Tous ces aspects permettent en outre des attaques plus efficaces et menÃ©es Ã plus grande Ã©chelle.

Il est ainsi courant pour les hackers, surtout dÃ©butants, de rÃ©utiliser du code Open Source ou ayant fait lâobjet dâune fuite dans leurs logiciels malveillants.

Avec ChatGPT, les pirates moins expÃ©rimentÃ©s peuvent exploiter le moteur de lâIA pour gÃ©nÃ©rer ces Ã©lÃ©ments de code, mais aussi pour mieux comprendre leur fonctionnement, ou encore sÃ©lectionner lâoutil le mieux adaptÃ© Ã leurs visÃ©es.

En plus dâÃªtre capable dâexpliquer le fonctionnement de diffÃ©rentes techniques malveillantes, cette IA gÃ©nÃ¨re Ã©galement des exemples de code presque parfaits, Ã lâaide du langage de programmation C++, pour effectuer une sÃ©rie de tÃ¢ches susceptibles dâaider les hackers ; telle que lâinjection de processus, la dÃ©tection de machines virtuelles et mÃªme le chiffrement de fichiers pouvant Ãªtre utilisÃ© lors dâattaques de ransomware.

Les entreprises et les utilisateurs individuels doivent donc se protÃ©ger : les attaques dâingÃ©nierie sociale constituent un risque Ã©levÃ© et persistant pour les entreprises (avec ou sans recours Ã lâIA) et ont augmentÃ© depuis le dÃ©but de la pandÃ©mie de Covid.

Une majoritÃ© des salariÃ©s pratiquent encore le tÃ©lÃ©travail, et ils se mÃ©fient bien moins quâavant des solutions numÃ©riques tout en adoptant en masse des outils de collaboration Ã distance. Lâexistence dâun outil dâIA capable dâimiter notre comportement rend ce risque encore plus grand.

Les entreprises doivent donc impÃ©rativement recrÃ©er un "pare-feu humain" en formant leurs employÃ©s et clients Ã repÃ©rer les indices de fraude, et Ã vÃ©rifier systÃ©matiquement lâidentitÃ© de leur interlocuteur.

Cependant, les nouveaux vecteurs dâattaque susceptibles dâÃªtre dÃ©veloppÃ©s grÃ¢ce Ã lâIA peuvent en grande partie Ãªtre contrÃ©s en optimisant la stratÃ©gie de sÃ©curitÃ©. Cela

demande notamment de maintenir les logiciels Ã jour, dâ□□appliquer tous les correctifs, de veiller Ã lâ□□adoption de politiques et de technologies efficaces pour la protection des donnÃ©es et, enfin, de protÃ©ger Ã©troitement les atouts les plus prÃ©cieux dâ□□une entreprise.

Finalement, les risques associÃ©s Ã cette IA ne sont pas exagÃ©rÃ©s. Les hackers peuvent en effet dÃ©tourner ChatGPT de nombreuses maniÃ¨res diffÃ©rentes pour se faciliter la tÃ¢che. Mais force est de reconnaÃ®tre que lâ□□IA nâ□□est pas exclusivement une arme au service des cybercriminels.

Elle constitue Ã©galement un outil prÃ©cieux pour repÃ©rer les vulnÃ©rabilitÃ©s dans du code, ou pour Ã©valuer une posture de sÃ©curitÃ© et identifier comment amÃ©liorer les dÃ©fenses dâ□□une entreprise. Â»