ChatGPT et cybersÃ©curitÃ© : quels risques pour les entreprises ?
SÃ©curitÃ©
PostÃ© par : JulieM
PubliÃ©e le : 27/2/2023 13:00:00

Les plateformes de gÃ©nÃ©ration de texte tel que ChatGPT permettent de crÃ©er du contenu de qualitÃ©, instantanÃ©ment, gratuitement, et sur nâ□□importe quel sujet. Comme le confirme le lancement de Bard par Google, nous sommes dÃ©sormais entrÃ©s dans une course Ã lâ□□IA, ou chaque gÃ©ant du web cherche Ã possÃ©der la meilleure solution possible.

Si lâ□□avancÃ©e technologique est majeure, le risque notamment pour la cybersÃ©curitÃ© des entreprises est indÃ©niable. Comment lutter contre des campagnes de phishing de plus en plus ciblÃ©es et sophistiquÃ©es, maintenant alimentÃ©es par des technologies capables de parfaire encore plus la forme et la teneur dâ□□un email malveillantâ□□?

En quelques mots, ChatGPT offre une ingÃ©nierie sociale trÃ¨s performante, mais une automatisation encore limitÃ©e. Concernant la dÃ©tection de la menace par ranÃ§ongiciels, comme lâ□□explique LoÃ¯c GuÃ©zo, Directeur de la stratÃ©gie CybersÃ©curitÃ© chez Proofpoint, Â« Bien que les chatbots puissent gÃ©nÃ©rer du texte pour le corps dâ□□un email de phishing, ce nâ□□est quâ□□une partie de la menace.

Les en-tÃªtes, les expÃ©diteurs, les piÃ¨ces jointes et les URL font partie des nombreux autres indicateurs de menace pris en considÃ©ration. ChatGPT ne change pas la donne pour les attaques de spear-phishing plus ciblÃ©es puisque celles-ci sont de par leur nature trÃ¨s personnalisÃ©s, avec une ingÃ©nierie sociale trÃ¨s poussÃ©e. Â»

Pour rÃ©ussir, Â« les acteurs de la menace doivent constamment faire pivoter des aspects plus subalternes, ce que ChatGPT ne peut pas faire, comme enregistrer des domaines et dÃ©placer des Ã©lÃ©ments, autrement leurs tentatives dâ□□attaques seront constamment dÃ©tectÃ©es et neutralisÃ©es par des Ã©quipes de chercheurs comme la Threat Team de Proofpoint. Â»

Au-delÃ de la crÃ©ation de contenu, LoÃ¯c GuÃ©zo prÃ©cise que Â« les Ã©diteurs de logiciels malveillants doivent Ã©galement, non seulement diffuser leurs logiciels malveillants, mais aussi en vendre lâ□□accÃ¨s. ChatGPT nâ□□aide pas Ã automatiser les composants les plus importants de ces opÃ©rations.

Cela ne veut pas dire pour autant que ces capacitÃ©s nâ□□Ã©volueront pas; de toute Ã©vidence, cette technologie progresse trÃ¨s rapidement sur lâ□□ensemble de donnÃ©es sur lequel lâ□□outil a Ã©tÃ© formÃ©, mais il nâ□□en est pas lÃ aujourdâ□□hui. Â»