الخليج

اقتصاد, تقنية وسيارات

26 يناير 2023 15:48 مساء

في تهديد الأمن الإلكتروني؟ «ChatGPT» هل يستخدم

نظرت «كاسبرسكي» في الطرق التي يمكن أن يؤثر عبرها استخدام العامّة لتطبيق الذكاء الاصطناعي الشهير في القواعد المعمول بها في عالم الأمن الرقمي. وتأتي هذه الخطوة بعد بضعة أشهر فقط من طرح شركة ChatGPT بوصفه أحد أقوى نماذج الذكاء الاصطناعي البرمجية المبتكرة «ChatGPT3» للتطبيق OpenAI ««أوبن إيه آي حتى الآن. وبإمكان التطبيق الجديد شرح المفاهيم العلمية المعقدة بطريقة أفضل مما يفعل العديد من المعلمين، كما يستطيع، بناء على طلب المستخدم، تأليف المقطوعات الموسيقية وإنشاء النصوص، أياً كانت تقريباً.

في الأساس نموذجاً لغوياً قائماً على الذكاء الاصطناعي، يستطيع إنشاء نصوص مقنعة يصعب «ChatGPT-3» ويُعدّ تمييزها عن تلك التي يكتبها البشر، ما جعله يلفت انتباه مجرمي الإنترنت الذين يحاولون تطبيق هذه التقنية على تأليف النصوص المستخدمة في هجمات التصيّد الموجه، بعد أن كانت كتابة كل بريد إلكتروني موجّه في السابق أمراً مكلفاً مهيّأ لإحداث تغيير «ChatGPT» جداً، الأمر الذي أعاقهم عن إطلاق حملات جماعية للتصيّد الموجه. لكن التطبيق جذري في توازن القوى، نظراً لأنه يسمح للمهاجمين بإنشاء رسائل بريد إلكتروني تصيّدية مقنعة لأنها ستكون مكتوبة بلغة شخصية، حتى وإن كانت سوف تُستخدم على نطاق واسع. وبوسع التطبيق أيضاً إضفاء طابع خاص على أسلوب

صياغة المراسلات، وإنشاء رسائل بريد إلكتروني مزيفة، ولكنها مكتوبة بلغة مقنعة، لدرجة أنها قد تبدو واردة إلى .موظف ما، من أحد زملائه، الأمر الذي يعني أن عدد هجمات التصيّد الناجحة قد يزداد

• رسالة تصيّد أنشئت باستخدام «ChatGPT»

إنشاء شيفرات برمجية، بما فيها الأنواع الخبيثة، لذا سيصبح ChatGPT ووجد العديد من المستخدمين أن بإمكان إنشاء أداة برمجية لسرقة المعلومات أمراً بسيطاً وممكناً، من دون امتلاك أية مهارات برمجية على الإطلاق. ومع ذلك، لن يكون لدى المستخدمين الحذرين بطبعهم ما يخشونه، فالحلول الأمنية التي تستطيع اكتشاف البرمجيات الخبيثة التي يبرمجها الأفراد ستكون قادرة على اكتشاف نظيرتها التي تبرمجها الروبوتات، وتعمل على تحييدها بالسرعة نفسها.
من إنشاء برمجيات خبيثة مصممة بطابع شخصي ChatGPT وبينما أعرب بعض المحللين عن قلقهم من تمكّن لتناسب كل ضحية بنفسه، يرى خبراء كاسبرسكي أن هذه النسخ من البرمجيات ستظلّ تُبدي سلوكاً خبيثاً تتمكّن الحلول الأمنية، على الأرجح، من ملاحظته. ومن المحتمل أيضاً أن تحتوي البرمجيات الخبيثة التي تكتبها الروبوتات على أخطاء دقيقة وعيوب منطقية، ما يعني أن الأتمتة الكاملة لتشفير هذه البرمجيات لم تتحقق بعد.
بالرغم من أنه قد يكون مفيداً ChatGPT ويمكن للقائمين على منظومات الدفاع والحماية الاستفادة من التطبيق لمجرمي الإنترنت؛ إذ يُعتبر قادراً، مثلاً، على «شرح» ما يفعله جزء معين من الشيفرات البرمجية بسرعة، ما يلبي بعض احتياجات مراكز العمليات الأمنية، حيث يتعين على المحللين المنشغلين باستمرار تخصيص حدّ أدنى من الوقت لكل واقعة رقمية، ما يجعلهم يرحبون بأية أداة لتسريع عملهم. ومن المحتمل في المستقبل أن يرى المستخدمون للعديد من لحلّ CTF المنتجات المتخصصة، نموذجاً قائماً على الهندسة العكسية لتحسين فهم الشيفرات البرمجية، ونموذج المشكلات الأمنية، ونموذج البحث عن الثغرات الأمنية، وغيرها.
قد يساعد المهاجمين في مجموعة متنوعة ChatGPT وقال فلاديسلاف توشكانوف الخبير الأمني لدى كاسبرسكي، إن من السيناريوهات، مثل صياغة رسائل بريد إلكتروني للتصيد الموجّه بطريقة مقنعة، بالرغم من أنه لا يؤدّي أي عمل خبيث بالمطلق. وأشار إلى أن هذا التطبيق غير قادر في الوقت الحالي على أن يصبح نوعاً من الذكاء الاصطناعي المختصّ بالقرصنة الذاتية، موضحاً أن الشيفرة الخبيثة التي تنشئها الشبكة العصبية لن تعمل من تلقاء نفسها على الإطلاق، وستظل تتطلب شخصاً متخصصاً ماهراً لتحسينها وتوظيفها.
وأضاف توشكانوف: «قد نرى في السنوات القليلة المقبلة كيف يتم تكييف النماذج اللغوية الكبيرة، المدربة على معالجة اللغات الطبيعية وكتابة الشيفرات البرمجية، للتعامل مع حالات استخدام تخصصية في الأمن الرقمي. ويمكن أن تؤثر هذه التغييرات في مجموعة واسعة من أنشطة الأمن الرقمي، بدءاً من ملاحقة التهديدات وحتى الاستجابة للحوادث.
لذلك، سوف ترغب شركات الأمن الرقمي في التعرّف إلى الاحتمالات التي ستقدمها الأدوات الجديدة، فيما تُدرك كيف .«يمكن لهذه التقنية أن تساعد مجرمي الإنترنت