LITORALPRESS

Fecha: 02-04-2023
Medio: El Mercurio
Supl. : El Mercurio - Cuerpo A
Tipo: Ciencia y Tecnología
Título: El lado oscuro de ChatGPT: expertos alertan que facilita el cibercrimen y podría acelerarlo

Pág. : 15
Cm2: 810,1
VPE: $ 10.642.118

Tiraje: 126.654
Lectoría: 320.543
Favorabilidad: No Definida

Hasta ahora, los ataques cibernéticos eran algo que los delincuentes tenían que producir por su cuenta. Pero programas como ChatGPT pueden convertirse en sus aliados para agilizar sus fraudes, advierten los especialistas.

ISTOCK PHOTO

La empresa especializada Check Point Research realizó un análisis de la herramienta

# El lado oscuro de ChatGPT: expertos alertan que facilita el cibercrimen y podría acelerarlo

Con la ayuda del popular programa basado en inteligencia artificial, los ciberdelincuentes pueden crear fraudes de manera más rápida, más sofisticada y a una escala significativamente mayor, advierten especialistas.

JANINA MARCANO

ChatGPT, una popular herramienta programada por inteligencia artificial, ha ganado fama por su capacidad para mantener una conversación realista y hasta redactar textos "creativos" a gran velocidad. Pero el programa tiene una especie de lado oscuro.

Al menos eso es lo que múltiples grupos de especialistas de varias partes del mundo están alertando: el *software* puede ser una herramienta que ayude a acelerar el cibercrimen.

Así lo reveló, por ejemplo, un informe publicado hace pocos días por Check Point Research, una compañía especializada en amenazas cibernéticas, con base en EE.UU. e Israel.

## Una receta

Un grupo de expertos de la empresa probó la nueva versión del programa (ChatGPT4) y aseguró que esta permite a los ciberatacantes agilizar sus creaciones de ataques maliciosos, lo que resultaría en un crecimiento del cibercrimen.

> *Los últimos años se ha hecho tendencia el uso de inteligencia artificial por parte de los hackers. Ahora con ChatGPT y otras herramientas de uso abierto, esto se puede masificar".*
>
> **RICARDO SEGUEL.**
> ACADÉMICO DE LA U. ADOLFO IBÁÑEZ.

Según Alejandro Botter, gerente de Ingeniería de Seguridad de Check Point Research, el *software* permite que cualquier persona (incluso aquellas sin conocimientos técnicos de programación) pueda construir o mejorar un código computacional para realizar un ataque, "como si se tratara de una receta sencilla".

Concretamente, los investigadores pudieron identificar al menos cinco escenarios de uso potencialmente malicioso en la nueva versión de ChatGPT, entre los cuales están las suplantaciones de identidad en plataformas de bancos, los correos de *phishing* y otros *malware*.

Se trata de potenciales daños que incluso los creadores del *software* han reconocido. Sam Altman, director de Open AI, la empresa que diseñó ChatGPT, ha dicho tener "un poco de miedo" de que su creación se utilice para "desinformación a gran escala o ciberataques".

Además del chat, que es lo que los usuarios más utilizan de ChatGPT, el programa tiene una zona para desarrolladores, explica Botter. "Y lo que vimos es que para alguien con ese perfil no resulta muy difícil usar la herramienta para obtener información que sirve para generar un ataque, sino que basta con hacerle la pregunta correcta al sistema para que te diga cómo hacer ciertas cosas".

Cristián Barría, director del Centro de Investigación en Ciberseguridad de la Universidad Mayor, comenta: "Los delincuentes informáticos le pueden hacer preguntas cada vez más específicas a ChatGPT, con parámetros específicos, para dar como resultado que obtienen los códigos que sirven de base para crear aplicaciones o sitios que generen ataques".

Barría añade: "Si bien (ChatGPT) no te hace todo el trabajo, sí se ha visto que se puede usar para reescribir un código o mejorarlo y así engañar a la gente a través de cosas como duplicar el sitio web de un banco o desarrollar archivos que infecten un computador apenas se abra".

Todo lo anterior es posible, dicen los expertos, a pesar de que la herramienta ha sido mejorada en comparación con su versión anterior para evitar estas vulnerabilidades.

Los especialistas de Check Point Research pudieron comprobar que los filtros del sistema se pueden eludir fácilmente, lo que permite a los ciberdelincuentes alcanzar sus objetivos sin muchos obstáculos. Esto, de acuerdo con imágenes que la empresa subió a su página web de las veces que puso a prueba este sistema.

Pero además el equipo confirmó los casos reales de atacantes que ya están usando la herramienta para crear códigos maliciosos. Y los están compartiendo en internet.

"Estamos hablando de foros donde los cibercriminales están interactuando activamente y comparten su experiencia probando ChatGPT para crear o pulir ciertos códigos, y eso claramente tiene un peligro potencial importante", dice Botter.

## Sin ser hacker

Barría agrega: "Los delincuentes informáticos trabajan de forma organizada y son expertos en generar estos ataques, pero lo que se está alertando es que ahora muchas personas podrán hacer lo mismo sin ser parte de estos grupos de *hackers*".

Esta semana Europol también advirtió sobre el tema, a través de su primer informe sobre la posible explotación de este tipo de sistemas por parte de los delincuentes.

"Hasta ahora, este tipo de comunicación engañosa era algo que los delincuentes tenían que producir por su cuenta. En el caso de campañas producidas en masa, las víctimas de este tipo de delitos a menudo podían identificar la naturaleza no auténtica de un mensaje debido a errores ortográficos o gramaticales obvios o su contenido vago o inexacto", señaló Europol.

Pero con la tecnología artificial, indicaron, el fraude virtual se puede crear de "manera más rápida, mucho más auténtica y a una escala significativamente mayor", agregó.

Coincide Ricardo Seguel, matemático experto en estadística y computación y académico de la Facultad de Ingeniería y Ciencias de la Universidad Adolfo Ibáñez: "ChatGPT puede ser usado para sofisticar la forma en la cual se realizan ataques. A veces los delincuentes fallan porque los textos donde la persona debe hacer clic son muy básicos, pero este sistema puede afinarlos para que la persona no pueda identificar rápidamente que se trata de un engaño y ejecuten sin querer un *malware* en su computador, por ejemplo".

Ante las alertas del posible uso malicioso de la popular herramienta, los expertos hacen un llamado a la educación en ciberseguridad y a aumentar la discusión sobre regulaciones de la inteligencia artificial (ver recuadro). "Queremos dar visibilidad a este tema y que la sociedad sepa que puede haber muchos más ciberataques ahora, y alertar de que la inteligencia artificial tiene otra cara, la del cibercrimen", puntualiza Botter.

### Avanzar en regulaciones

Tras el *boom* de ChatGPT, gigantes tecnológicos como Microsoft y Google anunciaron sus propios *chatbots* similares, lo que da cuenta del veloz crecimiento de la inteligencia artificial y de la feroz competencia por dominarla. Pero ante los peligros que se han advertido, los especialistas creen que es necesario avanzar en la discusión sobre regulaciones. "Los Estados podrían decirles a los programadores cómo pueden o no usar estos sistemas, como se hace en Europa", plantea Cristián Barría. En tanto, Ricardo Seguel asegura que en Chile se está avanzando en una agenda relacionada con la ética y la inteligencia artificial en diferentes industrias, pero "esto debería incluir un aspecto de ciberseguridad", opina el académico.