Publicado en CDMX el 23/03/2023

# [Hillstone Networks desmitifica el poder de ChatGPT en la creación de ataques maliciosos](http://www.notasdeprensa.es)

## Recientemente la empresa de investigación e implementación de inteligencia artificial conocida como OpenAI que diseñó ChatGPT, anunció una actualización denominada GPT-4, la cual incluye mejores capacidades de razonamiento y un 82% menos de probabilidades de responder a solicitudes de contenido no permitido

 Y este último tema fue precisamente el que causó inquietud en el mercado de ciberseguridad, debido a que se hicieron públicos algunos ejercicios donde se utilizaba ChatGPT para desarrollar diversos tipos de ataques maliciosos. Si bien la plataforma alertaba al usuario cuando detectaba un posible riesgo o ilegalidad en la petición, haciendo las preguntas adecuadas el usuario lograba obtener la información requerida. En este sentido se abrieron diferentes preguntas acerca de si este sistema podría ser utilizado por ciberdelincuentes para facilitar el desarrollo de nuevos ataques de malware. Y la evidencia hace pensar que es posible. Al respecto, Manuel Acosta, director general de Hillstone Networks México, explicó que contar con la ayuda de un sistema de inteligencia artificial como ChatGPT no significa que el desarrollo de código malicioso haya llegado al punto de ser indetectable. Sin embargo, es posible que ChatGPT pueda ser utilizado por cibercriminales para llevar a cabo actividades ilegales como generar correos electrónicos falsos o mensajes de texto persuasivos para intentar engañar a las personas y hacerlas caer en una trampa. Además, los cibercriminales podrían utilizar ChatGPT para mejorar su capacidad de crear algoritmos de phishing y otros ataques de ingeniería social que sean más sofisticados y difíciles de detectar. Es importante tener en cuenta que cualquier herramienta, incluyendo ChatGPT, puede ser utilizada tanto para fines legítimos como ilegítimos. La responsabilidad recae en los usuarios de la herramienta para utilizarla de manera ética y legal; y en los desarrolladores para implementar medidas de seguridad y control de calidad para evitar el uso malintencionado. "Las herramientas actuales de ciberseguridad desarrolladas por Hillstone Networks, como iSource XDR, protegen la infraestructura y datos de las empresas a través de servicios de visibilidad e inteligencia de amenazas, los cuales permiten ver, comprender y actuar rápidamente contra las ciberamenazas multicapa y multietapa", destacó Acosta. "Hillstone iSource XDR tiene la capacidad de detectar amenazas basadas en comportamiento, es decir, la tecnología permite identificar si un archivo está realizando tareas para las que no fue diseñado. Por ejemplo, hay ataques que provienen de un archivo legítimo y después de un tiempo despliegan sus verdaderas intenciones; en este caso la inteligencia artificial de iSource XDR investiga el incidente y determina qué hacer para detener la amenaza, además ubica de dónde provino el ataque y cuáles son las alternativas para mitigar esa vulnerabilidad", añadió Utilizando este tipo de tecnologías, que por cierto también están basadas en inteligencia artificial, las empresas pueden tener la certidumbre de que cuentan con las mejores herramientas para hacer frente a los ataques maliciosos, aun cuando usuarios malintencionados hayan hecho uso de herramientas como ChatGPT o la nueva versión GPT-4.

**Datos de contacto:**

Carlos Alberto Soto

Comunicación en Movimiento

5532322068

Nota de prensa publicada en: [https://www.mexicopress.com.mx/hillstone-networks-desmitifica-el-poder-de](http://www.notasdeprensa.es/educalivecom-disfruta-de-cursos-presenciales-y-clases-particulares-a-traves-de-internet)

Categorías: Inteligencia Artificial y Robótica Ciberseguridad Ciudad de México



[**http://www.mexicopress.com.mx**](http://www.notasdeprensa.es)