Siguiendo el ejemplo de WormGPT, los actores de amenazas están promocionando otra herramienta de inteligencia artificial (IA) generativa de ciberdelincuencia llamada FraudGPT en varios mercados y canales de Telegram de la dark web.

> *«Se trata de un bot de IA, exclusivamente orientado a fines ofensivos, como la redacción de correos electrónicos de phishing dirigido, la creación de herramientas de cracking, el carding, etc.»*, dijo el investigador de seguridad de Netenrich, Rakesh Krishnan en un informe publicado el martes.

La empresa de ciberseguridad dijo que la oferta circula al menos desde el 22 de julio de 2023, por un costo de suscripción de 200 dólares al mes (o 1.000 dólares por seis meses y 1.700 dólares por un año).

> *«Si estás buscando una alternativa a Chat GPT diseñada para ofrecer una amplia gama de herramientas, características y capacidades exclusivas adaptadas a las personas sin límites, ¡no busques más!»,* afirma el actor, que se hace llamar CanadianKingpin.

El autor también afirma que la herramienta se puede utilizar para escribir código malicioso, crear malware indetectable, encontrar fugas y vulnerabilidades, y que ha habido más de 3.000 ventas y revisiones confirmadas. El modelo de lenguaje grande (LLM) exacto utilizado para desarrollar el sistema se desconoce actualmente.

Este desarrollo se produce a medida que los actores de amenazas aprovechan cada vez más el surgimiento de herramientas de IA tipo OpenAI ChatGPT para crear nuevas variantes adversarias que están diseñadas explícitamente para fomentar todo tipo de actividad ciberdelictiva sin ninguna limitación.

Estas herramientas, además de llevar el modelo de phishing como servicio (PhaaS) a un nivel

superior, podrían actuar como una plataforma de lanzamiento para los actores principiantes que buscan realizar ataques convincentes de phishing y compromiso del correo electrónico empresarial (BEC) a gran escala, lo que conduce al robo de información sensible y pagos por transferencia no autorizados.

> *«Mientras que las organizaciones pueden crear ChatGPT (y otras herramientas) con salvaguardias éticas, no es una proeza difícil reimplementar la misma tecnología sin esas salvaguardias»,* indicó Krishnan.

> *«Implementar una estrategia de defensa en profundidad con toda la telemetría de seguridad disponible para un análisis rápido se ha vuelto aún más esencial para encontrar estas amenazas de rápido movimiento antes de que un correo electrónico de phishing pueda convertirse en ransomware o exfiltración de datos».*