Microsoft y OpenAI advierten que los actores de los estados-nación están utilizando ChatGPT para automatizar algunas fases de sus cadenas de ataques, incluido el reconocimiento de objetivos y los ataques de ingeniería social.

Desde que la **Inteligencia Artificial (IA)** se hizo presente en nuestra vida, frecuentemente nos sorprendemos de las cosas fantásticas que se pueden hacer con ella. En muchos ámbitos de nuestra vida la AI nos puede ofrecer múltiples ayudas que son bien valoradas.
¿Pero qué sucede cuando esas magníficas capacidades caen en manos de delincuentes? Así de fantásticas también podrían ser los daños y consecuencias de esas acciones.

Un estudio conjunto de **Microsoft** y **OpenAI** identificó y detuvo operaciones llevadas a cabo por cinco grupos de actores estatales que abusaban de los servicios de IA para sus ataques.

Esta es la lista de los grupos APT y sus países de origen:

China: Charcoal Typhoon y Salmon Typhoon
Irán: Crimson Sandstorm
Corea del Norte: Emerald Sleet
Rusia: Forest Blizzard

Estos grupos de APT (Advanced Persistent Threats) estaban vinculados a China, Irán, Corea del Norte y Rusia, y empleaban la IA y los LLM en diversas fases de sus cadenas de ataque.

Los investigadores observaron que los actores estatales utilizaban la **IA** y los **LLM** para el reconocimiento de objetivos, la ingeniería social, el desarrollo de malware, la evasión de detección y otras actividades relacionadas con

los ciberdelincuentes.

Microsoft y OpenAI han establecido principios para mitigar el abuso de sus servicios de IA por parte de actores estatales y otros grupos malintencionados, lo que incluye la identificación y acción contra amenazas maliciosas, la colaboración con otras partes interesadas y la transparencia.

En resumen, la colaboración entre Microsoft y OpenAI destaca la importancia de abordar el uso indebido de la IA en actividades cibernéticas maliciosas y promover medidas para proteger la seguridad en línea.

A medida que la gravedad, la sofisticación, la escala y el alcance de la actividad del Estado-nación continúan aumentando, debemos reinventar la seguridad para mantenernos a la vanguardia.

Por favor, síguenos y danos «me gusta»: