Microsoft reveló el jueves la identidad de cuatro individuos que, según la compañía, estaban involucrados en un esquema de explotación de Azure. Este esquema consistía en obtener acceso no autorizado a servicios de inteligencia artificial generativa (GenAI) para generar contenido ofensivo y dañino.

Esta operación, denominada LLMjacking, ha afectado a diversas plataformas de IA, incluida la Azure OpenAI Service de Microsoft. La empresa está rastreando a esta red de ciberdelincuentes bajo el nombre Storm-2139. Los sospechosos identificados son:

- Arian Yadegarnia, alias *«Fiz»*, de Irán.
- Alan Krysiak, alias *«Drago»*, del Reino Unido.
- Ricky Yuen, alias *«cg-dot»*, de Hong Kong, China.
- Phát Phùng Tấn, alias *«Asakuri»*, de Vietnam.

> Según Steven Masada, abogado general adjunto de la Unidad de Delitos Digitales (DCU) de Microsoft, *«los miembros de Storm-2139 aprovecharon credenciales de clientes filtradas en fuentes públicas para acceder ilegalmente a cuentas que utilizan ciertos servicios de inteligencia artificial generativa.»*
>
> *«Posteriormente, modificaron las capacidades de estas plataformas y vendieron el acceso a otros actores malintencionados, proporcionando instrucciones detalladas sobre cómo generar contenido perjudicial e ilegal, incluyendo imágenes íntimas no autorizadas de celebridades y otros materiales explícitos.»*

Microsoft señaló que este tipo de actividad se realizó con el propósito explícito de sortear los mecanismos de seguridad de los sistemas de IA generativa.

La demanda modificada se presentó poco más de un mes después de que la compañía anunciara acciones legales contra estos ciberdelincuentes, acusándolos de robo sistemático de claves de API de múltiples clientes, incluidas empresas en EE.UU., para luego revender

ese acceso.

Además, obtuvo una orden judicial para confiscar un sitio web (*«aitism[.]net»*) que aparentemente desempeñó un papel clave en la operación ilícita del grupo.

El grupo Storm-2139 está compuesto por tres tipos de participantes:

1. Desarrolladores, responsables de crear las herramientas ilegales utilizadas para explotar los servicios de IA.
2. Distribuidores, encargados de modificar y vender estas herramientas a diferentes clientes.
3. Usuarios finales, quienes las utilizan para generar contenido sintético que infringe la Política de Uso Aceptable y el Código de Conducta de Microsoft.

Asimismo, Microsoft identificó a dos individuos adicionales en Estados Unidos, localizados en Illinois y Florida, cuyos nombres no fueron revelados para evitar interferir en posibles investigaciones criminales.

El informe también incluye a otros co-conspiradores, distribuidores y usuarios finales aún no identificados:

- Un John Doe (DOE 2) que probablemente reside en los Estados Unidos
- Un John Doe (DOE 3) que probablemente reside en Austria y usa el alias «Sekrit»
- Una persona que probablemente resida en los Estados Unidos y use el alias «Pepsi»
- Una persona que probablemente resida en los Estados Unidos y use el alias «Pebble»
- Una persona que probablemente resida en el Reino Unido y use el alias «dazz»
- Una persona que probablemente resida en los Estados Unidos y use el alias «Jorge»
- Una persona que probablemente resida en Turquía y use el alias «jawajawaable»
- Una persona que probablemente resida en Rusia y use el alias «1phlgm»
- Un John Doe (DOE 8) que probablemente reside en Argentina
- Un John Doe (DOE 9) que probablemente reside en Paraguay
- Un John Doe (DOE 10) que probablemente reside en Dinamarca

> *«Combatir a actores maliciosos requiere esfuerzo constante y una vigilancia activa»*, declaró Masada. *«Al exponer a estos individuos y hacer públicas sus acciones, Microsoft busca establecer un precedente en la lucha contra el uso indebido de la inteligencia artificial.»*