TECNOLOGÍA | SIGUE LA POLÉMICA

**Las estafas relacionadas con ChatGPT superan al fraude criptográfico, según Meta**

*Meta ha bloqueado más de 1.000 recursos online malignos relacionados con ChatGPT en sus plataformas.*

**Por Julián M. Zappia.  
Diplomatic Week.**

Según un informe publicado por Meta, la compañía ha bloqueado más de 1.000 direcciones web únicas relacionadas con ChatGPT desde marzo.

Estas páginas están diseñadas para entregar software malicioso a los dispositivos de los usuarios en las tres principales plataformas de la empresa: Facebook, Instagram y WhatsApp.

Los ciberdelincuentes han utilizado el creciente interés en chatbots de inteligencia artificial como ChatGPT para inducir a las personas a hacer clic en correos electrónicos de phishing, registrar dominios maliciosos y desarrollar aplicaciones falsas similares al software generativo de IA.

El equipo de seguridad de Meta ha observado alrededor de 10 familias de malware que utilizan temas relacionados con ChatGPT y otras IA generativas para atraer a las víctimas e instalar malware en sus sistemas.

Guy Rosen, director de seguridad de la información de Meta, comparó el fenómeno con las estafas relacionadas con criptomonedas. Los atacantes intentan tomar el control de páginas y cuentas comerciales para ejecutar anuncios no autorizados que pueden conducir a actividades maliciosas adicionales.

Meta anuncia además una herramienta de soporte que guía a los usuarios en un proceso paso a paso para identificar y eliminar malware.

La compañía descubrió una nueva cepa del mismo llamada “NodeStealer”, dirigido a navegadores en sistemas Windows. Esta cepa fue identificada por primera vez en Vietnam y tenía como objetivo robar cookies, nombres de usuario y contraseñas guardados en cuentas de Facebook, Gmail y Outlook.

Las investigaciones de Meta también revelaron que el malware se distribuyó a través de diversas plataformas, incluidas empresas de intercambio de archivos como Dropbox, Google Drive y Mega. Meta ha compartido información sobre las herramientas maliciosas con las plataformas involucradas.

Para enfrentar estos problemas, además del lanzamiento de la herramienta de eliminación de malware, Meta está realizando cambios en la gestión de las páginas comerciales.

Estos incluyen dar a los administradores más control sobre el acceso a funciones clave y expandir los requisitos de autorización para acciones sensibles.

Más adelante, planea lanzar cuentas Meta Work para que los usuarios empresariales puedan iniciar sesión y operar páginas sin requerir una cuenta personal.

Por último, según el informe trimestral adversarial threat report publicado por Meta, la compañía eliminó tres redes de ciberespionaje y varias redes de comportamiento inauténtico coordinado vinculadas a países como China, Irán y Venezuela.