Publicado en Madrid el 15/03/2023

Ciberatacantes se hacen pasar por ChatGPT para robar credenciales de redes sociales

Los investigadores de Kaspersky han identificado una nueva campaña de malware que se sirve de la popularidad de ChatGPT para robar contraseñas de redes sociales. Los cibercriminales distribuyen el software a través de Facebook, ofreciendo una versión falsa del chatbot. En lugar de ChatGPT, los usuarios son atacados por un troyano denominado Fobo que roba información sensible, como las credenciales de Facebook, TikTok o Google, además de datos personales y bancarios

Los investigadores de Kaspersky han identificado una campaña maliciosa que se centra en los entusiastas de ChatGPT, el chatbot de moda. Los atacantes crean grupos en redes sociales haciéndose pasar por cuentas oficiales del servicio que en realidad son falsas. Estos grupos fraudulentos publican noticias sobre el servicio y ofrecen un cliente de escritorio de ChatGPT a través de un enlace.

Cuando el usuario hace clic sobre el mismo, es redirigido a un sitio web que parece ser el de ChatGPT, donde podrá iniciar la descarga de la aplicación. El proceso de instalación de la falsa app se interrumpirá de forma abrupta. Algunos usuarios pensarán que, por algún motivo, no se ha podido instalar el programa, y no le darán mayor importancia.

Sin embargo, lo que se habrá instalado en el equipo de la víctima es el Troyano-PSW.Win64.Fobo. Está diseñado para el robo de información de cuentas de navegadores como Chrome, Edge, Firefox o Brave, entre otros. El interés de los ciberatacantes es el robo de cookies y credenciales de redes sociales como Facebook, TikTok o Google, especialmente las de empresas. El troyano se hace con los datos de inicio de sesión y trata de robar también de otra información, como las cifras de inversión publicitaria o el saldo de las cuentas comerciales. La campaña de malware se expande a escala mundial y ya se ha detectado en África, Asia, Europa y América.

"Esta campaña utiliza la popularidad de ChatGPT y es un buen ejemplo de cómo los ciberatacantes utilizan técnicas de ingeniería social aprovechando la popularidad de determinadas marcas y servicios. Es importante entender que, aunque parezcan servicios legítimos, en realidad son falsos. Estar informados y mantenerse alerta puede protegernos de este tipo de ataques", explica Darya Ivanova, experta en seguridad de Kaspersky.

Para mantenerse protegido y explorar nuevas tecnologías de forma segura, los expertos de Kaspersky recomiendan:

Ser precavido al descargar software de Internet, especialmente si se hace desde webs de terceros. Siempre se ha de descargar software de sitios oficiales de la compañía o servicio que se vaya a utilizar.

Verificar que la web desde la que se va a descargar el software es legítima. Se debe revisar que la dirección muestre el clásico icono del candado y con la secuencia "https://". Esto certifica que son seguras.

Adoptar un programa de gestión de vulnerabilidades para recibir regularmente los datos más relevantes sobre las vulnerabilidades de los Controladores Lógicos Programables (PLC), los equipos y el firmware, así como aplicar parches o utilizar cualquier solución de protección.

Desconfía de enlaces que provienen de fuentes desconocidas. Los atacantes a menudo utilizan técnicas de ingeniería social para que los usuarios hagan clic sobre enlaces o descarguen software malicioso.

Utilizar una solución de seguridad de confianza y mantenerla siempre actualizada. Es el caso de Kaspersky Premium, que cuenta con la última inteligencia de amenazas y puede detectar y eliminar el malware.

Leer más sobre el troyano Fobo en Kaspersky Daily

Datos de contacto:
Mónica Iglesias
690196537

Nota de prensa publicada en: Madrid

Categorías: Nacional Inteligencia Artificial y Robótica Ciberseguridad