Troyanos bancarios para Android se hacen pasar por ChatGPT

El equipo de investigación de ESET, compañía líder en detección proactiva de amenazas, detectó que cibercriminales están aprovechando el auge de ChatGPT para promover falsas aplicaciones que utilizan el nombre del popular chatbot para infectar con troyanos bancarios. ESET analizó las extensiones maliciosas que utilizan el nombre de ChatGTP para robar cookies y pone en evidencia algunas de las formas de engaño que utilizan el nombre de esta herramienta desarrollada por OpenAI.

“Está claro que los cibercriminales están aprovechando la popularidad de ChatGPT para distribuir malware a través de páginas web y aplicaciones falsas. Es probable que sigan apareciendo sitios falsos y campañas distribuyendo malware y otros engaños aprovechando el auge de las herramientas basadas en inteligencia artificial. Es importante que los usuarios estén al tanto de estas campañas para tomar conciencia y ser cautos a la hora de instalar una extensión o una app que se presenta como atractiva.”, menciona Camilo Gutiérrez Amaya, Jefe del Laboratorio de Investigación de ESET Latinoamérica.

Los troyanos detectados por ESET, son:
Chameleon: Ataca sistemas operativos Android. Ya ha sido identificado en otras campañas en las que se distribuyó usurpando los nombres de Google, Bitcoin, aplicaciones de criptomonedas, bancarias o incluso agencias gubernamentales. Monitoreando los sistemas de ESET, se detectó que también utilizó el nombre y la imagen de ChatGPT: en el dispositivo de la víctima se instala una aplicación que usa como ícono el logo de la app, pero al hacer clic para abrirla, el ícono desaparece.

Chameleon no solo tiene la capacidad de robar credenciales, sino que también es capaz de robar contraseñas y cookies, acceder a los SMS y recolectar, por ejemplo, el código de la verificación en dos pasos (2FA), entre muchas otras cosas más.

Troyano Cerberus: Desde ESET se analizaron campañas que distribuyen este malware para Android que ha estado utilizando el nombre de ChatGPT. El investigador de ESET Lukas Stefanko explicó, en 2019, las características y la historia de su surgimiento. Un año después de su aparición el código de este malware se filtró en foros de hacking y el malware llegó a manos

de otros actores maliciosos para su uso, lo que probablemente dio lugar a la creación de variantes desarrolladas por otros.

En este caso, a través de la telemetría de ESET se encontró una aplicación maliciosa distribuyendo una variante de este malware que utiliza el nombre del chatbot como parte de su ingeniería social.

Al analizar la aplicación, lo primero que llamó la atención del equipo de ESET son los permisos excesivos que solicita, permitiéndole al cibercriminal obtener prácticamente control total del dispositivo. Este troyano es capaz de interceptar mensajes SMS, leer los contactos, acceder a la cámara, a la lista de contactos, al registro de llamadas, modificar audio, obtener una lista de aplicaciones instaladas y muchas otras cosas más. En el caso de los SMS, esta capacidad permite obtener el código de verificación en dos pasos para acceder a una cuenta online.

“Con todos estos permisos concedidos, la aplicación maliciosa es capaz de realizar varias acciones en el equipo infectado, por lo tanto, no solo es importante evitar descargar aplicaciones de repositorios no oficiales, sino también evaluar los permisos que solicita una app y si tiene sentido concederlos de acuerdo a la funcionalidad de la misma”, comenta Camilo Gutiérrez Amaya de ESET Latinoamérica.

Como recomendación principal, desde ESET aseguran que es fundamental tener instalado en los dispositivos un software antimalware de confianza y mantener actualizados los equipos y el software que se utiliza. Si se cree que se ha instalado malware en un dispositivo, se sugiere desconectarlo de Internet y buscar ayuda de un experto en seguridad informática.

Con información de El Impulso