Más de 200 apps de bancos y 110 de criptomonedas tienen un virus que está robando datos

23/12/2022

Un malware está infectado aplicaciones y dispositivos imitando a **Google Protect**, la herramienta de protección de **Android.**

El troyano es conocido como **Godfather o El Padrino** y está en más de 400 aplicaciones en **Google Play Store**, según una investigación de The Hacker News.

Entre las plataformas infectadas se incluyen 215 bancos internacionales, 94 billeteras de criptomonedas y 110 plataformas de intercambio de criptomonedas en **Estados Unidos, Turquía, España, Canadá, Alemania, Francia y el Reino Unido.**

Un virus que evoluciona

Este malware fue detectado por primera vez en junio de 2021, pero dejó de aparecer durante un tiempo hasta que volvió a atacar en los últimos meses.

Para su funcionamiento, El Padrino se sobrepone a las aplicaciones verdaderas y de esta forma, toma los datos que los usuarios ingresan.

La metodología que se implementa es a través del API de accesibilidad de **Android** llamada **Google Protect**, donde logran grabar videos, revisar los clics que hacen las personas, hacer capturas de pantalla, tomar mensajes de texto y rastrear llamadas.

Los investigadores descubrieron que la infraestructura de red del virus cuenta con una dirección de dominio y el control desde otra aplicación; además, de tomar el troyano bancario **Anubis** como base para mejorar sus herramientas de ataque.

“Los desarrolladores de Godfather también modificaron el algoritmo de cifrado de tráfico de Anubis, actualizaron varias funcionalidades como las OTP de **Google Authenticator** y añadieron un módulo independiente para gestionar las conexiones informáticas de redes virtuales”, aseguraron los investigadores.

Lo anterior, da muestra del nivel de complejidad que tiene el malware al mejorar sus protocolos y capacidades de comunicación para el control, lo que le ha permitido extenderse por 16 países.

Cómo evitar caer en estos ataques

Ante el avance de este tipo de malware los usuarios deben saber muy bien desde dónde descargan las aplicaciones en las

que dan datos personales, especialmente las que están relacionadas a bancos. La mejor alternativa es optar por las tiendas oficiales de los teléfonos como **Google Play Store** y **App Store.**

Pero también es fundamental mantener el celular actualizado para que tenga todos los parches de seguridad disponibles dispuestos por el fabricante del teléfono y el sistema operativo.

Además de reportar cualquier anomalía en el uso de las plataformas bancarias y frenar cualquier proceso ante un reporte de ciberataque.

Identifican otro malware bancário

Recientemente se conoció de otro virus que también está atacando aplicaciones bancarias llamado **Zombinder**. En este caso los ciberdelincuentes usan aplicaciones de autorización de conexión wifi, como las que aparecen en hoteles o redes públicas, para invitar a las víctimas a descargar una supuesta plataforma oficial que permita establecer la conexión.

Al instalar la app en el celular, el malware tiene la capacidad de realizar diferentes ataques como robar correos electrónicos, códigos de verificación, credenciales y las frases que protegen los monederos de las criptomonedas.

El virus viene escondido en aplicaciones ‘zombie’, de ahí su nombre. Estas plataformas no tienen ningún tipo de utilidad para el usuario, pero sí se encargan de infectar el dispositivo, incluso con malwares de terceros.

Fuente: Infobae