Estafa por WhatsApp usa nombre de la aerolínea Iberia para distribuir malware en los celulares

30/09/2022

Un mensaje malicioso difundido por **WhatsApp** pretende que las víctimas de este engaño crean que la aerolínea Iberia está regalando **5.000 pasajes** para viajar a Europa, reportó ESET Latinoamérica, compañía de detección de **amenazas**.

El objetivo de esta campaña es que los usuarios ingresen a un link que no está relacionado con la **aerolínea** y descarguen una aplicación de dudosa reputación que perjudica el correcto funcionamiento de **smartphones**. Iberia confirmó que el mensaje se trata de un engaño.

Cómo funciona la estafa

Una vez que los usuarios acceden al enlace que se les envió por **WhatsApp**, son redirigidos a una **página web** que hace uso malicioso de la imagen de Iberia en la que se solicita completar una encuesta. Esta modalidad es muy común en estafas que circulan por medio de la **aplicación** de mensajería instantánea, indicó ESET.

Para aportar credibilidad, la **página web** incluye comentarios falsos de supuestos beneficiarios de los **pasajes aéreos**, quienes en realidad no existen sino que son avatares falsos **programados** para aparecer en el sitio.

Los cibercriminales construyen una página web que incluye comentarios falsos de supuestos beneficiarios de los pasajes aéreos, quienes en realidad no existen.

Luego de completar la **encuesta**, se simula el procesamiento de los datos antes de pasar a la siguiente etapa: un juego en el que la víctima debe seleccionar, de entre varias cajas, aquella que contiene el supuesto premio. Sin importar la opción elegida, tras el segundo intento un **mensaje** informará

al usuario que ganó.

Como requisito adicional, se solicita al usuario que comparta el “sorteo” con sus contactos por medio de **WhatsApp** para poder recibir el premio. Esto es lo que genera que el **engaño** se vuelva masivo en un corto periodo de tiempo.

Sin embargo, luego de haber pasado por todo el proceso, los usuarios son redirigidos a otro sitio web en el que se notifica que el **teléfono** no está funcionando correctamente y se recomienda **descargar una aplicación** con el fin de **optimizar** el dispositivo.

Aunque no se acepte la descarga, las víctimas son redirigidas nuevamente a **Google Play** para descargar la aplicación de nombre Velvet Phone Cleaner & Booster.

Los usuarios que caen en la estafa son redirigidas a Google Play para descargar la aplicación de nombre Velvet Phone Cleaner & Booster.

Comentarios de usuarios indican que la aplicación despliega

anuncios de manera constante aún cuando no está abierta. Sin embargo, dependiendo de la zona geográfica en la que se encuentre la víctima, la **campaña maliciosa** puede que en lugar de llevar a la descarga de una app dirija a las potenciales víctimas a sitios de **suscripción** pagos.

Camilo Gutiérrez Amaya, Jefe del Laboratorio de Investigación de ESET Latinoamérica, comenta que aún cuando se recomienda descargar aplicaciones solo de tiendas oficiales como **Google Play** o **App Store** como parte de una práctica de seguridad, sin embargo esto no es suficiente para mantener el dispositivo seguro.

“Es cierto que **Google** aplica filtros de seguridad para evitar que aplicaciones maliciosas lleguen a la tienda, algo que garantiza una mayor seguridad en comparación con repositorios sin reputación, igualmente los **cibercriminales** logran la forma de colocar sus aplicaciones en las tiendas oficiales”, afirmó Gutiérrez.

También indicó que recientemente, ESET Latinoamérica alertó a usuarios sobre apps en **Google Play** que son utilizadas para distribuir el **malware** Joker, y que “las aplicaciones que prometen limpiar o mejorar el rendimiento del teléfono, o incluso de seguridad, suelen ser utilizadas para distribui**r publicidad invasiva** en los equipos de los usuarios y de esta forma los operadores monetizan estos engaños”.

Fuente: Infobae