Trabajo Práctico

Seguridad en los Sistemas de Información

Objetivos: que el alumno pueda:

- Identificar factores de riesgo en activos de Tecnología de la Información (TI)
- Identificar aspectos que hacen al desarrollo de una Estructura de Seguridad

Tarea previa:

Lectura del material teórico distribuido por la cátedra sobre el tema y asistir a clases teóricas.

Premisa:
"Conocer el riesgo al que están expuestos los activos de TI es imprescindible para gestionarlos y tomar acciones y decisiones acertadas"

EJERCICIO 1:

APP FALSA DE TREZOR EN IPHONE ROBA u$s600.000 EN BITCOINS DE USUARIO
Fuente: https://decrypt.co/es/63550/app-falsa-trezor-iphone-roba-600-000-usd-bitcoins-usuario. Fecha Consulta: 1-4-21

Una aplicación maliciosa para teléfonos inteligentes en la **App Store** de Apple, que imita el nombre y el estilo visual de las carteras de hardware **Trezor**, se utilizó para robar 17,1 **Bitcoin** (BTC) a un usuario desprevenido, con un valor de 600.000 dólares en ese momento, y más de un millón de dólares en la actualidad.

Según un reportaje de *The Washington Post*, el usuario de Trezor, Phillipe Christodoulou, había almacenado sus Bitcoin en un monedero de hardware de Trezor y, para comprobar su saldo, descargó una aplicación que decía ser de Trezor en la App Store de **iOS**.

Aunque Trezor no es actualmente compatible con el sistema operativo móvil iOS de Apple y no tiene una aplicación móvil, la aplicación utilizaba el nombre y la marca de la empresa, y tenía una calificación de los usuarios de casi cinco estrellas, por lo que parecía fiable.

Después de que Christodoulou descargara la aplicación e introdujera sus credenciales, todas sus criptomonedas desaparecieron inmediatamente.

"Han traicionado la confianza que tenía en ellos. Apple no se merece salirse con la suya", dijo Christodoulou.

Christodoulou no es la única persona que ha sido víctima de la estafa; James Fajcz, residente en Georgia, también declaró al medio que perdió 14.000 dólares en Bitcoin y **Ethereum** por la aplicación falsa.

Apple promociona su tienda como "el mercado de aplicaciones más fiable del mundo". En declaraciones al *Washington Post*, un portavoz de Apple explicó que todas las aplicaciones se someten a un riguroso proceso de revisión, pero reconoció que ha habido otras estafas con criptomonedas en la App Store. La aplicación que se utilizó para estafar a Christodoulou estuvo disponible en la App Store al menos del 22 de enero al 3 de febrero y se descargó unas 1.000 veces.

En este caso concreto, la falsa aplicación Trezor se presentó inicialmente en la categoría de "**criptografía**" -como una solución para encriptar archivos del iPhone y almacenar contraseñas- antes de que los desarrolladores la cambiaran por una aplicación de monedero de criptomonedas. Apple declaró al Washington Post que el año pasado había eliminado 6.500 aplicaciones por "funciones ocultas e indocumentadas", pero reconoció que depende de que los usuarios y clientes denuncien las aplicaciones falsas.

Cuando Christodoulou comprobó las reseñas escritas sobre la falsa aplicación Trezor, leyó numerosas quejas de otras personas que habían sido estafadas del mismo modo.

Apple no es la única empresa cuya tienda de aplicaciones ha acogido aplicaciones falsas de monederos de criptomonedas. El 18 de enero 2021, Trezor acudió a Twitter (@Trezor) para advertir a los usuarios de una aplicación maliciosa para Android en **Google Play Store** que se había descargado más de 1.000 veces:

*"¡Advertencia a todos los propietarios de Trezor que utilizan dispositivos **Android**! Esta aplicación es maliciosa y no tiene relación con Trezor o **SatoshiLabs**. Por favor, no lo instale. Recuerda que nunca debes compartir tu clave con nadie hasta que tu dispositivo Trezor te lo pida."*

Por su parte, el portavoz de Google, Colin Smith, dijo al Washington Post: "No permitimos aplicaciones que engañen a los usuarios haciéndose pasar por otra aplicación, desarrollador o empresa, y cuando descubrimos una aplicación que viola nuestras políticas, tomamos las medidas oportunas"; la empresa señaló que recientemente había identificado y eliminado dos aplicaciones falsas de Trezor de la Google Play Store, aunque la empresa de análisis App Figures habría identificado ocho aplicaciones falsas en la tienda.

Se pide:

- Analizar el articulo
- Desarrollar un glosario con términos destacados en letra negrita
- Identificar amenazas asociadas a este incidente de seguridad de la información
- Recomendar medidas de seguridad que minimicen la ocurrencia del incidente

EJERCICIO 2

Una empresa online se dedica a la venta de indumentaria deportiva. Para operar cuenta con los siguientes recursos:

Oficina central; Centro de Cómputo; Hardware; Software; Base de Información de pedidos y facturación; proceso de negocio de ventas; Personal; entre otros.

Se solicita:

- Considerando el concepto de sistema informático elaborar un análisis de riesgos tecnológicos sobre los recursos con los que opera. Se sugiere tomar el siguiente esquema de análisis:
    - Activos e interdependencias
    - Amenaza
    - Impacto
    - Probabilidad de ocurrencia de la amenaza
    - Nivel de Riesgo