Cómo identificar mensajes en WhatsApp que descargan virus y generan publicidad automática

16/12/2022

Los **cibercriminales** siguen buscando beneficios económicos a costa de la **privacidad** de las personas, esta vez se identificaron en **WhatsApp** unos enlaces que descargan un programa tipo **adware** (programa que ofrece publicidad automáticamente)en el **celular,** los cuales afectan el funcionamiento del equipo y roba datos personales.

Cómo funciona un adware

A diferencia de los virus que roban datos privados, este se dedica a generar publicidad de manera exagerada ya sea a modo

de **notificaciones** emergentes, ventana emergente o de otra manera que pueda incomodar a los usuarios durante el tiempo de uso del **smartphone**.

Es por eso que aún cuando los **adware** no son un virus particularmente dañino, sí son capaces de generar malas experiencias de uso mediante la **publicidad** que se genera y al mismo tiempo, hace ganar dinero al **cibercriminal**, pues cada una de esas publicidades le da un porcentaje de ganancia a quienes las difunden.

En ese sentido, los usuarios deben evitar interactuar con cualquier tipo de mensaje que contenga el enlace: : “wp20.ru”.

La gravedad también está en que los contactos de **WhatsApp** están en peligro porque muchas veces esos programas, recogen la data de ellos y propagan el virus con enlaces que tienen las mismas características.

Por tal motivo, aún cuando se trate de un contacto de confianza si el usuario recibe un mensaje que incluya un **link**, deberá preguntar al amigo o familiar si esa información es de confianza, si lo replicó o si nunca envió nada y se trata de una suplantación.

Cuidado con los ciberataques en WhatsApp que contiene virus. Foto: difusión.

La actitud preventiva también tiene que tomarse en plataformas como PCs o laptops, pues no son menos vulnerables a este tipo de malware, por ejemplo, la infección puede modificar la configuración del **navegador** para cambiar la página de inicio, entre otros cambios.

Cómo eliminar y prevenir estos ciberataques

En el caso de que se haya producido una infección, la opción más segura para eliminar los **adwares** del sistema, ya sea smartphone o **PC**, es utilizar un programa antivirus de confianza.

El dispositivo que haya sido vulnerado necesita fortalecer su **sistema** de seguridad y las víctimas necesitan mantener su actitud preventiva para evitar caer nuevamente en este tipo de ataques o en otros.

La recomendación de prevención sobre los links en **WhatsApp** también es aplicable a los **correos electrónicos**, un método comúnmente utilizado para las campañas de phishing con el fin de que los usuarios entreguen información de manera "voluntaria" a los **cibercriminales**.

Para evitar ser una victima de estos agentes maliciosos, es preferible denunciar los correos y cuentas desde las que llegan este tipo de contenidos para que se bloquee el e-mail desde el cual proviene el ataque.

Los ciberataques más comunes

Felipe Sánchez, CEO de WeKall, explicó los 5 tipos de afectaciones más comunes durante este fin de año.

– Ransomware: es un software malicioso de cripto virología que amenaza con publicar los datos de la víctima o bloquear perpetuamente el acceso a ellos a menos que se pague un precio.

– Cryptomining: el programa y componentes de malware son desarrollados para apropiarse de los recursos del ordenador y utilizarlos para la extracción de criptomonedas.

Según la firma de análisis Crystal Blockchain, entre 2011 y lo que va de 2022, las estafas y ataques a la industria de los activos digitales han generado pérdidas de 14.000 millones de dólares.

– Phishing: es un intento fraudulento de obtener información confidencial como nombres de usuario, contraseñas y datos de tarjetas de crédito disfrazándose de una entidad de confianza por medio de e-mails.

– 'Botnets': según la definición del Oxford Dictionary, una cadena de bots es "una red de ordenadores privados infectados con software malicioso y controlados como grupo sin el conocimiento de sus propietarios". ¿Cómo funciona? Primero, un

hacker crea un malware para tener el control de miles de ordenadores. Luego, esclaviza a su ordenador y a otros miles, utilizando su potencia para realizar ataques a gran escala.

– Virus y gusanos: una amenaza camuflada en archivos y programas de procedencia desconocida.

Fuente: Infobae