Image not found or type unknown

www.juventudrebelde.cu

Image not found or type unknown

Los usuarios necesitan ser más conscientes de los modos en que emplean sus terminales, pues si ocurre un ataque sus vidas pueden quedar expuestas. Autor: Getty Images Publicado: 04/09/2019 | 05:15 pm

Lo que pasa en tu iPhone, ¿se queda en tu iPhone?

Vulnerabilidades graves en el sistema operativo iOS permitieron a atacantes desconocidos robar información de miles de usuarios durante años

Publicado: Miércoles 04 septiembre 2019 | 06:49:23 pm.

Publicado por: Yurisander Guevara

Si de algo se precian los equipos con sistema operativo iOS, es de la enorme seguridad que muestran. En teoría, es muy difícil que se vean afectados por virus informáticos, tal y como sucede con los sistemas a base de GNU/Linux.

Asimismo poseen un sistema de encriptación potente; tanto es así que luego de los ataques terroristas de 2015 en San Bernardino, California, el Buró Federal de Investigaciones de Estados Unidos tuvo que pagar cerca de un millón de dólares —de acuerdo con fuentes especializadas en tecnología—, para desbloquear el iPhone 5c de Syed Rizwan Farook, uno de los perpetradores de la masacre.

La compañía con sede en Cupertino, California, Estados Unidos, incluso se ha jactado de ello con anuncios como «Lo que pasa en tu iPhone, se queda en tu iPhone».

Sin embargo, la pasada semana un caso extraño se dio a conocer en los medios a partir de la revelación hecha por expertos en seguridad, quienes afirmaron que desde al menos 2017 y hasta febrero último múltiples iPhone fueron hackeados por una serie de sitios webs que, al ser visitados por usuarios de este tipo de teléfonos, instalaban un malware capaz de brindar al atacante datos privados.

Un salidero

Google Project Zero, el equipo de investigaciones de seguridad informática de Alphabet Inc., reveló el pasado jueves un curioso esquema de hackeo del iPhone. Se trata de una meticulosa cadena de ataques montados a partir del enlazamiento de varios sitios web que explotaban varias «debilidades del día cero» en los móviles de Apple.

Por debilidad del día cero los expertos de Google se refieren a una vulnerabilidad presente en el sistema operativo iOS desde su lanzamiento que no había sido cubierta por Apple, la cual fue empleada por los hackers para atacar silenciosamente a los celulares de la compañía estadounidense.

De acuerdo con la información publicada por los expertos de Google Project Zero, los atacantes se aprovecharon de 14 vulnerabilidades de seguridad presentes en iOS que permitían acceder tanto al mecanismo de seguridad del navegador como hasta el mismo kernel (núcleo) del sistema operativo.

La revista Wired reportó por su parte que en teoría todos los equipos que empleen las versiones de iOS 10 hasta iOS 12 estuvieron expuestos a este tipo de ataque.

Ian Beers, uno de los integrantes del equipo de Google Project Zero y que descubriera el malware, dijo que no hubo discriminación de objetivos, potencialmente cualquiera que accediera a alguno de los sitios web maliciosos era atacado.

Nuevo paradigma

El ataque ha levantado las alarmas no solo por su amplitud, sino por la capacidad que tenían sus perpetradores para recopilar información una vez afectado el equipo. Así, se conoce que en los móviles infestados con este malware los atacantes podían monitorear en vivo su locación, así como extraer fotos, audios, contactos e información sensible como contraseñas personales.

Con tal grado de sofisticación del ataque, los hackers pudieron haber escuchado o leído, además, información de servicios encriptados como WhatsApp, Telegram o Messenger, afirma Gizmodo. En ese sentido explica la publicación que el software dañino no rompe la encriptación de las mencionadas aplicaciones de mensajería, pero a nivel de usuario (una vez arriban al teléfono) las comunicaciones sí son desencriptadas y, por tanto, podían haber sido interceptadas.

Para Beers la situación es muy preocupante, ya que los usuarios de iPhone toman «decisiones arriesgadas» basadas en la gran seguridad del teléfono, y que este aspecto se vea vulnerado es perturbador, aseveró.

Google no ha brindado detalles de los nombres de los atacantes, los sitios web involucrados o quiénes fueron las víctimas. Sin embargo, reveló que los sitios web maliciosos recibían miles de visitas diariamente.

Apple fue informado de esta vulnerabilidad el pasado 1ro. de febrero, y la corrigió seis días después con el parche 12.1.4 de iOS.

Empero, no son pocos los que aseguran que el ataque es el hackeo más grande conocido en la historia del iPhone.

La preocupación se extiende por lo sofisticado del ataque. Y es que emplear sitios web para afectar a móviles es una técnica antiquísima, pero en este caso solo apuntaba a los usuarios de iPhone.

Que un grupo determinado de personas llegue a un lugar de internet siempre está relacionado con los gustos. Este tipo de ataque focalizado puede haber tenido como motivos la recopilación de información de sectores poblacionales específicos.

El método, indican los expertos de seguridad de Google, concuerda con actividades de espionaje a nivel de Estado, y al mismo tiempo marca un parteaguas en la forma de operar de los ciberdelincuentes. La cuestión radica en que si esta manera de atacar a equipos móviles se extiende, los atacantes pueden pasar inadvertidos durante años, tal y como sucedió con el iPhone.

«Ser objetivo de un ataque de este tipo puede significar, simplemente, haber nacido en una región específica o pertenecer a un grupo étnico en particular», reflexionó Ian Beers, y agregó: «Todo lo que pueden hacer los usuarios es ser conscientes del hecho de que la explotación masiva de fallas en un software todavía existe, y así comportarse consecuentemente con posibles repercusiones de un ataque como el descubierto. Las personas deben comenzar a ver sus móviles no solo como equipos cotidianos en sus vidas, sino como dispositivos que, una vez comprometidos por un ataque, pueden exponer su privacidad a personas desconocidas de formas que quizá nunca lleguen a averiguarse». Vale la pena reflexionar al respecto, ¿no creen?

http://www.juventudrebelde.cu/suplementos/informatica/2019-09-04/lo-que-pasa-en-tu-iphone-se-queda-en-tu-iphone