



Un grupo de hackers afirma haber hackeado el sensor dactilar del iPhone 5S

Un grupo de ciberactivistas alemanes afirmó haber descifrado el escáner de huellas dactilares del iPhone, sólo dos días después de que Apple lanzara una tecnología que promete proteger mejor a los dispositivos de los delincuentes e intrusos.

Si se verificara esta afirmación, supondrá una situación embarazosa para Apple, que está apostando por el escáner para configurar su teléfono inteligente, lejos de los nuevos modelos de Samsung Electronics y otros que funcionan con el sistema operativo Android de Google.

Dos eminentes expertos de seguridad en iPhone dijeron a Reuters que creían que el grupo alemán, conocido como Chaos Computer Club (CCC en sus siglas en inglés), tuvo éxito en sortear el sistema de seguridad Touch ID de Apple, aunque no habían reproducido personalmente el logro.

Uno de ellos, Charlie Miller, coautor del Manual de Hackers de iOS, describió el trabajo como una «ruptura completa» de la seguridad del Touch ID. «Realmente abre una nueva posibilidad para los atacantes», señaló.

Representantes de Apple no respondieron a la petición de comentarios.

CCC, uno de los mayores y más respetados grupos de hackers del mundo, colgó un video en su página web que parecía mostrar a alguien accediendo al iPhone 5S con una impresión fabricada de la huella digital.

El sitio describió cómo miembros de su equipo biométrico habían descifrado el nuevo lector de huella digital, una de las pocas grandes características de alta tecnología añadida a la última versión del iPhone.

El grupo dijo que había elegido el Touch ID para derribar los informes sobre sus «maravillas», que sugerían que iba a ser difícil de sortear.

«Las huellas digitales no deberían ser utilizadas para asegurar cualquier cosa. Las dejas por todas partes, y es demasiado fácil hacer dedos falsos de impresiones levantadas», dijo un



hacker de nombre Starburg citado en el sitio de CCC.

El grupo dijo que entró en el Touch ID fotografiando la huella digital de un usuario de iPhone, después la imprimió en una lámina transparente que se utiliza para crear un modelo para un «dedo falso».

CCC dijo que se habían utilizado procesos similares para violar la «gran mayoría» de los sensores de huellas digitales en el mercado.

«Creo que es legítimo», dijo Dino Dai Zovi, otro coautor del Manual del Hacker iOS. «El CCC no engaña o exagera, sobre todo cuando están tratando de demostrar un tema político», añadió.

Touch ID, el sensor biométrico del iPhone 5S, permite a los usuarios desbloquear sus dispositivos o hacer compras en iTunes simplemente poniendo su dedo en el botón de inicio. Se utiliza un sensor de cristal de zafiro incrustado en el botón.

Dos expertos en seguridad que patrocinaron una competición con una recompensa en dinero y otros premios a los primeros hackers que violasen la seguridad del iPhone dijeron que habían revisado la información colgada en la web de CCC, pero que querían más documentación.

«Estamos simplemente esperando un video completo con toda la documentación y el inicio del proceso que han reivindicado (para llevarse la recompensa)», dijo el investigador de seguridad móvil Nick DePetrillo, que empezó el concurso junto con otro experto, Robert Graham.

El premio en metálico para el ganador asciende a 13.000 dólares.

Fuente: eluniversal