WhatsApp: riesgos de uso

WhatsApp ha calado en el uso diario de una gran mayoría de usuarios de los dispositivos móviles con conexión a Internet. El intercambio de información sensible que se produce a través de esta plataforma es constante y, sin embargo, la seguridad de WhatsApp no está garantizada. En este informe se analizan algunas de las debilidades de esta aplicación en materia de seguridad.

1 Contexto de la aplicación

La aplicación para dispositivos móviles WhatsApp fue lanzada al mercado en el año 2009 y actualmente gestiona alrededor de mil millones de mensajes al día. Se trata de una plataforma que permite, pues, enviar mensajes de texto mediante la conexión a Internet, ya sea la del 3G asociado al propio dispositivo móvil o una conexión inalámbrica de tipo Wi-fi. Al ser inicialmente gratuita en algunas plataformas, WhatsApp ha contribuido substancialmente al declive en el uso de los SMS; la mayoría de personas cuyo móvil tiene conexión a Internet están optando por utilizar WhatsApp y abandonar los SMS, especialmente cuando descubren que muchos de sus contactos ya utilizan la aplicación y, por consiguiente, van a poder comunicarse con ellos a un precio virtualmente gratuito.

Este proceso, que ha ido retroalimentándose, explica que WhatsApp se haya convertido en poco tiempo en una de las diez aplicaciones más descargadas en 16 países –en cinco de éstos es incluso la primera aplicación más descargada. Al tener un comportamiento semejante en cierta medida al de una red social convencional (incorpora de forma automática los contactos existentes en el móvil y posibilita el reencuentro del usuario con personas con quien se había perdido el contacto, por ejemplo), WhatsApp es propenso a su

expansión y a situarse en el punto de mira de los ciberatacantes que intentan obtener datos e información de sus usuarios.

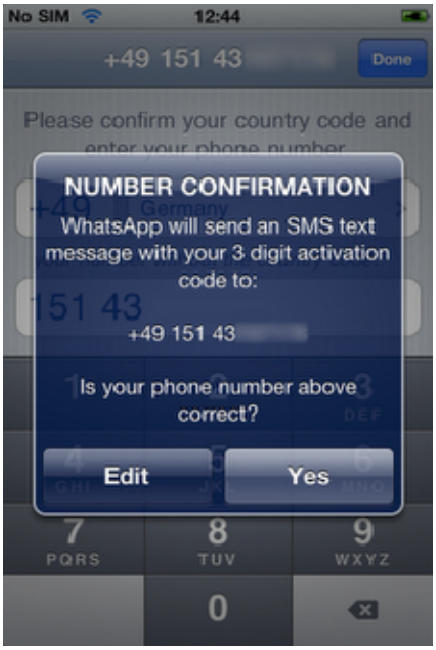
2 Problemas de seguridad

La compartición de información personal sensible que se produce a diario en WhatsApp, por un lado, y la escasa percepción de riesgo que los usuarios tienen para con la seguridad de la información vinculada a los dispositivos móviles, por el otro, ha convertido a esta plataforma en un entorno atractivo para intrusos y ciberatacantes. A este respecto, sorprende que los creadores de WhatsApp hayan descuidado desde el principio algunos elementos básicos en cuanto a la protección de la aplicación y de los datos personales que se gestionan en ella.

En este sentido, la carencia más importante de la plataforma hasta el momento ha residido en el proceso de alta y verificación de los usuarios. A partir de la explotación de esta vulnerabilidad, **cualquier intruso puede hacerse con la cuenta de usuario de WhatsApp de otra persona, leer los mensajes que reciba e incluso enviar mensajes en su nombre**. Se trata de un secuestro de la cuenta en toda regla, propiciado por las características del proceso de registro. A continuación, se describen los pasos que siguen los ciberatacantes para comprometer las cuentas de WhatsApp de terceros.

2.1 Vulnerabilidad en el proceso de registro

Para darse de alta en WhatsApp, la aplicación pide un número de teléfono al usuario y, posteriormente, éste recibe un SMS con un código de activación de tres dígitos, con el fin de poder demostrar que efectivamente el número de teléfono y el dispositivo asociado a este número le pertenecen. Sin embargo, este PIN puede ser interceptado por un ciberdelincuente.



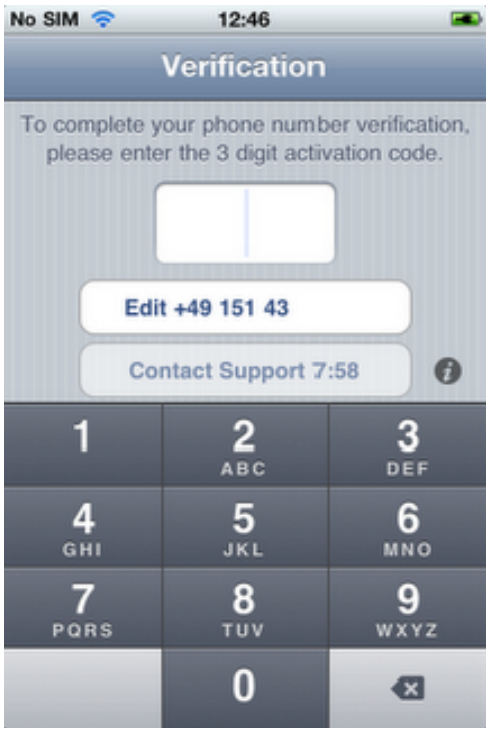
Durante este proceso, el código de activación se genera en el propio entorno de la aplicación, incluso antes de ser enviado a los servidores internos para que éstos manden el mensaje SMS, con el código, al usuario.

Por consiguiente, un intruso que quiera interceptar una cuenta de WhatsApp ajena puede:

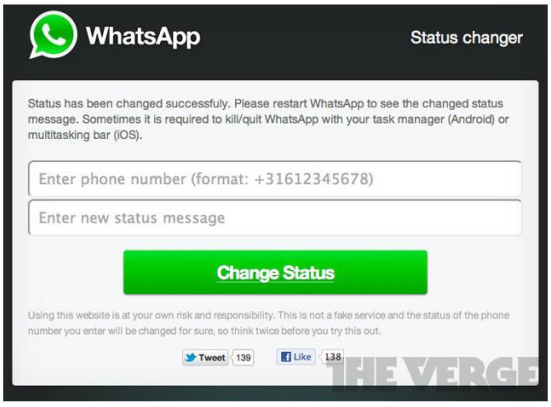
→ Introducir cualquier número de teléfono para iniciar el proceso de alta en WhatsApp

→ Interceptar la petición HTTP(S) y averiguar el código de activación de tres dígitos, que se presenta asociado al parámetro *auth.*

A partir de este momento, y al haber sido interceptada la petición HTTP(S) antes de que ésta llegara a los servidores internos, no se llegará a generar ni a enviar ningún mensaje SMS de activación al número de teléfono objeto del secuestro de identidad, por lo que la víctima no será consciente de ello. Para terminar el proceso, el atacante recreará una supuesta respuesta HTTP por parte del servidor y la enviará a la aplicación de WhatsApp, de manera que ésta crea que el mensaje SMS se envió correctamente al usuario y que el proceso de registro ha finalizado con éxito.



Llegado a este punto, el intruso empleará el código de activación –que fue obtenido mediante la intercepción de la petición HTTP(S)- para darse de alta en WhatsApp con un número de teléfono que no corresponde al dispositivo móvil utilizado. Posteriormente, este número seguirá el proceso de registro automático en el chat de WhatsApp Messenger, mediante otra petición a los servidores internos que, a su vez, podrá ser interceptada por el intruso. La intercepción de esta última petición es la más importante, y permitirá al intruso secuestrar cualquier número de teléfono y asociarlo a su propio UDID (Unique Device Identifier, esto es, un texto de 40 caracteres que identifica a un dispositivo, en este caso a uno de tipo iPhone/iPod)



Para futuras autenticaciones de la cuenta, el número de teléfono se utilizará como usuario y el UDID del dispositivo del intruso, como contraseña. Además, **cualquier mensaje que WhatsApp decida enviar al usuario se redirigirá al dispositivo del intruso que le ha secuestrado la cuenta.** En este sentido, la víctima no sabrá que su cuenta de WhatsApp ha sido comprometida; sólo cuando se conecte al chat de la aplicación la próxima vez, se le informará de que no puede acceder al servicio a causa de un cambio de configuración del dispositivo –se trata del citado cambio de UDID por parte del intruso.

2.2 Otros fallos de seguridad

Desde sus inicios, **WhatsApp ha tenido que convivir con las críticas por la pésima gestión de la seguridad de su aplicación**. La falta de cifrado, por ejemplo, demostró que los datos intercambiados por los usuarios estaban desprotegidos de cualquier protocolo de seguridad; esta situación, que se puso de manifiesto hace poco menos de un año, permitía el acceso a la agenda telefónica y a los mensajes de los usuarios conectados a Internet mediante Wi-fi. El problema consistía en que la información enviada por y entre los usuarios salía por el puerto de tráfico cifrado 443 (HTTPS) pero, en cambio, era recibido por los servidores de WhatsApp como texto simple. A efectos prácticos, **cualquier persona podía acceder a los números de teléfono y al contenido de los mensajes enviados a través de WhatsApp**. Además, si éstos se mandaron con el GPS del dispositivo activado, los intrusos o ciberatacantes podían descubrir fácilmente la ubicación del usuario puesto que WhatsApp también almacena las coordenadas geográficas y las mantiene desprotegidas.

Por otro lado, a principios de año apareció en Internet una página web que permitía cambiar el estado de la cuenta de WhatsApp de cualquier usuario, simplemente introduciendo su número de teléfono móvil. Para conseguirlo, los creadores de esta web simplemente tuvieron que utilizar uno de los fallos de seguridad descubiertos en diciembre de 2011. La consecuencia fue que muchos usuarios encontraron su mensaje de estado cambiado.

Ante los recurrentes problemas de seguridad, WhatsApp ha mantenido una posición bastante críptica. A través de su Twitter, y en alguna ocasión puntual mediante su blog, ha emitido algún mensaje para intentar tranquilizar a sus usuarios, aunque la realidad es que ha solido reaccionar tarde y a destiempo.

Si bien en los últimos meses WhatsApp ha desarrollado actualizaciones de la aplicación con el fin de corregir los problemas de seguridad, la sensación es que siempre actúa a posteriori, una vez los fallos y las vulnerabilidades se han hecho públicas y han dañado su imagen y credibilidad. Éstas, además, no amainan. Recientemente, sin ir más lejos, **un portal de seguridad de la información se hizo con los más de diez millones de números de teléfono asociados a las cuentas de WhatsApp en España.**