Informe de Amenazas
CCN-CERT IA-21/16

Riesgos de uso de WhatsApp

Septiembre de 2016

CENTRO CRIPTOLOGICO NACIONAL
2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, cn=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2016.10.07 13:07:22 +02'00'

ÍNDICE

1. SOBRE CCN-CERT

El CCN-CERT (www.ccn-cert.cni.es) es la Capacidad de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN. Este servicio se creó en el año 2006 como **CERT Gubernamental Nacional español** y sus funciones quedan recogidas en la Ley 11/2002 reguladora del Centro Nacional de Inteligencia, el RD 421/2004 de regulación del CCN y en el RD 3/2010, de 8 de enero, regulador del Esquema Nacional de Seguridad, modificado por el RD 951/2015, de 23 de octubre.

De acuerdo a todas ellas, el CCN-CERT tiene responsabilidad en ciberataques sobre **sistemas clasificados** y sobre sistemas de las **Administraciones Públicas** y de **empresas y organizaciones de interés estratégico** para el país. Su misión, por tanto, es contribuir a la mejora de la ciberseguridad española, siendo el centro de alerta y respuesta nacional que coopere y ayude a responder de forma rápida y eficiente a los ciberataques y a afrontar de forma activa las ciberamenazas.

2. ÁMBITO

La información contenida en este informe es válida para las versiones de WhatsApp anteriores a agosto de 2016. Hay que tener en cuenta que, debido al ritmo de desarrollo de la herramienta es posible que, en el momento de la lectura de este informe, alguno de los puntos descritos no sea aplicable o sea inexacto. Por este motivo, se anima a cualquier lector que quiera colaborar en la mejora de este informe, nos haga llegar cualquier comentario o sugerencia a info@ccn-cert.cni.es

3. 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 enviar mensajes de texto mediante la conexión a Internet, ya sea mediante el módem 3G/4G asociado al propio dispositivo móvil o una conexión inalámbrica de tipo Wi-Fi (*Wireless Fidelity*).

Al ser inicialmente gratuita en algunas plataformas, WhatsApp ha contribuido sustancialmente al declive en el uso de los SMS (*Short Message Service*). 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 de manera gratuita.

Este proceso, que ha ido retroalimentándose, explica el hecho por el que WhatsApp se ha convertido, en poco tiempo, en una de las diez aplicaciones más descargadas[1] en 16 países, siendo incluso en cinco de estos países 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.

3.1 PROBLEMAS DE SEGURIDAD EN LA ACTUALIDAD

La compartición de información personal sensible que se produce a diario en WhatsApp, junto con la escasa percepción de riesgo que los usuarios tienen con la seguridad de la información vinculada a los dispositivos móviles, ha convertido a esta plataforma en un entorno atractivo para intrusos y ciberatacantes.

[1] **App Annie 2015 Retrospective:** https://www.appannie.com/insights/market-data/app-annie-2015-retrospective/

Desde sus inicios, los creadores de WhatsApp han descuidado algunos elementos básicos en cuanto a la protección de la aplicación y de los datos personales que se gestionan en esta aplicación.

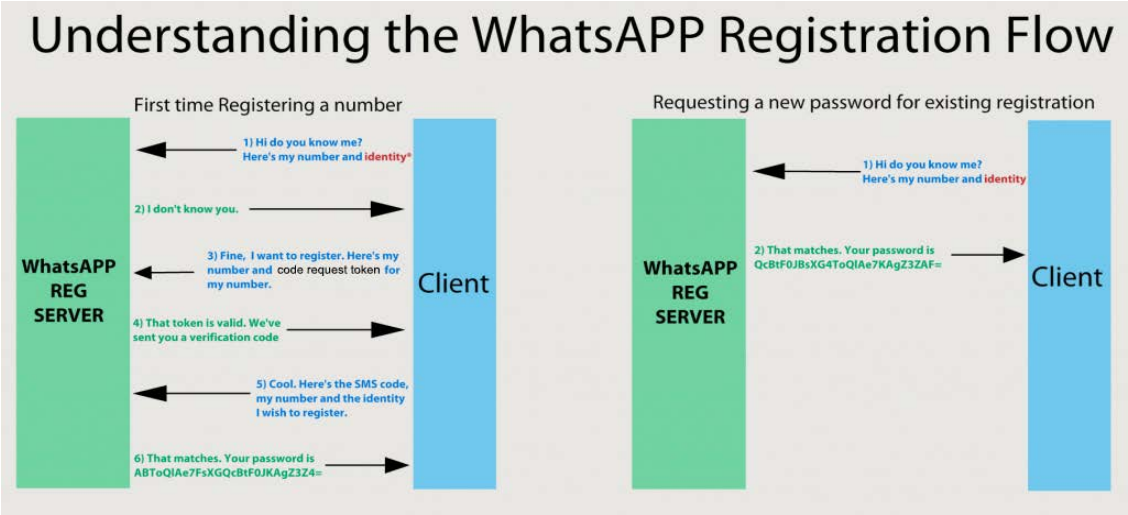


Ilustración 1. Flujo en el registro de usuario

En este sentido, la carencia más importante de la plataforma hasta el momento ha residido en la seguridad en el proceso de alta[2] y verificación de los usuarios. Las características del proceso de registro propician que un intruso pudiera hacerse con la cuenta de usuario de WhatsApp de otra persona, leer los mensajes que reciba e incluso enviar mensajes en su nombre.

3.2 SECUESTRO DE CUENTAS APROVECHANDO FALLOS DE LA RED

Hace unos meses, la firma Positive Technologies hizo público un vídeo[3] mostrando cómo secuestrar cuentas, tanto de WhatsApp como de otras aplicaciones como Telegram, utilizando fallos conocidos en el protocolo de telecomunicaciones **SS7**[4] (Signalling System No. 7).

El protocolo SS7 es el estándar global para las telecomunicaciones, desarrollado por AT&T en 1975, y define el protocolo y procedimientos mediante los cuales los elementos de una red de telefonía intercambian información sobre una red digital para efectuar el enrutamiento, establecimiento y control de llamadas y que forma parte, entre otros, del funcionamiento interno de servicios como los SMS.

Anteriormente, algunos investigadores ya mostraron[5] fallos de seguridad de este protocolo en la conferencia de hacking alemana *Chaos Communication Congress*, demostrando que en el caso de que un atacante consiguiera acceso al sistema SS7,

[2] **WhatsApp Registration Flow:** https://github.com/mgp25/Chat-API/wiki/WhatsApp-Registration-Flow

[3] **How to hack WhatsApp and Telegram:** https://habrahabr.ru/company/pt/blog/283052/

[4] **SS7:** https://es.wikipedia.org/wiki/SS7

[5] **SS7: Locate. Track. Manipulate :** https://berlin.ccc.de/~tobias/31c3-ss7-locate-track-manipulate.pdf

podría interceptar o grabar llamadas, leer SMS, o detectar la localización del dispositivo utilizando el mismo sistema que la red del teléfono.

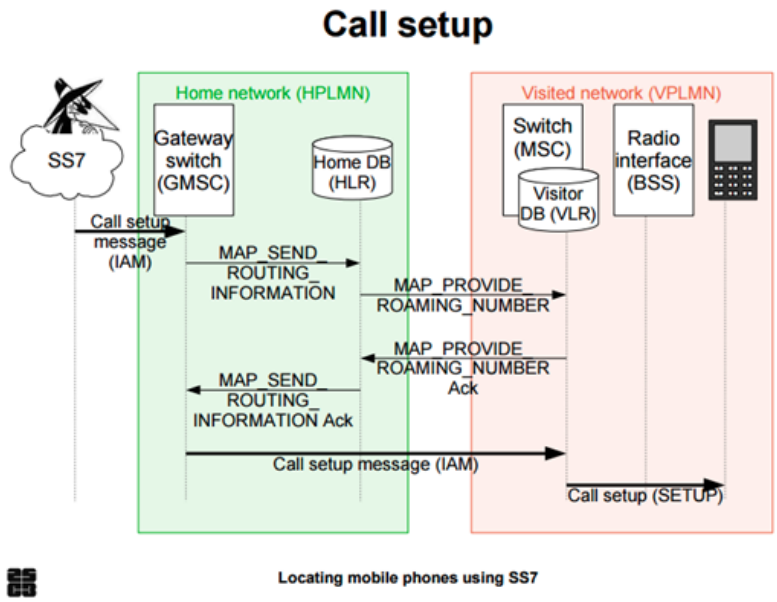


Ilustración 2. Localización de teléfonos usando SS7

Aprovechando estos fallos de seguridad conocidos y aún sin resolver, el ataque se realiza de forma sencilla, haciendo creer a la red telefónica que el teléfono del atacante tiene el mismo número que la víctima.

De esta forma se consigue recibir un código de verificación de WhatsApp válido, teniendo acceso completo a la cuenta de la víctima, independientemente del cifrado incluido en las comunicaciones.

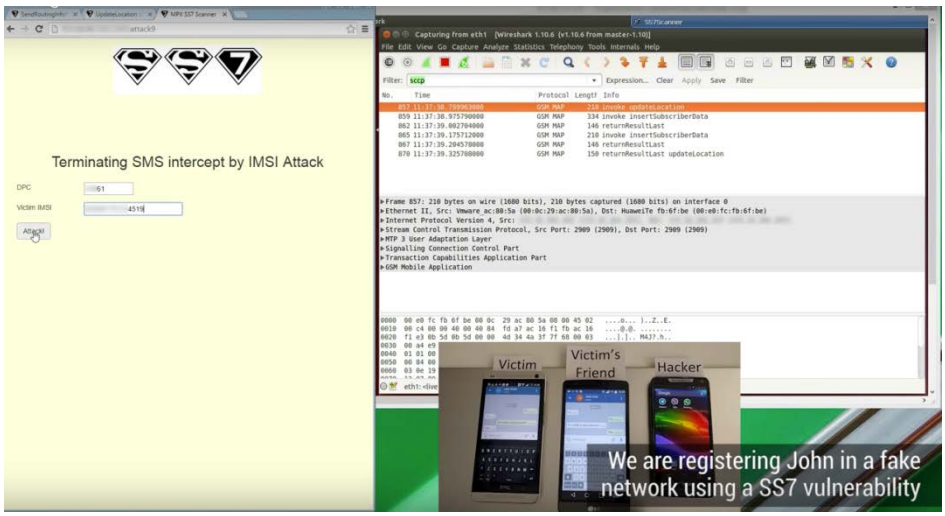


Ilustración 3. Ejemplo de vulnerabilidad en SS7

Al tratarse de un fallo de red, no dependiente de la aplicación en sí misma, no existe una forma directa de resolver estos fallos de seguridad.

Como alternativa, se recomienda activar la opción de "Mostrar notificaciones de seguridad":

1. Abrir WhatsApp y presionar sobre ***Ajustes***.
2. Tocar en ***Cuenta*** y seleccionar ***Seguridad***.
3. En esta pantalla se pueden habilitar las notificaciones de seguridad cuando se selecciona ***Mostrar notificaciones de seguridad***.

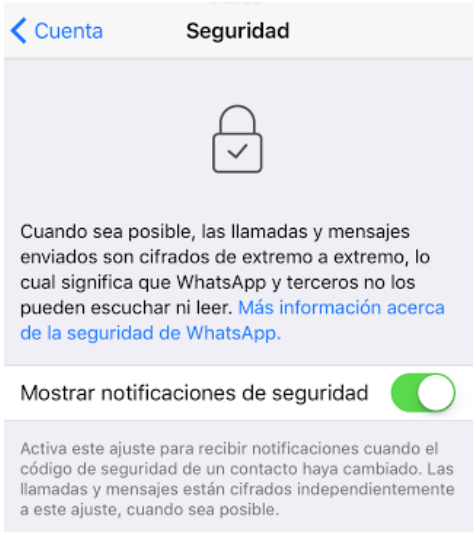


Ilustración 4. Mostrar notificaciones de seguridad en WhatsApp

Cada chat tiene un código de seguridad único que es usado para confirmar que las llamadas y mensajes que se envían a ese chat, están cifrados de extremo a extremo. Este código se encuentra en la pantalla de información de los contactos y está disponible en forma de código QR y de 60 dígitos:

Ilustración 5. Código de seguridad único

Estos códigos son únicos para cada chat y pueden ser comparados entre los receptores de los mensajes para confirmar que, los mensajes enviados a ese chat, están cifrados de extremo a extremo. Los códigos de seguridad son una versión visible de esas

claves especiales compartidas. El código que se observa no es la clave en sí, esa siempre se mantiene secreta.

El código de seguridad usado en el cifrado de extremo a extremo puede cambiar algunas veces. Esto puede suceder porque algún contacto reinstaló WhatsApp, cambió de teléfono móvil o porque haya sido víctima de un ataque como el que se ha indicado anteriormente.

3.3 BORRADO INSEGURO DE CONVERSACIONES

Uno de los fallos más comunes en las aplicaciones de mensajería es la forma insegura que utilizan para borrar las conversaciones almacenadas en el teléfono. Este fallo, que ya se utilizaba en versiones anteriores de la aplicación para obtener los registros de las conversaciones utilizando técnicas forenses, vuelve a afectar a las versiones más recientes de WhatsApp.

Para entender el problema, es necesario explicar brevemente el funcionamiento de la base de datos (SQLite[6]) que utiliza la aplicación para guardar y mantener las conversaciones en el teléfono.

Ilustración 6. Proceso de borrado de una conversación

El proceso de borrado de una conversación, mensaje o grupo es sencillo en el teléfono, pero no implica la eliminación directa de los mensajes, sino que estos quedan marcados como libres, de tal forma que puedan ser sobrescritos por nuevas conversaciones o datos cuando sea necesario. Esto permite mejorar el consumo de recursos en los dispositivos y mejorar el sistema de almacenamiento, actuando de forma

6 **SQLite:** https://es.wikipedia.org/wiki/SQLite

similar a la papelera de reciclaje de un ordenador convencional, pero no garantiza el borrado seguro de las conversaciones.

Ilustración 7. Copia de seguridad Apple

Esta opción está disponible a través de **iCloud** para la versión *iOS*, así como a través de **Google Drive** en versiones *Android*. WhatsApp, en cada copia de seguridad sólo subirá las nuevas conversaciones y archivos. Siempre existirá en Google Drive una copia exacta de las conversaciones y archivos que se tienen en ese momento en WhatsApp. En el caso de iCloud, los archivos se encuentran ocultos y tan solo la aplicación WhatsApp podrá acceder a ellos.

Además, hay que tener en cuenta las implicaciones cuando se tenga activa la opción de copia de seguridad, ya que esta información también será respaldada de forma automática, almacenando una posible conversación ya borrada, y que podría ser recuperada en un futuro.

Ilustración 8. Copia de seguridad Android

Como medida preventiva, y mientras los creadores de la aplicación no implementen otros mecanismos para el borrado de los datos, la única forma de eliminar estas conversaciones de una forma más segura en nuestro teléfono será desinstalar la aplicación e instalarla de nuevo. Aunque se debe tener en cuenta que este proceso no eliminará las posibles copias de seguridad de nuestros datos que se hayan hecho en la nube.

3.4 DIFUSIÓN DE INFORMACIÓN SENSIBLE DURANTE LA CONEXIÓN INICIAL

Durante el establecimiento de conexión con los servidores de la aplicación WhatsApp intercambia en texto claro información sensible acerca del usuario, como:

1. Sistema operativo del cliente.
2. Versión de la aplicación en uso.
3. Número de teléfono registrado.

Esta información puede quedar expuesta a cualquier atacante en el caso de utilizar redes Wi-Fi públicas o de dudosa procedencia.

En versiones anteriores al cifrado extremo a extremo, una traza de conexión que muestra esta información podría ser similar a la siguiente:

Ilustración 9. Número de teléfono transmitido en claro

En ellas se puede apreciar toda la información anteriormente descrita, siendo expuesta al atacante. A partir de la implementación del cifrado E2E (extremo a extremo), este mecanismo de conexión ha variado ligeramente. El formato de codificación del número de teléfono (utilizado como nombre de usuario para acceder al sistema) ha sido modificado. Ahora se muestra como una representación en binario, tal y como se puede apreciar a continuación:

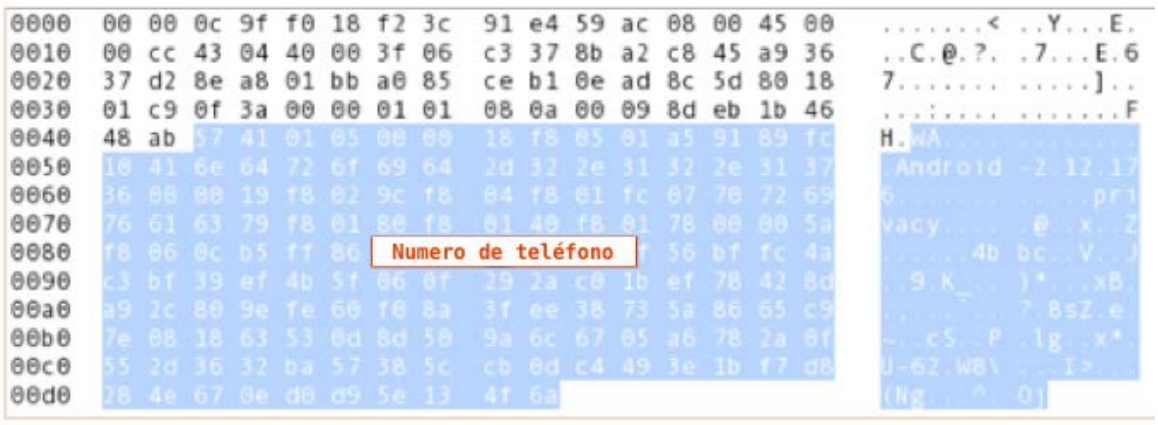


Ilustración 10. Número de teléfono transmitido en binario

De esta forma, la variación en el sistema de conexión inicial no implica una mejora sustancial en la seguridad ya que, la información, a pesar de estar codificada de forma diferente, es mostrada igualmente en texto plano para cualquier atacante con acceso al canal de comunicación que utilice.

La única solución a este problema de difusión de información sensible será el uso de una conexión VPN.

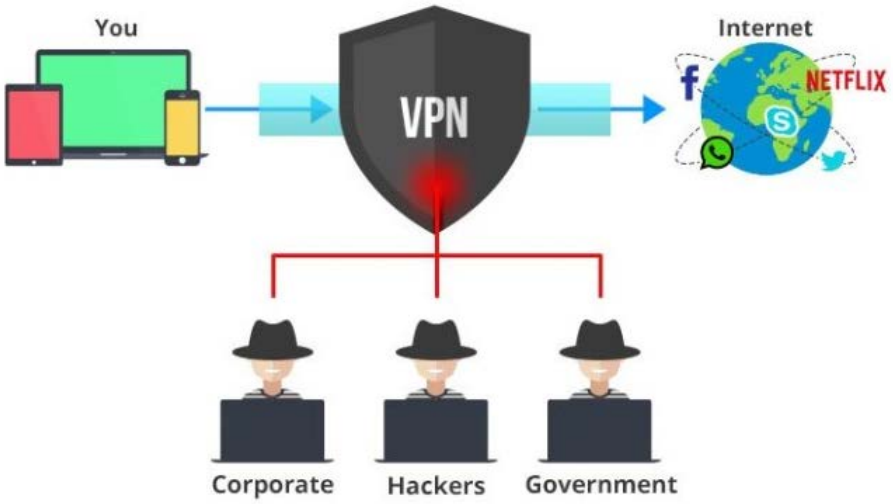


Ilustración 11. Perspectiva de seguridad del uso de VPN

Al usar una VPN se crea una red privada virtual que mantiene todo el tráfico intercambiado por el teléfono con un extra de seguridad. Mientras se navega, se mantiene una conversación o se escucha música, todos los datos enviados y recibidos pasan cifrados entre el emisor y el receptor, añadiendo una nueva capa de seguridad para evitar posibles atacantes que estén interceptando el tráfico de red (*man-in-the-middle*).

3.5 ROBO DE CUENTAS MEDIANTE SMS Y ACCESO FÍSICO

Algunos de los ataques con mayor índice de éxito no implican el uso de vectores de ataque avanzados o tecnología sólo accesible para unos pocos. Un posible descuido o pérdida del teléfono (a pesar de tener los mecanismos de bloqueo de pantalla y código de seguridad) puede permitir que una persona con acceso físico al teléfono pueda secuestrar la sesión de WhatsApp de una forma sencilla.

El primer método tiene que ver con el sistema de registro de la aplicación. Un atacante podría utilizar un teléfono propio o un emulador de terminal y comenzar el proceso de registro con el número de la víctima, como si se tratara de un cambio de terminal.

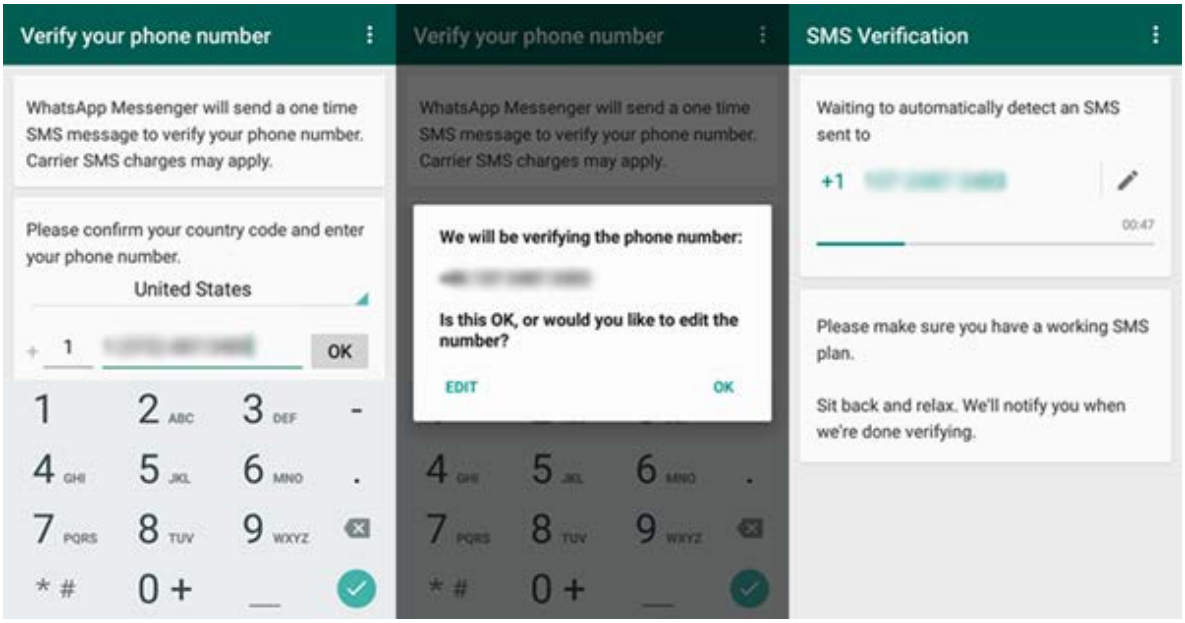


Ilustración 12. Verificación del teléfono en WhatsApp

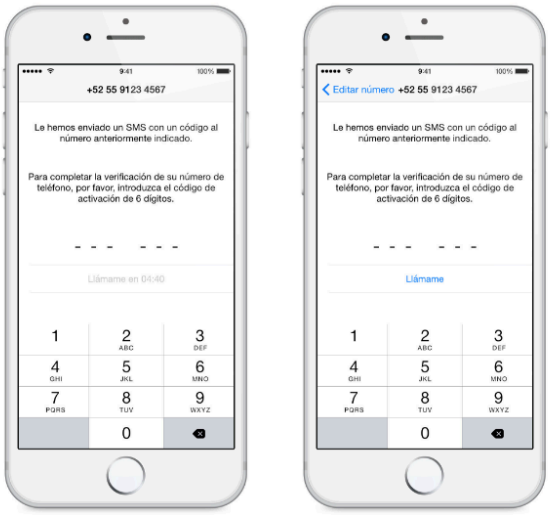
Si el atacante consigue acceso físico al teléfono y la previsualización de SMS se encuentra activada, podrá observar el código de seguridad que el teléfono reciba, registrando satisfactoriamente su terminal y obteniendo acceso a la sesión de la víctima.

Para evitarlo, se procederá a desactivar la previsualización del remitente y contenido en la pantalla de bloqueo del terminal.

3.6 ROBO DE CUENTAS MEDIANTE LLAMADA Y ACCESO FÍSICO

De forma similar a la descrita anteriormente, es posible secuestrar una sesión de WhatsApp utilizando la opción de verificación por llamada telefónica.

Si el método para ocultar las notificaciones de SMS se encuentra activo, el atacante sólo deberá tener físicamente el teléfono durante 5 minutos para poder acceder a la verificación por llamada, descolgar y obtener el código de verificación.



El problema de esta fórmula de ataque reside en la dificultad para evitarlo, debido a que no existe una opción, tanto para *Android* como para *iPhone*, que fuerce al usuario a desbloquear el terminal para poder responder a una llamada, por lo que un atacante con acceso físico siempre podrá responder y completar el ataque.

Además, cuando la víctima quiera recuperar el control de su cuenta, deberá esperar, al menos, 30 minutos como plazo de seguridad por la aplicación para obtener un código de verificación nuevo, por lo que durante este periodo de tiempo no existirá forma posible de evitar el secuestro y manipulación de la sesión por parte del atacante.

Por el momento, la única contramedida sería recopilar los diferentes números de teléfono utilizados por la aplicación para realizar estas llamadas de verificación y bloquearlos desde el terminal para no poder realizar la activación utilizando este mecanismo.

3.7 PELIGROS DE LA DESCARGA DE WHATSAPP DE *MARKETS* NO OFICIALES

Cuanto más famosa es una aplicación, más interesante se vuelve para los ciberdelincuentes para la realización de fraudes.

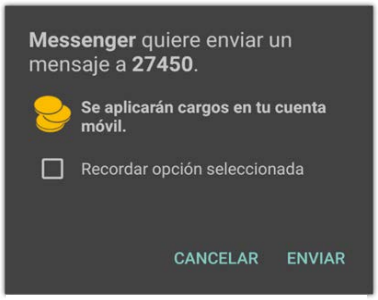


Ilustración 13. SMS *Premium*

Como gancho para captar usuarios, normalmente, se utilizan las características más novedosas de la aplicación o la promesa de funciones poco fiables, como la posibilidad de espiar otras cuentas u obtener servicios no disponibles oficialmente. Como, por ejemplo, el caso de una aplicación denominada **WhatsApp Trendy Blue**, que prometía altas posibilidades de personalización y características no disponibles en la versión oficial. Los estafadores entonces se hacían con el número de teléfono del usuario y exigían el envío de una invitación a 10 amigos para suscribirles a un servicio SMS Premium, consiguiendo propagarse entre los contactos más cercanos obteniendo un beneficio económico.

Ilustración 14. Servicios de fraude relacionados con WhatsApp

Además de este caso, existen innumerables estafas como la aplicación **Whatsapp Plus** que prometía herramientas personalizadas, multitud de fondos y paletas de colores diferentes para las conversaciones y que, a principios de año, obligó al servicio oficial a bloquear todas las cuentas de los usuarios que se hubiesen descargado la aplicación falsa (según las estadísticas fue instalada en los teléfonos de más de 35 millones de usuarios). Se puede obtener información de este caso incluso desde la página oficial[7] de WhatsApp:

¿Por qué me han suspendido por el uso de WhatsApp Plus y cómo puedo revocar la suspensión?

WhatsApp Plus no es una aplicación autorizada por parte de WhatsApp. WhatsApp Plus no está asociado con WhatsApp y no apoyamos a WhatsApp Plus. WhatsApp no puede garantizar la seguridad de WhatsApp Plus y su uso puede poner en riesgo los datos personales y privados en tu teléfono móvil. Es posible que WhatsApp Plus comparta tu información con aplicaciones de terceros sin tu conocimiento o permiso.

Debes desinstalar esta aplicación y descargar una versión autorizada de WhatsApp desde nuestro sitio web o desde Google Play. Después de que termine el periodo de 24 horas de suspensión, podrás usar WhatsApp.

Ilustración 15. Preguntas frecuentes WhatsApp

3.8 ATAQUES DE PHISHING UTILIZANDO WHATSAPP WEB

WhatsApp Web es una extensión de la cuenta del teléfono móvil que permite usar la popular aplicación de mensajería desde cualquier equipo de sobremesa o portátil. Todos los mensajes enviados y recibidos estarán sincronizados entre los dispositivos, dando más libertad de uso a los usuarios.

[7] **Preguntas Frecuentes (Whatsapp.com):** https://www.whatsapp.com/faq/es/general/105

Para comenzar con su uso, tan solo hay que acceder a la dirección https://web.whatsapp.com y escanear el código QR que figura en la página con la aplicación del teléfono:

Ilustración 16. Inicio de sesión web

Con la falsa promesa de promociones exclusivas de grandes empresas o de descuentos en productos del momento, un posible atacante puede sugerir a la víctima escanear un código QR con su aplicación para acceder a estas ventajas, cuando en realidad está robando las credenciales de inicio de sesión.


```
"s":{
   "remember-me":"true",
   "WAVersion":"\"0.1.4391\"",
   "qwefsdafadsdf==":"false",
   "debugCursor":"146",
   "WAWamDimensionCache":"{\"AppVersion\":\"0.1.4391\",\"BrowserVersion\":\"Firefox 39.0\",\"DeviceName\":\"Linux
   x86_64\",\"WebcEnv\":0}",
   "WAToken2":"\"0.asldkamäsdflkasdfasdf\"",
   "WAWamLastRotate":"1439140177924",
   "WALangPref":"\"de-DE\"",
   "WAWamStatus":"\"completed\"",
   "y8fY/zQ8P+asdfadfg==":"[
     ...
   ]",
   "WAToken1":"\"asdf+ams,dfhlaskdjfhasdfasdf=\"",
   "Dexie.DatabaseNames":"[\"wawc\"]",
   "storage_test":"storage_test",
   "LKAJsdlksdjfasdf==":"false",
   "logout-
   token":"\"alkjsdhfkjashldkjpweoaLKNKASBkasjbdaksdjLKjhhndosiaosa;AljkhJKhlKAJShkljqjDJSAOlkjbnhasdklWAdm==\"",
   "ver":"1",
   "whatsapp-mutex":"\"x781239870495:init0.987123490234\"",
   "WASecretBundle":"{\"key\":\"sldkfjsdf+asdlfijlasdkjfasdf=\",\"encKey\":\"asldkfjasldkfjsdfsdf0=\",\"macKey\":\"a,
   sdfasdf+alskdjföalskdhiopasdf=\"}",
   "WABrowserId":"\"aö,ksdjflöasdf==\""
```


Ilustración 17. Credenciales de inicio de sesión

Para ello, el atacante monitoriza un código QR de la web oficial y, cuando el usuario piense que se está suscribiendo a alguna promoción cebo, estará autorizando el acceso web desde su sesión. En ese momento el atacante guardará las credenciales y datos de la sesión web almacenados en las cookies para posteriormente utilizarlos de nuevo y comprometer la sesión de la víctima utilizando el servicio web.

3.9 ALMACENAMIENTO DE LA INFORMACIÓN EN LA BASE DE DATOS

La base de datos de conversaciones, ficheros, mensajes, así como otros datos que maneja la aplicación, se almacena de forma local dentro del teléfono, independientemente de que se tenga la opción de "backup" en la nube activada en nuestro dispositivo.

Como se ha visto en apartados anteriores, WhatsApp utiliza SQLite para almacenar este tipo de información en la base de datos, por lo que si un atacante lograra hacerse con este fichero podría acceder a todas las conversaciones y datos privados del usuario. Por este motivo, y a pesar de que durante los primeros años de vida de la aplicación este fichero se encontraba sin cifrar, en la actualidad se encuentra protegido contra este tipo de casos.

Ilustración 18. WhatsApp Viewer

Durante los últimos años este cifrado se ha ido modificado, pretendiendo hacer la tarea de descifrado más complicada para posibles atacantes, añadiendo al fichero de base de datos la extensión .crypt más el número de versión de cifrado utilizado. En el momento de la escritura de esta guía, la versión actual de cifrado de la base de datos es **.crypt12**.

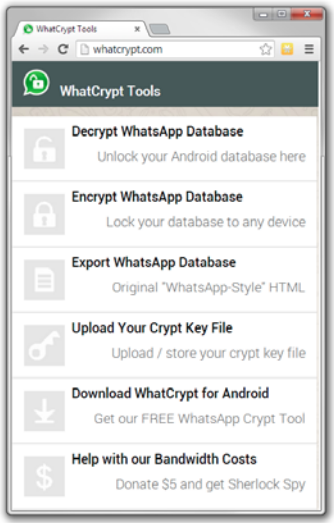


Ilustración 19. WhatsCrypt Tools

En función de la versión utilizada, existen multitud de aplicaciones[8] que permiten de una forma sencilla el descifrado de la información contenida, tanto en versión local para un equipo, como a través de una aplicación en el teléfono o interfaz web.

Para evitar que un atacante pueda tener acceso a toda la información privada que WhatsApp almacena en el teléfono hay que prestar especial

[8] **WhatCrypt:** http://whatcrypt.com/

atención a qué aplicaciones de terceros se instalan, así como el acceso físico de otra persona al terminal ya que, para cada versión de cifrado nueva publicada, las herramientas se actualizan para poder tratarlas correctamente.

3.10 INTERCAMBIO DE DATOS PERSONALES ENTRE WHATSAPP Y FACEBOOK

En el momento de la compra de WhatsApp por parte de Facebook, en febrero de 2014, los fundadores de la aplicación se apresuraron a asegurar que no existirían cambios dentro de la aplicación y que seguirían trabajando de forma independiente, indicando, a través de un post en el blog oficial que "*El respeto a su privacidad está codificado en nuestro ADN, y hemos construido WhatsApp en torno al objetivo de conocer un poco acerca de usted como sea posible.*"

Esta política ha sido mantenida por parte de la compañía hasta la modificación de sus términos y condiciones de uso el jueves 25 de agosto de 2016. El nuevo documento[9] indica una serie de cambios, incluyendo el que WhatsApp, a partir de entonces, transferirá los datos de sus usuarios a Facebook y el resto de compañías que Mark Zuckerberg posee para "actividades diversas".

A pesar de que los mensajes, fotos e información de perfil no serán objetivos a compartir, otra información como tu número de teléfono, contactos, hora de última conexión así como tus hábitos de uso de la aplicación serán compartidas con Facebook.

3.11 OTROS FALLOS DE SEGURIDAD ANTERIORES

Desde sus inicios, WhatsApp ha tenido que convivir con las críticas por la mala gestión de la seguridad de su aplicación. La falta de cifrado[10], por ejemplo, demostró que los datos intercambiados por los usuarios carecían de cualquier protocolo de seguridad. A efectos prácticos, cualquier persona podía acceder a los números de teléfono y al contenido de los mensajes enviados inicialmente a través de WhatsApp. Además, si estos se mandaron mientras estaba activado el GPS del dispositivo, los intrusos o ciberatacantes podían descubrir fácilmente la ubicación del usuario puesto que WhatsApp también almacena las coordenadas geográficas y las mantenía desprotegidas.

Para evitar este tipo de actividades por parte de posibles atacantes, WhatsApp ha evolucionado a lo largo de los años implementando diferentes sistemas de cifrado, desde el uso de una contraseña basada en el IMEI o dirección MAC de la tarjeta Wi-Fi del teléfono, pasando por el uso inseguro del algoritmo RC4, hasta llegar en la actualidad al sistema de cifrado extremo a extremo.

9 **https://www.whatsapp.com/legal/?l=es**

10 **WhatsApp Authentication: MD5 vs WAUTH-1 vs WAUTH-2**
http://www.seguridadofensiva.com/2014/06/whatsapp-authentication-md5-vs-wauth-1-vs-wauth-2.html

Por otro lado, y afectando a otra implementación de la aplicación, también apareció en Internet una página web (**WhatsAppStatus.net**) 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.

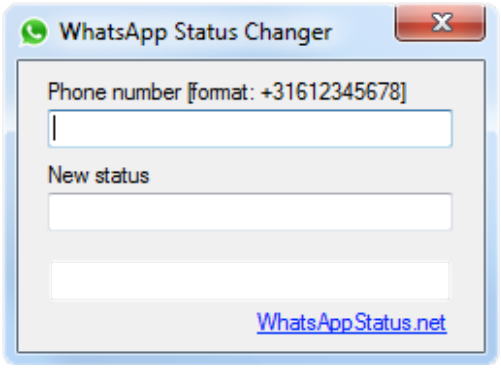


Ilustración 20. WhatsApp Status Changer

Ilustración 21. Vulnerabilidad Priyanka

Muchas son las vulnerabilidades y riesgos que ha albergado la aplicación desde su inicio, propiciando la expansión de gusanos, como el caso de **Priyanka**, capaz de expandirse entre los usuarios de *Android* con tan solo guardar un contacto en la agenda; hasta los diferentes riesgos que ha supuesto la insuficiente seguridad en los métodos de almacenamiento de información de las conversaciones desde el inicio, que se realizaba en texto claro.

4. RECOMENDACIONES ADICIONALES PARA TELÉFONOS MÓVILES

Además de los riesgos de seguridad que implica el uso de la aplicación, también será necesario adoptar una serie de precauciones para que la información de nuestros teléfonos quede a salvo de posibles criminales o programas dañinos.

Las siguientes recomendaciones ayudarán en esta tarea:

- Mantener el teléfono bloqueado. De esta forma se reducirá el riesgo si el teléfono cae en las manos equivocadas. Además, como se ha visto a lo largo de esta guía, será recomendable eliminar las previsualizaciones de los mensajes y extremar las medidas cuando no se disponga del teléfono al alcance, ya que con una simple llamada de teléfono se podría comprometer la seguridad de alguna sesión o aplicación que se esté utilizando.
- Hay que tener cuidado con el acceso y las solicitudes de permisos de las aplicaciones que se ejecuten en nuestro teléfono, especialmente cuando se trata de terminales *Android*.
- Conocer los riesgos que implica realizar "jailbreaking" o" rooting" del terminal, que a pesar de ser tentador para acceder a aplicaciones o servicios

específicos, puede comprometer y reducir considerablemente la seguridad del teléfono.

- Desactivar la conectividad adicional del teléfono cuando no se vaya a utilizar, como podría ser la conexión Wi-Fi o Bluetooth, ya que además de reducir el consumo de batería, reduce la posible superficie de ataque sobre el terminal.

5. REFERENCIAS

1. App Annie 2015 Retrospective: https://www.appannie.com/insights/market-data/app-annie-2015-retrospective/
2. WhatsApp Registration Flow: https://github.com/mgp25/Chat-API/wiki/WhatsApp-Registration-Flow
3. How to hack WhatsApp and Telegram:https://habrahabr.ru/company/pt/blog/283052/
4. SS7: https://es.wikipedia.org/wiki/SS7
5. SS7: Locate. Track. Manipulate : https://berlin.ccc.de/~tobias/31c3-ss7-locate-track-manipulate.pdf
6. SQLite: https://es.wikipedia.org/wiki/SQLite
7. Preguntas Frecuentes (Whatsapp.com): https://www.whatsapp.com/faq/es/general/105
8. WhatCrypt: http://whatcrypt.com/
9. WhatsApp Authentication: MD5 vs WAUTH-1 vs WAUTH-2 http://www.seguridadofensiva.com/2014/06/whatsapp-authentication-md5-vs-wauth-1-vs-wauth-2.html