¿Confiable y seguro?

Un vistazo a las potenciales vulnerabilidades de WhatsApp

Ignacio Espinosa
Carlos Guerra
María Paz Canales

@ | DERECHOSDIGITALES
Derechos Humanos y Tecnología en América Latina

Diagramación: Constanza Figueroa.
Ilustraciones: Andres Alaerkhon-Schiavi
Edición: Vladimir Garay.
Junio 2018.

DERECHOS DIGITALES
América Latina

Derechos Digitales es una organización independiente y sin fines de lucro, fundada en el año 2005 y cuya misión es la defensa, promoción y desarrollo de los derechos fundamentales en el entorno digital, desde el interés público. Entre sus principales ejes de interés está la defensa y promoción la libertad de expresión, el acceso a la cultura y la privacidad.

Introducción

¿Cuántas de nuestras interacciones sociales se realizan a través de aplicaciones de mensajería? ¿Cuán seguros nos sentimos al usarlas? ¿Cuán seguros debiéramos sentirnos? Todas estas preguntas se instalaron en las cabezas de los chilenos en Septiembre de 2017, cuando la prensa daba a conocer las primeras informaciones acerca de una operación de inteligencia realizada por Carabineros, en la cual se habría accedido al contenido de las comunicaciones de dirigentes de comunidades mapuches, realizadas a través de Whatsapp y Telegram. Hablamos de la denominada "Operación Huracán".

Nos llamó profundamente la atención que desde la prensa, los órganos de investigación judicial y el público en general se aceptara tan fácilmente que un servicio de inteligencia local tuviese la habilidad de vulnerar el cifrado de aplicaciones de mensajería que operan a lo ancho del mundo, transportando no solo mensajes familiares o amistosos, jocosos o cotidianos, sino que sirve también como un medio de comunicación para quienes viven en ambientes hostiles, de represión política, inmigración ilegal o persecusión religiosa. ¿Era plausible pensar que las habilidades de la policía chilena habían alcanzado un nivel inédito a escala mundial en la explotación de vulnerabilidades de las aplicaciones de mensajería?

El posterior desarrollo de la zaga ha mostrado que la versión de Carabineros de Chile habría sido, hasta cierto punto, falsa en los hechos. Sin embargo este episodio plantea preguntas importantes sobre las que vale la pena reflexionar: ¿Cuánto realmente sabemos acerca de la fortaleza del cifrado de las comunicaciones electrónicas y la seguridad que ese cifrado brinda al contenido de esas comunicaciones? ¿Cuánto realmente sabemos acerca de las capacidades de nuestras policías para vulnerar ese cifrado?

A contestar la primera de esas preguntas se abocó el equipo técnico de Derechos Digitales. La oscuridad que rodeaba el caso no permitía recabar elementos suficientes para contestar la segunda pregunta, que generó confusión y alarma entre organizaciones que, como la nuestra, están interesadas en la protección de la privacidad de las personas y la inviolabilidad de las comunicaciones, que a su vez permiten el ejercicio de otros derechos, como la libertad de expresión y el derecho a reunión.

Es por ello que en Derechos Digitales decidimos investigar, en base a las declaraciones, reportajes y referencias externas, las diferentes formas en las que teóricamente se puede acceder al contenido de las comunicaciones de Whatsapp. Aparentemente el cifrado de extremo a extremo no garantizaría en forma absoluta que el contenido de las conversaciones sea completamente protegido.

La información que a continuación presentamos tiene por objeto entregar elementos de análisis crítico respecto de potenciales ataques que intenten vulnerar la seguridad de las comunicaciones desarrolladas en Whatsapp. Estos antecedentes son útiles para usuarios en general, para ayudarles a despejar

hipótesis de sospecha respecto a potenciales ataques sufridos o el riesgo de sufrirlos, y cómo prevenirlos. Por otra parte, la información que aquí se comparte resulta útil para abordar de manera inicial una investigación periodística o judicial que implique la denuncia de hechos de intervención de comunicaciones electrónicas a través de Whatsapp.

Sobre el cifrado en las comunicaciones

En tiempos en que discutimos sobre la autenticación biométrica en servicios cotidianos (como tu teléfono celular o tu cuenta bancaria), sobre inteligencia artificial y los algoritmos avanzados usados para predecir qué contenidos queremos consumir, cobra más que nunca relevancia la pregunta sobre la seguridad y privacidad de los usuarios.

Los grandes proveedores de servicios digitales se han visto forzados a integrar más funciones de seguridad en sus plataformas y servicios. Un ejemplo es Whatsapp: la aplicación de mensajería adquirida por Facebook en 2014 y -actualmente- la más usada en el mundo, pasó de manejar sus comunicaciones de forma no cifrada a implementar protocolos de cifrado débiles y vulnerables, a finalmente establecer una alianza con Open Whisper Systems para incorporar el protocolo de cifrado de Signal en la aplicación y así permitir el cifrado de extremo a extremo entre usuarios. De esta forma se incrementa la protección de los mensajes enviados a través de la plataforma y se limita el acceso a los datos por parte de la empresa, bajo la premisa de que ni siquiera quienes trabajan en ella pueden leerlos.

Después de esta última mejora, parte de la comunidad de entrenadores de seguridad digital (particularmente en contextos de riesgo y/o de limitaciones tecnológicas y económicas) comenzó a recomendar Whatsapp como medio de comunicación seguro, comparándola con aplicaciones como Signal o Wire, debido a que comparten algoritmos de cifrado de extremo a extremo similares. Lo anterior parece una conclusión lógica, sin embargo, otra parte de la comunidad comenzó a resaltar algunos aspectos que podían hacer de Whatsapp una alternativa todavía insegura en ciertos casos:

- Es factible que existan vulnerabilidades en la aplicación, debido a la ausencia de estándares de seguridad en el diseño y desarrollo iniciales de Whatsapp.
- El modelo de código cerrado del software no permite auditar cómo están implementadas las medidas de seguridad de sus aplicaciones y servidores.
- El modelo de negocios de Facebook, la empresa detrás de Whatsapp, e basado en la entrega de publicidad y recopilación de datos de los usuarios para generar una mejor segmentación, con varios episodios negativos en términos de privacidad de sus usuarios.

Lo que sabemos hoy es que la transmisión de los mensajes entre usuarios de Whatsapp utiliza el protocolo Signal, el cual fue diseñado pensando en la seguridad: brinda cifrado de extremo a extremo (nadie en el camino de los mensajes podría leer su contenido); realiza la validación de participantes al contar con un sistema de generación de llaves de cifrado únicas por cada conversación que son verificables, y protege los mensajes en el tiempo, modificando las llaves de cifrado para cada mensaje de forma transparente para los usuarios (forward secrecy), dificultando aún más el compromiso de estos mensajes por parte de terceros.

Nuestra investigación sobre formas de vulnerar este protocolo arrojó que a la fecha no existen en el dominio público metodologías documentadas relevantes que planteen la vulneración del protocolo de cifrado, sino solo algunas en torno a las aplicaciones que lo implementan. En este sentido, seguimos nuestra exploración revisando la arquitectura de Whatsapp para entender mejor qué otras formas de vulneración resultan posibles.

Sobre la arquitectura de Whatsapp

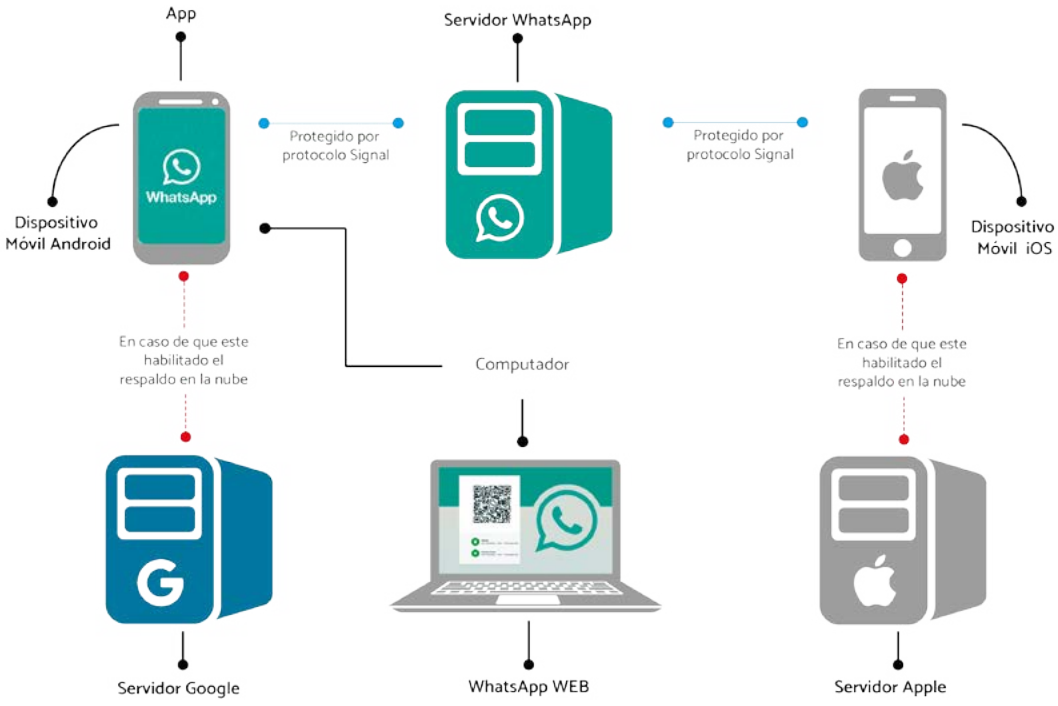

Figura 1

Para realizar nuestro análisis tomamos las diferentes partes que componen la infraestructura de Whatsapp e intentamos analizarlas una por una, en este caso consideramos:

- Whatsapp Web
- Computadora
- Equipo celular
- Aplicación de Whatsapp
- Servidor de Whatsapp
- Respaldos en la nube (iCloud/Google Drive en los casos que apliquen)

En el caso de explicaciones y pruebas en equipos móviles, usamos como referencia la arquitectura existente en Android; en nuestras investigaciones no utilizamos equipos con iOS, no implicando con ello que no sean vulnerables a los casos que describimos a continuación, sino que su potencial vulneración y sus detalles son desconocidos para nosotros al momento de esta publicación.

Vulnerar Whatsapp Web

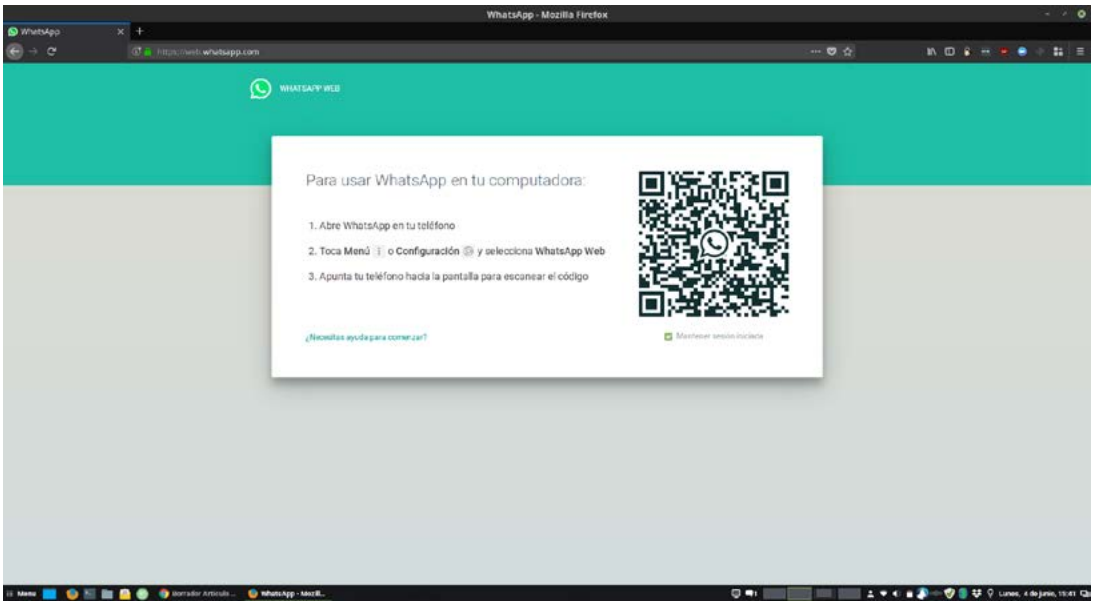

Figura 2

El principio de compromiso mediante esta herramienta es sencillo, si tomamos una computadora (en este caso de un atacante) e iniciamos una sesión en web.whatsapp.com, y luego afiliamos el equipo de la víctima, podremos utilizar Whatsapp desde la computadora y consultar mensajes y archivos multimedia, además de poder enviar mensajes legítimos a los contactos de

la víctima. Las barreras que existen para que este tipo de ataque sea exitoso serían:

- Hay que tener acceso físico al equipo y pasar el bloqueo de pantalla para poder afiliar el equipo de la víctima a la computadora del atacante.
- La afiliación del equipo hay que hacerla en la misma ubicación del equipo y la computadora, ya que esta se realiza mediante la pantalla de la computadora y la cámara del dispositivo móvil. Esto puede ser burlado con cierto nivel de sofisticación, sin embargo, el hecho de que el código QR de la herramienta web se actualiza cada cierta cantidad de segundos hace complicado el burlar la condición de cercanía de los equipos.

La afiliación del equipo móvil a Whatsapp web deja un rastro en el equipo de la víctima cuando busca las conexiones en menú-> Whatsapp Web. De tal forma, un usuario informado y proactivo puede constatar en su dispositivo si su cuenta ha sido afiliada a un equipo distinto al suyo.

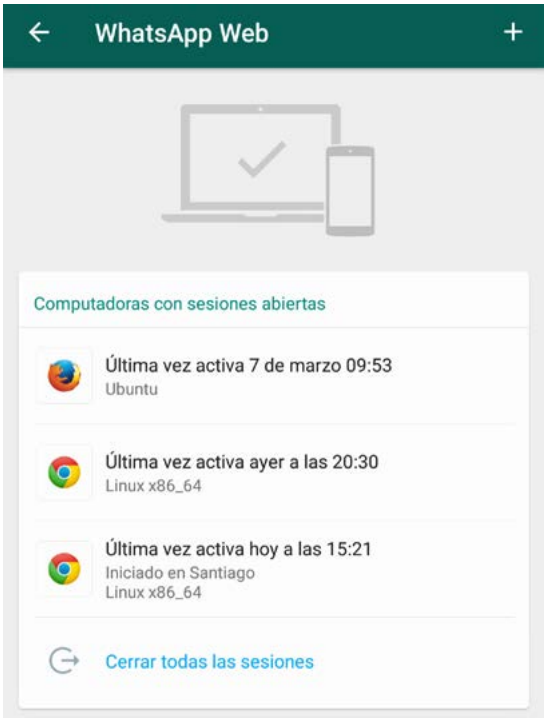

Figura 3

Vulnerar la forma en que funciona la aplicación

Figura 4

Una vez dentro del equipo celular, la aplicación de whatsapp almacena las conversaciones que son visibles al usuario en una base de datos cifrada localmente (usando un algoritmo de cifrado simétrico AES-256), una llave que descifra esta base de datos y los archivos multimedia que se incluyen en nuestras conversaciones sin cifrar. Cada vez que vemos en nuestros equipos un mensaje de texto en Whastapp estamos consultando esta base de datos, entonces si un atacante quiere obtener acceso a los mensajes almacenados en nuestros equipos bastará con obtener tanto la base de datos como la llave que la descifra. En caso en que solo necesite mensajes multimedia, bastará con obtener los archivos crudos, pues estos no se encuentran cifrados.

Sobre la base de datos (y respaldos en la nube)

La base de datos con nuestras conversaciones se encuentra en una zona desprotegida del almacenamiento de nuestro equipo y puede llegar a pesar una cantidad importante de Megabytes en el caso en que tengamos muchas conversaciones y no las borremos frecuentemente.

Esta base de datos se guarda en varios archivos por días, los que están construidos como bases de datos de SQLite adaptadas para manejar cifrado simétrico de una forma personalizada, por lo que acceder a estos archivos sin la llave de cifrado haría imposible poder consultar su contenido.

Además de estar almacenada en nuestro equipo para poder ser utilizada por la aplicación, si tenemos activados los respaldos de seguridad en la nube (Google Drive para Android y iCloud para iOS), estas bases de datos se copian en estos servicios para ser potencialmente restablecidos en el caso de un cambio de equipo o eliminación y reinstalación de la aplicación en nuestro teléfono.

Desde el punto de vista de un atacante, pueden haber varias formas de obtener esta base de datos de mensajes:

- Tomar control físico del dispositivo y extraer los archivos de forma sencilla. Sin embargo, además de acceso físico habrá que desbloquear la pantalla del dispositivo.
- Instalar un malware que extraiga de forma remota los archivos y los envíe al atacante. Para esta acción no es necesario acceso root o administrativo.

En el caso de que estas bases de datos estén respaldadas en la nube, se requeriría obtener acceso a la cuenta de usuario correspondiente (Google o iCloud) y extraer desde sus interfaces estos archivos. Esto puede lograrse mediante varias formas:

- Acceder físicamente a computadoras con sesiones previamente iniciadas.
- Obtener remotamente las credenciales de los servicios en la nube mediante phishing o spyware, y acceder manualmente o utilizar herramientas que descargan estos respaldos.

Sobre la llave de cifrado

A diferencia de la base de datos de mensajes, la llave de descifrado de esta base de datos se encuentra en una zona protegida del almacenamiento del dispositivo móvil, haciendo imposible su extracción en un caso de uso general. Esta zona protegida evita que un proceso diferente a la propia aplicación tenga acceso a ella, por lo que otras aplicaciones (incluido malware) no deberían poder acceder a la llave. Sin embargo, existen algunos casos de estudio en los cuales se indica que la llave sería posible de obtener:

- Si el equipo tiene habilitada la ejecución de programas con privilegios root, cualquier persona con acceso físico al equipo puede instalar una aplicación que use estos privilegios para acceder al área protegida en donde se encuentra la llave para poder extraerla y enviársela.
- Si el equipo tiene habilitada la ejecución de programas con privilegios root y es infectado con malware de forma remota, este último podría extraer la llave de cifrado y enviarla al atacante sin mayor problema.
- En algunos casos se ha podido comprobar que si en un equipo se instala manualmente una versión de Whatsapp anterior a la que permitía almacenar la llave en una zona protegida, esta versión genera la llave de cifrado en una zona desprotegida y con ello facilita su extracción. Sin embargo, para lograr esto habría que tener acceso físico al equipo y capacidad de manipularlo de forma extensiva para poder cambiar una aplicación existente. No obstante, al finalizar toda esta operación se puede volver a colocar la versión inicial de la aplicación, lo que hace no perceptible para el usuario su compromiso una vez vuelto a utilizar.
- En algunas pruebas realizadas de forma controlada, se ha comprobado que cuando se inicia Whatsapp en un segundo dispositivo móvil (en control del atacante), en éste se genera una llave de cifrado que en la mayoría de las pruebas descifró exitosamente bases de datos obtenidas desde el dispositivo original de la víctima. Lo anterior sugiere que la llave de cifrado es constante en el tiempo para el mismo usuario (en este caso para cada número telefónico), lo cuál explicaría porqué las bases de datos cifradas

pueden ser usadas en los respaldos en la nube, y pueden ser exitosamente importadas en nuevos dispositivos a pesar de no tener en estos las llaves de cifrado de los dispositivos que crearon las bases de datos respaldadas. Este tipo de ataque requeriría obtener las bases de datos a descifrar previamente por cualquiera de las vías descritas anteriormente, además de acceso a los mensajes SMS de la víctima para poder recibir el código de confirmación de Whatsapp en el segundo dispositivo en el que se inicia la aplicación con el número de la víctima. Esta técnica también genera que el dispositivo de la víctima se desvincule de su cuenta Whatsapp y tenga que volver a iniciarlo, sin embargo, para este momento ya la llave de cifrado pudo haber sido capturada por el atacante. Para el usuario esto es perceptible bajo la forma de un mal funcionamiento de la aplicación que debiera llamar su atención (coloquialmente las personas se referirán a una "desconfiguración" de Whatsapp).

Sobre los archivos multimedia

En cuanto a las fotografías, notas de voz, videos y archivos en general que se reciben a través de Whatsapp, estos son protegidos en la comunicación entre usuarios por el protocolo Signal, de la misma forma que los mensajes escritos. Sin embargo, en el almacenamiento interno del equipo pueden ser encontrados fácilmente sin ningún tipo de cifrado en el área desprotegida de almacenamiento, por los que las técnicas antes descritas para obtener la base de datos aplican por igual para los archivos multimedia, con la fundamental diferencia de que no es necesario obtener la llave de cifrado de la base de datos para poder consultarlos.

En cuanto a los respaldos de seguridad, estos también almacenan los archivos multimedia sin ningún tipo de cifrado, haciendo este tipo de información particularmente vulnerable a extracciones simples desde cuentas en la nube asociadas.

Vinculaciones con la Operación Huracán

En el espacio de tiempo en que la Operación Huracán fue objeto de investigación periodística y judicial, se mencionaron muchas técnicas (incluyendo algunas contradictorias entre sí o técnicamente inviables) a través de las cuales se habría producido el monitoreo de mensajes de Whatsapp por parte de la unidad de inteligencia de Carabineros involucrada en la operación.

La mayor parte de las técnicas inicialmente informadas son incompatibles con los hallazgos de esta investigación, en cuanto a formas de compromiso de la seguridad de las comunicaciones desarrolladas a través de Whatsapp. Lo anterior sugiere que muchas de las hipótesis manejadas, incluyendo las capacidades asignadas al supuesto software "Antorcha" (cuya existencia a la fecha no ha sido acreditada), no son sostenibles a nivel técnico.

No obstante lo anterior, llamamos la atención respecto a que sobre la base de la información que se hizo pública durante el proceso de investigación, algunas declaraciones arrojan información de relevancia consistente con las hipótesis técnicas abordadas en este trabajo de investigación.

En primer lugar, destaca la recurrente mención a ataques de phishing (a través de enlaces enviados por correo electrónico) a las cuentas de Google de las víctimas, lo que permite deducir que estas tenían habilitados los respaldos de conversaciones en Google Drive, correspondiendo este tipo de ataque a una de las técnicas explicadas más arriba para obtener las bases de datos cifradas de las víctimas. De ser lo anterior efectivo, los archivos asociados a las conversaciones pudieron ser fácilmente obtenidos, pero en el caso de los mensajes escritos (algunos de los cuales fueron incluso publicados en medios) tal contenido solo habría podido ser accedido si el atacante contaba con la llave que permitía descifrar estas bases de datos. A continuación ensayamos algunas hipótesis, con sus consideraciones, de cómo ello podría haber ocurrido:

Se tuvo acceso físico a los equipos, sin embargo, esta hipótesis habría que dividirla en dos escenarios alternativos distintos:

- Hubo acceso a los equipos luego de los arrestos. Hipótesis que no es útil para explicar la obtención previa de los mensajes que llevaron a la atribución de los delitos supuestamente cometidos y que motivaron las órdenes de aprehensión de los imputados.
- Hubo acceso físico previo a los dispositivos por parte de los cuerpos de seguridad. En este escenario habría sido necesario adicionalmente que fuera posible desbloquear la pantalla de los dispositivos, y luego instalar versiones de Whatsapp antiguas o habilitar la ejecución de programas como root para hacer la extracción de las llaves de cifrado. Lo anterior, aunque posible, requiere un episodio de intervención física importante en los dis-

positivos afectados, que de haber ocurrido habría constituído un acceso ilegítimo desde el punto de vista de la persecución penal, pues no se habría producido amparada por una orden de un juez de garantía.

No se tuvo acceso físico previo a los equipos, sin embargo, se habilitaron equipos secundarios para realizar la extracción de la llave de cifrado. Esto resultaría más viable en términos que evita la intervención física de los equipos de las víctimas. Sin embargo, esta hipótesis requiere que ocurran dos circunstancias: que las víctimas no notaran que su Whatsapp "se desconfiguró" y que no llamara su atención el que hayan tenido que vincularlo de nuevo a su número telefónico; y aún más importante, que la agencia de inteligencia encargada de la operación tuviera acceso remoto a los mensajes de texto de las víctimas en el momento en que se vincularon los dispositivos secundarios a los números de teléfono de las víctimas, para poder generar las llaves de cifrado correspondientes a las cuentas objetivo. Nuevamente esta última hipótesis implicaría que habría tenido lugar un acceso ilegítimo desde el punto de vista de la persecución penal, pues no se habría producido amparada por una orden de un juez de garantía.

En suma, según las técnicas revisadas y descritas en este trabajo, no habría sido posible acceder al contenido de las comunicaciones de los mensajes de texto transmitidos a través de la aplicación Whatsapp por los comuneros mapuches, blanco de la Operación Huracán, sin realizar actividades ilegales que violan garantías procesales tales como la exigencia de autorización judicial previa de un juez de garantía para la realización de diligencias de investigación que implican la afectación de derechos fundamentales garantizados por la Constitución Política de la República.

Adicionalmente, de comprobarse (lo que no se ha hecho hasta ahora, en nuestro conocimiento) que alguna de la acciones recién descritas fueron efectivamente llevadas a cabo, podría llegar a configurarse un delito informático tipificado por la Ley Nº19.223, ya que la víctima habría sido objeto de un ataque informático para obtener credenciales personales (a través de los ataques de phishing) de acceso a su servicio de mensajería, y se habría concretado un acceso no autorizado a equipos informáticos (con fines de espionaje).

Todo lo anterior no solo resulta preocupante en el caso concreto, si no que lo es aún más en la perspectiva de la señal de desapego de la legalidad de las policías u otras ramas de las Fuerzas Armadas que cuentan con unidades de inteligencia. Ello teniendo en consideración que ya en 2015 desde Derechos Digitales informábamos acerca de la compra a Hacking Team de software de espionaje por la Policía de Investigaciones de Chile, y que adicionalmente habrían existido más organismos nacionales interesados en su adquisición, incluyendo al Ejército y la Armada. La PDI solicitaba software espía principalmente para

sistemas Android, utilizando URL maliciosas que redirigen a portales de venta al detalle (como Dafiti, Falabella, Ripley) o de cupones de descuento (Groupon).[1]

En este sentido, debe tenerse en cuenta que la Organización de Estados Americanos (OEA) ha expresado que "[r]esulta preocupante que la legislación en materia de inteligencia y seguridad haya permanecido inadecuada frente a los desarrollos de las nuevas tecnologías en la era digital. Preocupan de manera especial los efectos intimidatorios que el acceso indiscriminado a datos sobre la comunicación de las personas pueda generar sobre la libre expresión del pensamiento, búsqueda y difusión de información en los países de la región".2

Pretender enterrar hoy todo lo sucedido durante el desarrollo de la Operación Huracán fundado en la afirmación reciente de los involucrados en ella de que los antecedentes técnicos originalmente proporcionados son en realidad falsos3 debiera movernos a un sano escepticismo como ciudadanos y como activistas de derechos humanos. Lo cierto es que los antecedentes muestran intentos, exitosos o no, de utilizar tecnología de vigilancia con fines ilícitos acorde de nuestro ordenamiento jurídico y los estándares internacionales. Dejar desatendidas tales capacidades en desarrollo por parte de la policía y servicios de inteligencia nos pone en el severo riesgo de que estas encuentren espacio para aprender de esta fallida operación y perfeccionarse en el futuro.

Conclusiones y Recomendaciones

Después de realizar esta corta investigación, comprobando las técnicas disponibles para vulnerar las comunicaciones de Whatsapp, contrastando los hallazgos con la información disponible sobre el caso de la Operación Huracán, y teniendo en consideración además cómo éste fue cubierto por la investigación de prensa y judicial, notamos que existe una fuerte desinformación sobre la seguridad que Whatsapp ofrece tanto a nivel de los usuarios en general, como incluso en las comunidades de activismo digital y de seguridad de la información.

Este tipo de desinformación se intensifica dado el hecho de que Whatsapp es de código cerrado y es difícil comprobar exactamente cómo son las imple-

1 *Ver reporte completo https://www.derechosdigitales.org/wp-content/uploads/HACKINGTEAMChile.pdf*

2 *Relator Especial de las Naciones Unidas (ONU) para la Protección y Promoción del Derecho a la Libertad de Opinión y de Expresión y Relatora Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos de la OEA. "Declaración Conjunta sobre Programas de Vigilancia y su Impacto en la Libertad de Expresión en Línea." https://www.oas.org/es/cidh/expresion/showarticle.asp?artID=926&lID=2*

3 *Ver https://www.fayerwayer.com/2018/06/carabineros-antorcha-engano/*

mentaciones de su tecnología en comunicaciones, servidores y dispositivos de usuario, haciendo necesario recurrir a la ingeniería de reversa para entender sus vulnerabilidades reales, haciendo más difícil su detección, difusión y corrección.

En el caso puntual de la Operación Huracán, con la información pública disponible no es posible determinar a ciencia cierta si alguna de las hipótesis técnicas de vulneración de las comunicaciones aquí descrita tuvo lugar. Sin embargo, con la poca información disponible, el acceso efectivo a comunicaciones de Whatsapp de los dirigentes mapuches blanco de la operación revelaría prácticas de los organismos de inteligencia y un proceder de la fuerza de seguridad pública abiertamente ilegales y de exceso de atribuciones en el uso de tecnologías de vigilancia, que es incompatible con el respeto de los derechos humanos garantizados por nuestra Constitución.

Como iniciamos señalando en este informe, más allá del caso concreto de la fallida Operación Huracán, resulta relevante que existen algunas medidas posibles de implementar por cualquier usuario de Whatsapp, que apuntan a evitar estos escenarios de riesgo identificados. Estas prácticas cobran particular relevancia para todos aquellos que, por su trabajo vinculado a activismo social, protección de derechos humanos o investigación periodística, se encuentran particularmente expuestos a convertirse en blanco de ataques, ya sea agentes del estado o privados que busquen impedir su acción.

Tales recomendaciones pueden resumirse en la forma siguiente:

- Evitar usar Whatsapp para comunicaciones sensibles. A la fecha de esta publicación, se recomienda Signal como alternativa,
- No habilitar los respaldos en la nube del historial de conversaciones.
- Borrar frecuentemente las conversaciones del equipo celular.
- Comprobar frecuentemente qué equipos están afiliados a Whatsapp Web en su dispositivo móvil (ver figura 3).
- No tener habilitada la posibilidad de ejecución de programas con privilegios root en los teléfonos Android, en el caso de iOS investigar sobre los aspectos similares que pueden afectar la seguridad de la aplicación.
- Mantener bloqueos de pantalla en los dispositivos móviles lo más difíciles de vulnerar posibles, como contraseñas largas o con factores biométricos.
- No desatender los equipos móviles en ningún momento. Por ejemplo, entrega en custodia para acceder a algún recinto o sala de reuniones.
- No cargar los dispositivos móviles en computadoras, especialmente si no son de confianza.
- No instalar aplicaciones ni abrir enlaces de dudosa procedencia o confianza.


DERECHOSDIGITALES
Derechos Humanos y Tecnología en América Latina