Inseguridad en el uso de Mensajería Instantánea: WhatsApp vs Telegram

Ing. Alejandra Di Gionantonio[12], Ing. Laura del Carmen Ligorria[13], Ing. Roxana María Manera[14], Ing. Lorena Peralta[1,5], Ing. Luis Contrera[1,6], Mairena Di Gionantonio[17]

[1]UTN Facultad Regional Córdoba
{[2]ing.alejandradg, [3]liuniversidad, [4]roxanamanera, [5]peralta.lorenas.d, [7]mairenadg}@gmail.com,
[6]contluis@hotmail.com

RESUMEN

Como consecuencia del avance de la tecnología, el uso de aplicaciones de Mensajería Instantánea (MI) fue evolucionando hasta convertirse hoy en día en una herramienta de comunicación masiva. El empleo de la misma conlleva el incremento de incidentes de seguridad que la hacen cada vez más vulnerable. El concepto de MI se encuentra en continua evolución como su propagación.

El objetivo de este trabajo es investigar y analizar los rasgos distintivos de dos herramientas de MI más utilizadas en estos tiempos: WhatsApp y Telegram, y los diversos ataques que pueden presentarse en su aplicación, a los fines de identificar las vulnerabilidades existentes y establecer el grado de inseguridad en la información sensible de los usuarios.

Palabras claves: *WhatsApp, Telegram, Mensajería Instantánea, vulnerabilidad.*

CONTEXTO

El presente trabajo se encuentra inserto en el marco del proyecto "*Vulnerabilidad en aplicaciones de mensajería instantánea: WhatsApp – Telegram".*

El mismo es coordinado y acreditado por la Universidad Tecnológica Nacional – Facultad Regional Córdoba, dentro de la cual opera el Laboratorio de Investigación de Software (LIS), perteneciente al Departamento de Ingeniería en Sistemas de Información.

1. INTRODUCCIÓN

En una época donde la MI está desplazando a otros medios de comunicación tradicionales como el correo electrónico o la mensajería SMS, algunas aplicaciones se destacan por ser las más extendidas en el mundo y utilizadas por millones de personas en distintas plataformas: WhatsApp y Telegram [1]

Esto delinea una evolución determinada por la Tecnología disponible, la cual siempre ha sido impulsada por la necesidad imperante de la comunicación. [2]

En este escenario, la inmediatez y la conectividad son los aspectos más valorados a la hora elegir un servicio de mensajería y son precisamente las características que ofrece la mensajería instantánea (MI). Actualmente la MI permite establecer comunicación entre dos o varias personas, basadas en texto y audio. La inmediatez de estas herramientas y el uso de la tecnología en todos los ámbitos de nuestra vida, hacen que este tipo de comunicación sea el más utilizado en el siglo XXI. [3]

Sin embargo, las continuas transformaciones producto de los constantes avances de la tecnología y las condiciones de uso de la misma, presentan un conflicto entre la importancia de la comunicación digital y la falta de seguridad en las aplicaciones de mensajería instantánea existentes hasta la fecha. [4]

En virtud de lo expuesto surge la necesidad de realizar este trabajo investigativo a fin de proporcionar un análisis de las vulnerabilidades de las dos aplicaciones de MI mencionadas anteriormente.

Se trata de plataformas que al poder tener un comportamiento semejante al de una red social convencional son propensas a su expansión. Además, el uso compartido de la información personal y la escasa percepción

de riesgo que los usuarios tienen con la seguridad las han convertido en un entorno atractivo para intrusos y ciberatacantes que intentan obtener datos e información de sus usuarios con relativa facilidad.
Uno de los fallos más comunes en las aplicaciones de MI es la forma que utilizan para borrar las conversaciones almacenadas en el teléfono, ya que 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 siendo accesible por técnicas forenses. Esto resulta beneficioso para los servicios de inteligencia de los gobiernos para poder investigar y resolver actos delictivos. Sin embargo en Telegram existe la opción de configurarlo en modo secreto o punto a punto para que no realice la copia de la conversación en el servidor de la nube.[5]
También, hay que tener en cuenta las implicaciones cuando se tenga activa la opción de copia de seguridad (almacenando una posible conversación ya borrada) que podría ser recuperada en un futuro.
Durante el establecimiento de conexión con los servidores, se puede intercambiar información sensible acerca del usuario, quedando expuesta a cualquiera en el caso de utilizar redes WiFi públicas o de dudosa procedencia. [6]

2. LÍNEAS DE INVESTIGACIÓN Y DESARROLLO

La línea de investigación en la cual está circunscripto el presente trabajo es la Seguridad Informática en la Mensajería Instantánea, ya que la misma se ha convertido en el primer objetivo de los ciberdelincuentes para perpetrar cada una de sus estafas.

Para el desarrollo de este trabajo se aplicará el Método Empírico a partir del cual se puede obtener conocimiento basándose en la observación de la realidad. [7], [8]

También se realizará un análisis cualitativo, que permite hacer uso de las “percepciones”, es decir, las “cualidades” del mundo desde las representaciones de los sujetos con las aplicaciones de MI, por lo que es útil en la exploración de cómo o por qué las cosas han ocurrido. [9]

Desarrollo

En el ámbito de MI, las dos aplicaciones estudiadas en este trabajo son empleadas tanto por usuarios particulares para estar en contacto con amigos o familiares como por empresas y organizaciones para poder establecer contacto con clientes.

Ambas aplicaciones son "igual de seguras" al usuario, en cuanto a la protección de sus conversaciones personales, porque las dos tienen unos protocolos de cifrado de extremo a extremo muy similares, que les impide ver los mensajes privados. Cualquier llamada (o envío de mensajería) realizada con las aplicaciones, incluyendo si es al extranjero, está cifrada de extremo a extremo para que ningún tercero pueda escucharla o verla y no puedan ser intervenidas de ninguna manera, ya que ni la aplicación, ni el servidor ni el proveedor de datos conoce la clave de cifrado, que es creada por el propio dispositivo.

En referencia a lo anterior, se debe mencionar que la aplicación de WhatsApp integró el cifrado de extremo a extremo automáticamente para todas sus conversaciones y en aplicaciones propietarias. Por su parte, los usuarios de Telegram pueden crear activamente "chats secretos", en los que todos los mensajes se cifran de extremo a extremo como ya se explicó precedentemente. [10].

WhatsApp y Telegram notifican a los usuarios en cada pantalla de chat que existe cifrado de extremo a extremo para los mensajes, pero no reflejan si la conversación fue autenticada. En Telegram, una vez que la pantalla de chat contiene un mensaje, el mensaje cifrado de extremo a extremo desaparece. [11]. Ver

Figura 1

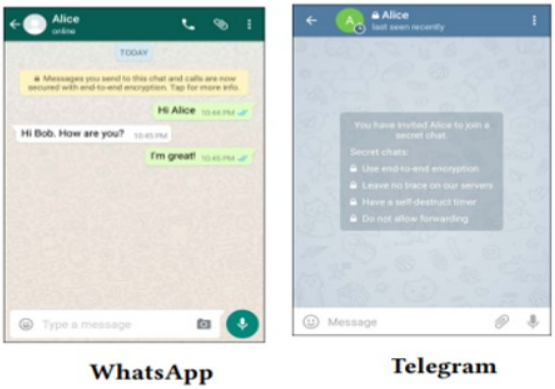

Figura 1: Mensajes e indicadores de cifrado de extremo a extremo en las dos aplicaciones.

A continuación se describirán algunas de las amenazas más recurrentes efectuadas en las aplicaciones de MI mencionadas.

Amenazas comunes

Media File Jacking

Según el equipo de Modern OS Security de Symantec, centrada en la protección de terminales móviles y sistemas operativos, la información de medios de WhatsApp y Telegram puede ser expuesta y manipulada por ciberatacantes.

La falla de seguridad, denominada "Media File Jacking", afecta a WhatsApp en Android de forma predeterminada, y a Telegram en Android si ciertas funciones están habilitadas. Se debe a que transcurre el tiempo entre el momento en que los archivos multimedia recibidos a través de las aplicaciones se escriben en el disco y cuando se cargan en la interfaz de usuario de chat (IU) de las aplicaciones para que los usuarios las consuman. Este lapso de tiempo crítico presenta una oportunidad para que los actores malintencionados intervengan y manipulen los archivos multimedia sin el conocimiento del usuario.

Si se explota la falla de seguridad, un atacante malintencionado podría hacer un mal uso y manipular información confidencial, como fotos y videos personales, documentos corporativos, facturas y notas de voz. Los atacantes pueden aprovechar las relaciones de confianza entre un remitente y un receptor al usar estas aplicaciones de MI para beneficio personal o para causar daño.

Recibir un enlace que es falso

El mismo podría llegar incluso de parte de un contacto en el que se confía, como puede ser un amigo o un familiar. Puede que esa persona haya sido atacada previamente y esté enviando enlaces sin ser consciente de ello. También se puede materializar cuando el usuario recibe links que lo conectan a una supuesta página para iniciar sesión en redes sociales o realizar una compra en plataformas como Amazon, etc. Generalmente suele ser algo atractivo para el usuario, una súper oferta que haga que la víctima cliquee en el enlace y posteriormente ponga sus datos para poder visualizar el contenido.

Archivo que es un malware

Otro ataque del que hay que estar atentos es de un posible archivo que en realidad es malware. Aunque este servicio de mensajería cuenta con filtros para evitar que sea sencillo enviar virus, lo cierto es que es posible que un documento pueda saltarse esa medida de seguridad y termine por llegar a la víctima.

Ha habido virus de WhatsApp como ZooPark o Tizi que se distribuyen a través de una imagen o un archivo que nos envían por esta aplicación.

Secuestrar WhatsApp

Es un tipo de ciberataque cuyo objetivo es conseguir robar dinero de la víctima y posteriormente continuar con su entorno es decir su lista de contactos. Esto se logra cuando se tiene el control de la cuenta y para devolverla se exige la realización de una transferencia de dinero, además se puede complicar la situación si el atacante interviene en conversaciones personales y fotos privadas. Para producir este ataque el ciberdelincuente solo necesita un Smartphone y la aplicación instalada en él, de esta manera puede enviar un mensaje diciendo que ha enviado un código por error y que la víctima se lo vuelva a pasar.

Otra forma es a través de las publicaciones que se realizan en avisos de

ventas en páginas web y de las redes sociales de productos o servicios. El atacante realiza una reactivación sobre la cuenta de la víctima, en base a esto la víctima recibe un mensaje con el código de verificación para activar su cuenta de WhatsApp y en pocos segundos le llegará un supuesto amigo o contacto solicitando dicho código porque acaba de cambiar su móvil y como no pudo vincular el número con su cuenta en la aplicación pensó en usar el número de la víctima para conseguir el número de verificación. Al enviarle el código el atacante pasa a tener el control de la cuenta pudiendo ver las conversaciones por WhatsApp y todos sus contactos.

Como la aplicación solo se puede utilizar en un único dispositivo, la víctima no podrá acceder a ella desde su móvil. Luego el atacante le solicitará una suma de dinero si quiere que le devuelva el control de su cuenta. [12] Ver **Figura 2**

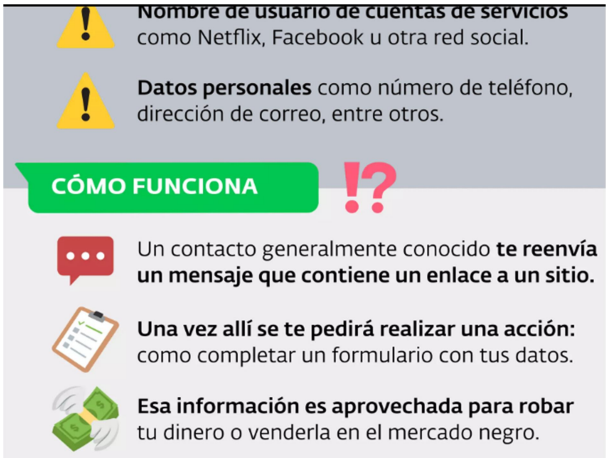

Figura 2. Phishing en WhatsApp.

Telekopye: Bot de Telegram ayuda a los ciberdelincuentes a cometer estafas en plataformas online de compraventa

Investigadores de ESET analizan Telekopye, un bot de Telegram que facilita la creación de contenido falso para plataformas de compraventa online y es usado por un grupo bien organizado y jerarquizado que sale a la caza de sus víctimas a las que llaman mamuts. Se trata de un conjunto de herramientas que se implementa como un bot de Telegram que, cuando se activa, proporciona varios menús fáciles de navegar en forma de botones.

Aplicaciones troyanizadas de Telegram distribuyen el código espía BadBazaar entre usuarios de Android

Los investigadores de ESET han identificado dos campañas activas dirigidas a usuarios de Android, donde los actores de amenazas detrás de la herramienta se atribuyen al grupo APT (Advanced Persistent Threat) GREF, alineado con China. Probablemente activas desde julio de 2020 y julio de 2022, las campañas distribuyeron el código de espionaje de Android BadBazaar a través de Google Play Store, Samsung Galaxy Store y sitios web dedicados que representan las aplicaciones maliciosas Signal Plus Messenger y FlyGram. Los actores de la amenaza parchearon las apps de código abierto Telegram para Android con el código malicioso que identificaron como BadBazaar. [13]

Aplicaciones troyanizadas de WhatsApp y Telegram roban billeteras de criptomonedas

El equipo de investigación de ESET descubrió docenas de sitios web que se hacían pasar por Telegram y WhatsApp apuntando principalmente a usuarios de Android y Windows con versiones troyanizadas de estas aplicaciones de mensajería instantánea. La mayoría de las aplicaciones maliciosas que identificaron son clippers, un tipo de malware que roba o modifica el contenido almacenado en el portapapeles (en inglés clipboard). Todos estos clippers buscan robar los fondos de las víctimas, y varios apuntan a las billeteras de criptomonedas. Esta es la primera vez que se observa el uso de clippers para Android disfrazados como apps de mensajería instantánea. Además, algunas de estas aplicaciones utilizan el reconocimiento

óptico de caracteres (OCR) para reconocer el texto de las capturas de pantalla almacenadas en los dispositivos comprometidos, que es otra novedad para el malware de Android. [14]

3. Resultados obtenidos/esperados

La propagación de amenazas informáticas por medio de MI se ha vuelto muy popular en los últimos tiempos, por la alta concentración de usuarios. En torno a las aplicaciones de MI, los ataques son diversos y con distintos grados de impacto en cuanto a la vulnerabilidad de los usuarios.

Los ataques comunes por WhatsApp y Telegram pueden poner en riesgo la seguridad. Es importante que siempre se establezcan medidas, se mantenga el sentido común, se usen programas de seguridad y se tenga todo actualizado para evitar vulnerabilidades. [15]

Este trabajo tiene una incidencia directa en los usuarios de aplicaciones de MI, ya que como resultado del proceso de investigación, se generó un compendio de las posibles amenazas en cuestión de seguridad que se manifiestan en el uso de las dos aplicaciones de MI estudiadas. Los resultados de este análisis proporcionarán información de interés para las personas y organizaciones que utilicen estas aplicaciones de MI para sus necesidades de comunicación.

4. Formación de Recursos Humanos

El equipo de trabajo está conformado por docentes-investigadores pertenecientes a la carrera de grado de Ingeniería en Sistemas de Información.
El grupo está compuesto por una Directora, una Co-Directora, tres ingenieros investigadoras de apoyo, y una estudiante aspirante a incorporarse a la carrera de investigador. Este proyecto enriquecerá la experiencia en la carrera de investigador de los integrantes del mismo.

5. Bibliografía

[1]Juano, Antonio. “Criptografía y Seguridad en WhatsApp”. 01 de Mayo de 2017. Book. DOI:10.13140/RG.2.2.23555.09764 Disponible en: https://www.researchgate.net/publication/316601633_Criptografia_y_Seguridad_en_WhatsApp

[2]García Pablo et al CACIC 2000
Disponible: http://sedici.unlp.edu.ar/handle/10915/23324

[3] Research on the Secure Communication Model of Instant Messaging

[4]CIBER SUCESOS Vol. Nº 11 Junio/2021 www.csirt.gob.cl - página nro. 6.

[5]CCN-CERT IA-23/17: Riesgos de uso de Telegram. Centro Criptológico Nacional. Pp 5-6, Sept. 2017.

[6] CCN-CERT BP/01: Principios y recomendaciones básicas en Ciberseguridad. “Informe de buenas prácticas”. Centro Criptológico Nacional. Pp 31-33. Marzo 2021

[7] B. Kitchenham, O. Pearl Brereton, D. Budgen, M. Turner, J. Bailey, and S. Linkman, “Systematic literature reviews in software engineering – A Systematic literature review,” Inf. Softw. Technol., vol. 51, no. 1, pp. 7–15, Jan. 2009, DOI: 10.1016/j.infsof.2008.09.009.

[8] A. Islas, M. Perea de la Fuente, J. Figueroa Velázquez, “Métodos empíricos de la investigación parte 1” Universidad Autónoma del Estado de Hidalgo. Enero-Junio 2020. Disponible en: https://www.uaeh.edu.mx/docencia/P_Presentaciones/icea/asignatura/mercadotecnia/2020/metodos-empiricos.pdf

[9] Pablo Sánchez Kohn, “Métodos de investigación: Qué son y cómo elegirlos”.
Disponible en:
https://www.questionpro.com/blog/es/metodos-de-investigacion/

[10] Josefina Quevedo González. 2017. “Investigación y prueba del ciberdelito”. Tesis: Programa de Doctorado en Derecho y Ciencia Política. - Línea de Investigación: Derecho procesal. Universitat de Barcelona. Disponible en: https://dialnet.unirioja.es/servlet/tesis?codigo=230669

[11] Amir Herzberg and Hemi Leibowitz. 2017. “Can Johnny Finally Encrypt? Evaluating E2E-Encryption in Popular IM Applications”. In Proceedings of, Los Ángeles, CA, USA, December 05 2016 (STAST ’16), 12 pages. https://doi.org/http://dx.doi.org/10.1145/3046055.3046059

[12] Pacheco Veliz, Sebastián Exequiel – Piazza Orlando, Carlos Damián. 2016. “Estudio y análisis de seguridad en dispositivos móviles. BYOD y su impacto en las organizaciones``. Tesina de Licenciatura. Universidad Nacional de La Plata. Facultad de Informática. Disponible en: http://sedici.unlp.edu.ar/bitstream/handle/10915/58591/Documento_completo

[13]Lukas Stefanko. “Welivesecurity”. 01 Sep 2023
Disponible:
https://www.welivesecurity.com/es/investigaciones/troyanizadas-telegram-signal-espia-badbazaar-usuarios-android/

[14]Lukas Stefanko. “Welivesecurity”. 16 Marzo 2023
Disponible: https://www.welivesecurity.com/la-es/2023/03/16/aplicaciones-troyanizadas-whatsapp-telegram-roban-billeteras-criptomonedas/?utm_source=responsys&utm_medium=email&utm_content=WLS%20Spanish%20-17-03-2023&utm_campaign=wls_newsletter

[15]https://www.redeszone.net/noticias/seguridad/4-ataques-whatsapp-infectar-movil/