Telegram: especialistas afirman que no es seguro y no protege a sus usuarios

09/04/2022

Desde su aparición, miles de usuarios afirmaban que Telegram era seguro y que la protección que ofrecía a sus usuarios era confiable y superaba ampliamente las expectativas. Pero según indicaron investigadores, su seguridad no sería tan eficiente como lo muestra.

Junto a WhatsApp, Telegram es una de las aplicaciones de mensajería más utilizadas y populares, pero dos estudios presentados en el marco del evento de ciberseguridad RootedCON 2022 y que ofrecen opciones para incrementar la seguridad, analizaron la aplicación y aspiran a romper los mitos de la seguridad con la que Telegram asegura contar.

Lo confirmaron el fundador de la compañía especializada en criptografía y protección de datos CriptoCert, Alfonso Múñoz, y el jefe de Evaluaciones Tecnicas en el departamento New Markets de Telefonica CyberTech, Pablo San Emeterio.

Por su parte, WhatsApp y Telegram afirman que desconocen el contenido de las conversaciones de sus usuarios gracias al cifrado punto a punto. La primera lo implementó en 2016 y, la segunda, fue creada con este cifrado.

El fundador de Signal, Moxie Marlinspike, criticó a Telegram por, según sus palabras, guardar la información que recopila del usuario en texto plano y no usar la encriptación de punto a punto por defecto (e2ee), sino que ofrece la posibilidad de crear ‘chats secretos’, que emplea un protocolo e2ee «dudoso».

En su ponencia durante la conferencia sobre ciberseguridad, Muñoz explicó que, sin embargo, la mayor parte de la

información y ficheros intercambiados en Telegram solo tiene cifrado cliente-servidor, lo que permite a la aplicación conocer la mayor parte de la información que se intercambia en ella.

Este ponente también hace alusión a los denominados chats secretos de Telegram que su servidor almacena en ficheros cifrados. Esta técnica permite de igual manera a la app conocer datos como qué personas se intercambian dichos ficheros, cuándo lo hacen, su tamaño y el nombre de estos.

Dentro de este contexto, la criptografía involucrada en las comunicaciones en tránsito no puede ser vulnerada sin la colaboración de la compañía. En este caso, Muñoz destaca que gran parte de la seguridad de Telegram se basa en la confianza depositada sobre la propia plataforma.

Fuente: Ámbito