Publicado en el 28/04/2014

INTECO descubre un fallo de seguridad en la autenticación de usuarios de Telegram

INTECO ha llevado a cabo un análisis minucioso del diseño del protocolo que la plataforma de mensajería Telegram emplea para autenticar a los usuarios, es decir, el modo en el que éstos se identifican para acceder al servicio.

La conclusión es clara: se trata de un fallo de seguridad en el que un atacante podría ser capaz de interceptar la información enviada por los usuarios sin que éstos sean conscientes de que está ocurriendo.

El problema se debe a que Telegram posibilita que cualquier persona que emplee la plataforma de mensajería pueda crear versiones de su aplicación y utilizar los servicios que proporcionan a través de sus servidores. En Telegram se incluye una clave pública que permite a la aplicación del usuario asegurarse de que se está comunicando con la plataforma oficial. Pero como el programa lo puede desarrollar cualquier persona, un atacante malicioso podría modificar esa clave, y suplantar, por tanto, a los servidores de Telegram, interceptando las comunicaciones que el usuario envíe o reciba.

INTECO ha hecho público este análisis tras la investigación y correspondiente notificación oficial al servicio Telegram.

Datos de contacto:
INTECO

Nota de prensa publicada en:

Categorías: Ciberseguridad

https://www.notasdeprensa.es