WhatsApp, Telegram ou Signal peuvent être piratés malgré le chiffrement des messages

	WhatsApp, Telegram ou Signal peuvent être piratés malgré le chiffrement des messages

Si les messageries mobiles se renforcent grâce à un dispositif de chiffrement, un hackeur a trouvé le moyen de récupérer l'intégralité des messages en clair.

Avec un chiffrement de bout-en-bout, les messages sont normalement sécurisés. Cela permet d'éviter les attaques de type man-in-the-middle, et par ailleurs, même le prestataire de service n'est pas en mesure de prendre connaissance du contenu de ces échanges. Pourtant, il existe un moyen de contourner ces dispositifs. La société Ability a partagé ses exploits en vidéo avec le magazine Forbes.

Concrètement, la faille se trouve au sein du système de signalisation n° 7 (SS7), un ensemble de protocoles de signalisation téléphonique. C'est le réseau principal permettant de connecter les réseaux téléphoniques entre eux. C'est également lui qui établit des relations entre le téléphone d'un utilisateur et le réseau, par exemple les tonalités d'appel après une numérotation ou de mise en attente ou encore le renvoi vers la messagerie.

Téléchargez WhatsApp Le hackeur fait ainsi croire au SS7 qu'il dispose du même numéro de téléphone que celui de la victime. Il est ensuite en mesure d'installer l'application WhatsApp ou Telegram puis de recevoir le code secret permettant d'authentifier son smartphone.

sécurité security banner gb

Dès lors, le hackeur peut récupérer l'historique des conversations synchronisées et se faire passer pour la victime. De son côté, cette dernière recevra un message l'avertissant que son compte est utilisé autre part. L'application sera donc déconnectée et l'identité de la victime… usurpée.

Puisque le SS7 est un réseau global utilisé par les opérateurs téléphoniques à travers le monde, celui-ci n'appartient vraiment à personne. Cela signifie que la vulnérabilité n'a pas été corrigée et le processus semble pour l'heure compliqué. Autant dire qu'il s'agit d'une porte ouverte pour les agences de renseignement.

Voici la procédure en vidéo :

Article original de Guillaume Belfiore

Réagissez à cet article

Original de l'article mis en page : WhatsApp, Telegram ou Signal peuvent être piratés malgré le chiffrement des messages