Sécurité IT : Telegram affectée par une faille 0-Day selon Kaspersky

L'app de messagerie instantanée chiffrée **Telegram**, d'origine russe, était affectée par une faille 0-Day (« Zero-Day »). Celle-ci était susceptible d'être exploitée par des pirates et cybercriminels.

Repérée par **Kaspersky**, la vulnérabilité a été colmatée sur la version desktop de Telegram, mettant les utilisateurs hors de danger.

L'éditeur de solutions antivirus (également d'origine russe) avait détecté une faille inconnue de l'outil de messagerie instantanée, qui était utilisée pour télécharger sur l'ordinateur des utilisateurs du codes malveillant.

Selon les découvertes des chercheurs de Kaspersky Lab, cette faille a notamment été utilisée pour « miner » des crypto-monnaies (Monero, Zcash et Fantomcoin) sur les ordinateurs infectés en détournant la puissance de calcul informatique.

En outre, une porte dérobée (backdoor) était aussi installée, permettant aux cybercriminels d'envoyer des commandes via l'API Telegram pour obtenir l'accès distant aux machines infectées et y installer des spyware (outils d'espionnage).

Plus troublant : les chercheurs signalent dans leur contribution blog qu'ils ont repéré sur un des serveurs utilisés pour les attaques des archives contenant les messages chiffrés volés aux utilisateurs.

Telegram utilise en effet un cache local chiffré pour conserver l'historique des discussions et c'est le contenu de ce cache qui était dérobé via la faille de la messagerie.

Ce qui interpelle les chercheurs, c'est que ce contenu étant chiffré, il est normalement inexploitable. Il n'y a donc en théorie aucun intérêt à le dérober.

Des analyses sont en cours pour essayer de déterminer l'identité des auteurs de ce détournement et leurs objectifs.

Depuis sa sortie en 2013, Telegram est critiquée par une communauté de chercheurs, qui reprochent aux créateurs de l'app de ne pas publier en open source le protocole de chiffrement et qui soupçonnent cette approche propriétaire de masquer les déficiences de l'implémentation.

Créée par les frères Nikolaï et Pavel Dourov (à qui l'on doit le réseau social VKontakte, le Facebook russe), la messagerie **Telegram** est réputée pour ses communications chiffrées.

Inventée à l'origine pour échapper à l'emprise du gouvernement russe et du FSB (ex-KGB) sur toutes formes d'échanges, elle est devenue populaire auprès des hacktivistes, des défenseurs des droits de l'Homme et des journalistes.

Plus globalement, l'app sécurisée est présentée comme un rempart pour contourner les risques de censure d'Etat. Revers de la médaille : elle est aussi pointée du doigt par les forces de police

engagées dans la lutte anti-terroriste comme un canal de communication privilégié par l'Etat Islamique.

En phase d'ICO pour assurer son développement (voir article d'ITespresso.fr), Telegram revendique une communauté de 170 millions d'utilisateurs actifs.

(Photo credit: Desiree Catani on Visualhunt / CC BY-NC-SA)