

Une faille de sécurité de WhatsApp a été utilisée pour installer un logiciel espion via un appel manqué



WhatsApp a annoncé avoir corrigé une faille de sécurité. Il était possible d'espionner l'ensemble de l'activité d'un téléphone mobile par le biais d'un simple appel. Plusieurs ONG veulent porter plainte contre l'éditeur du logiciel incriminé, NSO group, une société israélienne.

Avec Atlantico
Rédaction

Une importante faille de sécurité sur la fonction appel téléphonique de WhatsApp a été corrigée ce lundi 13 mai. Un logiciel espion est au cœur de cette révélation. Les pirates informatiques ont installé à distance un logiciel de surveillance sur les téléphones et d'autres appareils en utilisant une vulnérabilité de l'application WhatsApp.

Difficile à détecter, cette faille de sécurité ne pouvait être identifiée que par des équipes très qualifiées. Cette faille a été exploitée afin d'installer des logiciels espions Pegasus, de l'entreprise israélienne NSO Group.

WhatsApp, détenue par Facebook, a indiqué que l'attaque visait un "nombre restreint d'utilisateurs". Elle a été orchestrée par "un cyber-acteur avancé". Un correctif a été apporté vendredi dernier.

L'attaque aurait été initiée par la société de sécurité israélienne NSO Group, selon un rapport publié par le [Financial Times](#).

WhatsApp a donc incité ce lundi ses 1,5 milliards d'utilisateurs à mettre à jour leurs applications par mesure de précaution. WhatsApp se présente pourtant comme une application de communication "sécurisée", les messages étant chiffrés.

Selon les récentes révélations, le logiciel de surveillance aurait laissé un attaquant lire les messages sur le périphérique de la cible. Les assaillants auraient utilisé la fonction d'appel vocal de WhatsApp afin de faire sonner l'appareil de la cible. Même si l'appel n'était pas pris, le logiciel de surveillance serait installé, selon le *Financial Times*. WhatsApp a précisé à la *BBC* que son équipe de sécurité avait été la première à identifier la faille. Elle avait partagé cette information avec des groupes de défense des droits de l'homme ainsi que le département américain de la Justice.

WhatsApp a communiqué ce lundi en publiant un document d'information dédié aux journalistes.

"L'attaque a toutes les caractéristiques d'une entreprise privée qui travaillerait avec les gouvernements pour fournir des logiciels espions qui prendraient en charge les fonctions des systèmes d'exploitation pour téléphones mobiles".

Le groupe NSO est une société israélienne qui a été qualifiée par le passé de "cyber-revendeur d'armes". Cette entreprise appartient

à la société Novalpina Capital, selon des précisions de la *BBC*. Le logiciel de NSO, Pegasus, permet de collecter des données personnelles à partir d'un périphérique cible, notamment de capturer des données à travers le microphone et la caméra et de récupérer des données de localisation.

WhatsApp a déclaré qu'il était trop tôt pour savoir combien d'utilisateurs avaient été affectés par cette vulnérabilité. Les attaques présumées ont été très ciblées.

Ce mardi, un tribunal de Tel-Aviv doit se pencher sur une pétition menée par Amnesty International qui demande au ministère de la Défense israélien de révoquer la licence du groupe NSO lui permettant d'exporter ses produits.