

WhatsApp piraté : 3 choses à savoir pour échapper au virus Pegasus

Quel est la nature de la faille de WhatsApp ?

La vulnérabilité touche la fonction d'appel voix. Elle engendre un dépassement de capacité mémoire, que la victime décroche ou non.

« Un certain nombre de personnes » ont effectivement été visées, dans le cadre d'une attaque hyperciblée, déclare WhatsApp. Et [d'ajouter](#) : « *Tout pousse à dire que l'assaut est le fait d'une entreprise privée à la solde de gouvernements* ».

Selon [Lookout](#), expert en sécurité du mobile, il s'agit d'un logiciel de surveillance mobile baptisé Pegasus découvert en...2016. Destiné à l'origine à iOS, il est devenu multiplateforme en 2017.

« À en croire le [Financial Times](#), la société en question se nomme NSO Group. D'origine israélienne, elle vend sa technologie Pegasus – présentée comme capable de prendre le contrôle de presque tout smartphone – aux forces de l'ordre et aux agences de renseignement. » [indique](#) ITespresso.

Quels sont les effets de Pegasus ?

Pegasus permet d'accéder à l'ensemble des données du téléphone (contacts, SMS, emails, photos, etc.), d'activer le micro et la caméra sans que l'utilisateur ne s'en aperçoive pour l'espionner à distance.

Il a été identifié notamment sur plusieurs milliers de téléphones de personnes à "haut potentiel" dans de grandes entreprises financières et industrielles.

Comment se protéger de Pegasus ?

Le code malveillant de Pegasus est quasiment différent pour chaque téléphone mais globalement, la méthodologie d'attaque reste la même.

Une mise à jour est disponible sur App Store pour les iPhone et sur Google Play pour les smartphones motorisés par Android.

Ultime conseil, qui vaut pour toutes les mises à jour de logiciels : ne jamais installer une version d'une application mobile disponible en dehors de ces deux plateformes « officielles ».

