AGENCE NATIONALE DES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION

Centre d'Alerte et de Réponse et
Aux Incidents de Sécurité Informatique

NATIONAL AGENCY FOR INFORMATION AND COMMUNICATION TECHNOLOGIES

Computer Incident Response Team

ALERTE DE SECURITE

Faille de sécurité dans Whatsapp et le virus Pegasus

Contenu

I. Contexte 3
II. Fonctionnement 3
III. Comment se protéger ? 4

I. Contexte

Une faille dans l'application de messagerie WhatsApp, dont Facebook est la maison mère, a permis à des pirates informatiques d'installer un logiciel espion sur des téléphones, a admis les responsables de WhatsApp.

Cette faille dévoilée par des chercheurs, a permis aux pirates informatiques d'insérer le logiciel PEGASUS sur des téléphones de près 1,5 milliard de personnes dans le monde. La société NSO Group qui édite des logiciels d'espionnage indexée dans cette propagation affirme que ce logiciel avait été mis au point pour des besoins de sécurité. Ce logiciel à travers un simple clic sur un lien permet de siphonner toutes les données du mobile (contacts, SMS, emails, photos, etc.) et d'activer le micro et la caméra sans que l'utilisateur ne s'en aperçoive. Au départ conçu pour iOS, il est devenu multiplateforme en 2017.

NSO Group a rapidement réagi dans un communiqué en affirmant que sa technologie est commercialisée par l'intermédiaire de licences à des gouvernements dans le seul objectif de combattre la criminalité et le terrorisme.

II. Fonctionnement

Le code malveillant de Pegasus est quasiment différent pour chaque téléphone mais globalement, la méthodologie d'attaque reste la même. Le modus operandi est le suivant : la cible reçoit un message de WhatsApp, avec un lien de confirmation. Si vous cliquez, vous ouvrez l'accès à Pegasus.

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

Pegasus est un logiciel espion à la base pour Apple iOS qui a pour but de collecter des informations et de permettre un accès aux appareils touchés. La mise à jour iOS 9.3.5, publiée le 25 août 2016, a supprimé les vulnérabilités exploitées par Pegasus. Néanmoins, au moment de la découverte, 97 % des appareils iOS étaient vulnérables.

Le logiciel est fabriqué par la société israélienne NSO Group, sous contrôle majoritaire de la firme britannique Novalpina Capital. Sa vente est approuvée par le ministère israélien de la Défense3. Ce logiciel est controversé car si les contrats stipulent une utilisation strictement légale de cette technologie (enquêtes criminelles comme celle qui a mené à l'arrestation du baron de la drogue El Chapo), il est utilisé par des agences de renseignements de dictatures. Il infecte des téléphones dans 45 pays et est utilisé par une trentaine de gouvernements, notamment le Bahreïn, le Kazakhstan, le Maroc, les Émirats arabes unis. Au Mexique, où le gouvernement a payé 80 millions de dollars pour en faire l'acquisition, il a servi à suivre le journaliste mexicain Javier Valdez, assassiné en 2017, et au moins huit autres journalistes, ainsi que l'a démontré The Citizen Lab de l'université de Toronto dans une série d'articles. En Arabie

Saoudite, il a servi à espionner divers activistes, notamment un confident de Jamal Khashoggi en octobre 2018.

III. Comment se protéger ?

- Une mise à jour de Whatsapp est disponible sur App Store pour les iPhones 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, PlayStore ou AppStore.