Non, Telegram, WhatsApp et autre Viber ne sont pas inviolables

L'offensive lancée par Bernard Cazeneuve contre le chiffrement vise avant tout les messageries proposant du chiffrement de bout en bout. A commencer par Telegram, le service qu'ont cofondé deux frères d'origine russe (Pavel et Nicolay Durov) en Allemagne. Comme d'autres applications similaires, comme WhatsApp ou Viber, Telegram permet d'envoyer gratuitement des messages chiffrés de bout en bout à n'importe quel autre utilisateur du service (sur iOS, Android, Windows Phone, PC, Mac OS X). Ces messages peuvent également s'effacer après une certaine durée, des deux côtés de la communication. Dans ce mode (secret chat), Telegram affirme ne pas être en possession des moyens permettant de décoder les données transitant sur ses serveurs. D'où l'initiative de Bernard Cazeneuve qui, conjointement avec son homologue allemand, vient d'appeler l'Union européenne à écrire une directive forçant les sociétés éditrices de ces logiciels à déchiffrer les messages transitant sur leurs infrastructures dans le cadre d'enquêtes judiciaires. Une exigence qui reviendrait, par définition, à modifier leurs systèmes de chiffrement pour y introduire une backdoor ou une clef maître permettant de décoder tous les échanges.

Mais, ce qu'oublie de préciser le ministre français et son homologue allemand Thomas de Maizière, c'est que le chiffrement de bout en bout que proposent Telegram et consorts n'est pas une garantie absolue de confidentialité. Car il faut bien utiliser l'application en question sur un terminal donné. Et que ce dernier n'est, par définition, jamais 100 % sûr.

Pegasus soigne les messageries chiffrées

La semaine dernière, la mise au jour du malware Pegasus, vendu à des gouvernements par une société israélienne nommée NSO, a montré que les messageries chiffrées pouvaient également être espionnées. Selon l'analyse (PDF) de la société Lookout et du Citizen Lab (une émanation de l'université de Toronto), Pegasus serait en mesure d'espionner Telegram, WhatsApp et Viber. Si la version de ce spyware analysée par Lookout semble se cantonner à la récupération de la base de données de Telegram, elle assure par contre l'interception de divers types de communication (dont les appels vocaux) dans WhatsApp et Viber.

Bien entendu, l'emploi d'un outil de type Pegasus nécessite de piéger le téléphone de la cible, par exemple en l'amenant à cliquer sur un lien infectieux. Par ailleurs, la version du spyware de NSO analysée par les chercheurs en sécurité repose sur trois failles zero day d'iOS qu'Apple a comblées depuis. Il n'en reste pas moins que la mise au jour de Pegasus illustre l'existence de sociétés très discrètes – de type NSO – vendant à des Etats (le plus souvent) des outils d'espionnage efficaces y

compris contre les technologies réputées bien sécurisées. La société NSO ne se limite d'ailleurs pas à iOS. « *Notre offre couvre les systèmes d'exploitation les plus populaires et propose une solution de monitoring chirurgical à l'usage exclusif des gouvernements, forces de l'ordre et services de renseignement* », se vante la très discrète société israélienne dans une brochure.

Macron, Montebourg, Fillon aussi sur Telegram

Au passage, l'intérêt de NSO pour Telegram devrait aussi susciter quelques interrogations dans la classe politique française, visiblement elle aussi de plus en plus séduite par Telegram. Comme le raconte *Le Canard Enchaîné* de la semaine dernière, plusieurs candidats à la primaire, à droite ou à gauche, ont succombé aux charmes de la messagerie chiffrée : Arnaud Montebourg, Benoît Hamon et François Fillon. Emmanuel Macron, le ministre de l'Economie qui démissionne du gouvernement pour avoir les mains libres en vue de la future présidentielle, est lui aussi un adepte. Tout comme la conseillère spéciale de Bernard Cazeneuve, Marie-Emmanuelle Assidon, utilisatrice depuis longtemps de l'application, toujours selon l'hebdomadaire satirique.

A lire aussi :

Après les attentats, la messagerie chiffrée Telegram met (un peu) d'ordre

Sécurité : Telegram, une vulnérabilité qui prête à discussion

Crédit photo : Denys Prykhodov / Shutterstock