

La messagerie Olvid mise sur la sécurité pour concurrencer Signal

La bataille des applications de messagerie bat son plein sur fond d'enjeux sécuritaires. La jeune pousse parisienne Olvid, lancée en 2019, met en avant son aspect "plus sécuritaire" pour contre-barrer Signal. Des arguments critiqués par certains experts.

Temps de lecture : minute

15 juin 2021

En janvier dernier, WhatsApp reculait sur sa nouvelle politique de partage des données renforcée avec la maison mère Facebook par peur de voir ses utilisateurs et utilisatrices fuir vers sa concurrente Signal, jugée plus sécuritaire. Mais une autre startup, française cette fois-ci, avance également cet argument. L'application parisienne Olvid, fondée en 2019, se décrit comme "l'app de messagerie instantanée la plus sécurisée au monde". Son innovation: la suppression de l'annuaire centralisé d'utilisateurs, censé permettre une sécurisation maximale des conversations. Une solution critiquée par certains experts.

Supprimer l'annuaire d'utilisateurs

Si la plupart des applications de messagerie instantanée sont chiffrées "de bout en bout" , c'est-à-dire qu'elles appliquent un algorithme de chiffrement sur des données pour les rendre inintelligibles en cas d'interception des messages par un attaquant, elles sont également composées d'un serveur qui recense tous les utilisateurs, ce qui rend vulnérable la confidentialité des métadonnées d'une conversation. Dans ce cas, "vous faites confiance à un serveur tout puissant qui distribue les identités numériques, les clés de chiffrement" et qui peut savoir "qui parle à qui, quand et à quelle fréquence" , explique Cédric Sylvestre, cofondateur d'Olvid. "Nous, on a supprimé cet annuaire qui représente un vrai problème de sécurité. C'est la première fois au monde que deux individus peuvent entrer en contact sans faire confiance à un serveur quelque part sur la planète et aux personnes qui l'administrent" , assure-t-il.



À lire aussi

#Sécurité : Newmanity lève 800 000 euros pour développer sa messagerie éthique et durable

"Olvid permet d'avoir un très haut taux de sécurisation en matière de non-compromission de vos échanges, qu'il n'y a pas sur Signal ou WhatsApp" ou Telegram, application russe sous les feux de la rampe et donc plus susceptible d'être attaquée, témoigne Franck DeCloquement, expert en intelligence stratégique.

En septembre 2020, l'application a reçu une "certification de sécurité de premier niveau" par l'Agence nationale de la sécurité des systèmes d'information (Anssi).

Aucune application n'est à l'abri d'un hacker

Pourtant, pour plusieurs experts, Olvid n'est pas la réponse ultime en matière de sécurité, pour plusieurs raisons. Tout d'abord, *"il n'y a pas d'application qui ne puisse pas se faire hacker donc il n'y a pas d'application qui soit la meilleure au monde"*, tempère Baptiste Robert, hacker éthique fondateur de Predicta Lab. Ensuite, *"Olvid est encore trop petit pour se vanter d'être l'application la plus sécurisée"*, estime-t-il. Alors que Signal et WhatsApp ont amassé des millions d'utilisateurs sur plusieurs années, *"Olvid n'a que 25 000 utilisateurs quotidien, peu d'expérience et le passage d'une échelle à l'autre est extrêmement compliqué"*, détaille le hacker. Enfin, le code d'Olvid n'est pas en Open source, c'est-à-dire fermé aux audits. *"Avant de pouvoir attester de la fiabilité d'une application, il faut être sûr que l'entité qui produit la messagerie et qui la code n'a pas fait d'erreur"*, déclare Jérôme Saiz, expert indépendant en protection des entreprises et fondateur d'OPFOR Intelligence.

Aux mises en garde des experts, le co-fondateur d'Olvid, Cédric Sylvestre, répond que son application n'est pas hackable puisque "*15 000 attaquants tentent de la hacker depuis un an, en vain*". Il assure que la sécurité de l'application est garantie grâce à la force de son "*moteur cryptographique*", qui serait en mesure d'héberger beaucoup plus d'utilisateurs si leur nombre devait exploser. Et il promet que le code de l'application sera publié "*prochainement*".

Bien que l'innovation d'Olvid soit saluée sur le marché, Signal reste la référence pour bon nombre experts. En effet, malgré l'annuaire centralisé de Signal, il faut que le destinataire accepte de recevoir un message pour que l'expéditeur ait accès à ses données personnelles. Le niveau de sécurité est donc considéré comme supérieur à celui de WhatsApp.

Article écrit par Maddyne, avec AFP