28/04/2025

La messagerie instantanée Signal est-elle "compromise", comme Elon Musk l’affirme ?

La messagerie instantanée Signal est-elle “compromise”, comme Elon Musk l’affirme ?

Mini polémique dans le milieu du chiffrement. Elon Musk a affirmé que l’application de messagerie Signal, connue pour ses outils de protection de la vie privée, avait des « failles » qui la rendait dangereuse. Signal serait-elle moins sécurisée que l’application le prétend ? C’est en tout cas ce que semble penser Elon Musk qui a publié un message sur son réseau social X pour affirmer que le service de messagerie instantanée avait des « failles connues » et jamais corrigées. De quoi jeter le doute sur l’intégrité de l’application bien connue, surtout que le message du milliardaire faisait suite à la publication d’un article accusant à demi-mot la fondation Signal (qui édite le logiciel) de collaborer avec les services de l’état américain. Quelques jours plus tard, c’est Pavel Durov, le PDG de l’application concurrente Telegram, qui se permettait de mettre en doute la sécurité de Signal. Dans un message publié sur son application, le responsable explique que les choix techniques faits par la structure derrière Signal ne permettent pas de s’assurer de la réelle confidentialité des messages échangés sur la plateforme. Mais alors, qu’en est-il vraiment ? Elon Musk contredit par la communauté Signal, en plus d’être une application de messagerie instantanée, est aussi un protocole de chiffrement à part entière. Open source, il est utilisé dans de nombreux autres logiciels, dont WhatsApp et Skype. De par sa nature ouverte, l’algorithme a été audité par bon nombre de spécialistes en chiffrement qui n’ont, d’après un audit effectué en janvier 2024, pas trouvé les fameuses « failles » mentionnées par Elon Musk. La sécurité de Signal a d’ailleurs longtemps été saluée par des grands noms du numérique comme Edward Snowden… et Elon Musk en 2021. La Commission européenne a aussi adopté Signal pour protéger ses communications depuis 2020. Ces faits ont d’ailleurs été rappelés par Meredith Whittaker, PDG de Signal qui, dans un long message en réponse à Musk, explique que « une large communauté de chercheurs et chercheuses en cybersécurité examine attentivement chaque mise à jour et passe au peigne fin chacun de nos fichiers » pour justement s’assurer qu’aucun bout de code malveillant ne s’est glissé dedans. Ce contexte a d’ailleurs été rappelé sous le message d’Elon Musk via les fameuses « Notes de la communauté ». Les “compilations reproductibles”, preuves bancales Les doutes émis par le PDG de Telegram sont eux d’une autre nature et plus précis : il s’attaque à la question des « compilations reproductibles » de Signal. Principe important de sécurité, ce concept pose l’idée qu’en compilant soi-même le code d’une application open source on devrait obtenir exactement la même signature cryptographique que celle publiée par l’éditeur lui-même. Une manière de s’assurer qu’aucun bout de code n’a été injecté au moment de mettre l’application en ligne. Pavel Durov explique donc que, contrairement à Telegram, Signal ne permet pas de faire des compilations reproductibles sur son appli iOS. Preuve que Signal aurait quelque chose à cacher. La réalité est pourtant plus compliquée que ça. En raison de la manière dont Apple publie ses applications sur son AppStore (chacune passant par un processus de chiffrement), il est impossible de comparer les signatures d’une application téléchargée et d’une application compilée en local. Sur Android, Signal passe sans problème l’épreuve des compilations reproductibles en revanche.

Signal

Riche en fonctionnalités Open source Sécurisée Signal est une application de messagerie instantanée unique, offrant un chiffrement de bout en bout pour protéger les messages échangés sur sa plateforme. Préférée par les utilisateurs soucieux de préserver leur vie privée et d'éviter l'exploitation de leurs données, elle est totalement gratuite et sans publicité. Disponible sur Android, iOS, ainsi que sur PC (Windows, Mac et Linux), Signal peut être utilisée de manière complémentaire sur différents appareils pour une communication sécurisée et respectueuse de la confidentialité. Signal est une application de messagerie instantanée unique, offrant un chiffrement de bout en bout pour protéger les messages échangés sur sa plateforme. Préférée par les utilisateurs soucieux de préserver leur vie privée et d'éviter l'exploitation de leurs données, elle est totalement gratuite et sans publicité. Disponible sur Android, iOS, ainsi que sur PC (Windows, Mac et Linux), Signal peut être utilisée de manière complémentaire sur différents appareils pour une communication sécurisée et respectueuse de la confidentialité.
https://www.clubic.com/actualite-526578-la-messagerie-instantanee-signal-est-elle-compromise-comme-elon-musk-l-affirme.html