Signal hacké ? Cellebrite éteint la mèche qu'il avait allumée

Cellebrite a-t-il hacké Signal ? Demandez à Edward Snowden ! Ce dernier a en tout cas son avis sur la question. Et il est tranché : il n'y a pas de hack qui tienne.

L'entreprise israélienne s'en était pourtant vantée la semaine dernière. Dans un billet largement édulcoré depuis*, elle affirmait : « Déchiffrer les messages et les pièces jointes envoyées avec Signal était impossible… jusqu'alors ».

Suivait une démonstration faite d'analyses de code en cascade, menant tour à tour au déchiffrement des messages, puis des pièces jointes. Démonstration qui, en y regardant de plus près, présente bien des prérequis.

> *Si jamais, les contributeurs de Signal en ont parlé sur Github. Pour résumer : Cellebrite part du principe qu'ils ont l'accès root (Donc accès aux données privées des apps + la clé Android Keystore) et à partir de là c'est déjà game over pour n'importe quel app, Signal ou autre*
>
> *— Soladev □□□□ (@iSoladev) December 15, 2020*

Signal qui monte

Le créateur de Signal le confirme : dans la configuration présentée, Cellebrite aurait tout simplement pu ouvrir l'application et lire les messages.

> *This (was!) an article about « advanced techniques » Cellebrite uses to decode a Signal message db... on an *unlocked* Android device! They could have also just opened the app to look at the messages.*
>
> *The whole article read like amateur hour, which is I assume why they removed it.*
>
> *— Moxie Marlinspike (@moxie) December 11, 2020*

> *No, Cellebrite cannot decrypt Signal communications. What they sell is a forensic device cops connect to insecure, unlockable phones to download a bunch of popular apps' data more easily than doing it manually. They just added Signal to that app list. That's it. There's no magic.*
>
> *— Edward Snowden (@Snowden) December 15, 2020*

Qu'en penser ? Comme le suggèrent certains, que Signal a pris suffisamment d'importance pour que Cellebrite s'y intéresse. La Commission européenne en recommande tout du moins l'usage à son personnel pour la communication avec le public. Quant à Mozilla, il l'encense dans son

comparatif des applications qui incluent une composante visioconférence.

> *I guess the big brain take is that Signal has become important enough for people like Cellebrite to care about.*
>
> *— Matthew Green (@matthew_d_green) December 10, 2020*

** Il est désormais simplement question d'une « aide aux forces de l'ordre pour accéder légalement à l'application Signal ».*

Illustration principale © signal.org