

# Chiffrement : comment la messagerie Signal échappe à la censure

L'organisation à but non lucratif Open Whisper Systems a indiqué mercredi avoir ajouté à son application de messagerie chiffrée Signal une fonctionnalité de contournement de la censure. Elle est disponible sous Android et, bientôt, sous iOS. Il suffit de mettre à jour l'application pour en bénéficier.

Signal utilise une technique appelée « *domain fronting* ». Celle-ci consiste à masquer le trafic de la messagerie dans les connexions chiffrées de CDN (Content delivery networks) ou de services Internet majeurs, parmi lesquels Google, Amazon Cloudfront, Amazon S3, Azure, CloudFlare, Fastly et Akamai. Résultat, le trafic généré par l'application ne peut pas être distingué d'autres trafics non censurés.

« Désormais, lorsque les gens en Égypte ou aux Émirats Arabes Unis envoient un message Signal, cela ressemble à une simple recherche Google. En gros, si vous voulez bloquer Signal, vous devrez bloquer Google », résume Moxie Marlinspike, fondateur d'Open Whisper Systems. Le seul moyen pour un gouvernement de désactiver Signal consisterait donc à bloquer d'autres services, voire à bloquer purement et simplement Internet, selon l'organisation. Une extrémité que peu de pays peuvent en réalité se permettre.

## Signal utilise Google en proxy

L'astuce fonctionne car Google App Engine permet aux développeurs de rediriger le trafic de Google.com vers leur propre domaine. L'utilisation par Google du chiffrement avec le protocole TLS (Transport Layer Security) signifie que le contenu du trafic, y compris la requête de redirection, est masqué. Google devient ainsi une sorte de proxy pour Signal, explique [Wired](#).

D'autres services utilisent déjà cette astuce du domain fronting, comme Tor et Psiphon entre autres. « L'idée est que pour bloquer le trafic ciblé, le censeur doit également bloquer d'autres services. Avec suffisamment de services à grande échelle agissant comme des 'fronts', désactiver Signal finit par ressembler à désactiver l'Internet », dit Moxie Marlinspike.

### Lire aussi :

[Le chatbot de Microsoft se plie à la censure chinoise ?](#)

[Apple recrute le développeur de Signal pour renforcer l'iPhone](#)

[Facebook censure pour pouvoir revenir en Chine](#)

crédit photo © XXX