ProtonMail blinde son avenir avec 2 millions de dollars

Agrandir ses effectifs, emménager dans de nouveaux bureaux à Genève, réunir ses équipes américaines à San Francisco… et accélérer le développement de son système de messagerie « ultra-sécurisé » **ProtonMail** en redimensionnant notamment son infrastructure de serveurs : tels sont les principaux objectifs de Proton Technologies après son premier tour de table institutionnel.

La jeune entreprise fondée par une douzaine d'étudiants du MIT et un doctorant de Harvard ayant travaillé pour le CERN (Organisation européenne pour la recherche nucléaire) a levé **2 millions de dollars** auprès de Charles River Ventures et de FONGIT. Le premier est un fonds de capital-risque basé dans le Massachusetts. Il a déjà soutenu Twitter, Yammer ou encore le fabricant de montres connectées Pebble. Le second est un incubateur privé soutenu par la Commission fédéral suisse pour la technologie et l'innovation, selon ITespresso.

Proton Technologies avait déjà obtenu, à l'été 2014, une enveloppe de 550 000 dollars dans le cadre d'une campagne de financement participatif. La start-up compterait aujourd'hui 350 000 bêta-testeurs pour son offre ProtonMail, chiffrée de bout en bout et hébergée en Suisse, pays où les lois régissant l'accès aux données personnelles par les autorités sont très contraignantes.

Porté par l'ère post-Snodewn

Inscrit dans la lignée des révélations d'Edward Snowden sur les opérations de cyber-espionnage menées par les agences de renseignement, ProtonMail s'appuie sur des mécanismes de (dé)chiffrement côté client, dans le navigateur Internet, avant l'envoi et la réception de messages. Cette implémentation est d'autant plus difficile à réaliser qu'il faut y coupler la dimension d'analyse anti-malware ; mais elle permet de créer un service plus robuste.

ProtonMail s'utilise sans module complémentaire : pour lire un message, les utilisateurs de Yahoo, Gmail et autres reçoivent un lien à ouvrir sur le navigateur et, après authentification, ils peuvent accéder au contenu.

Une première bêta avait été lancée en mai 2014. Depuis lors, le design a évolué, l'espace de stockage alloué s'est élargi, les certificats SSL ont été mis à jour en RSA-4096 avec hachage grâce à l'algorithme SHA256, etc.

Une sécurité toujours relative

Des annonces relatives à la sécurité sont néanmoins régulièrement postées sur le blog de la société, dont la transparence avait un temps été mise en question par la révélation de failles qui avaient été corrigées sans que les utilisateurs en soient avertis. Illustration avec cette vulnérabilité découverte l'été dernier et qui permettait d'intégrer, dans le corps des e-mails, du code malveillant qui s'exécutait ensuite – sous certaines conditions – sur la machine du destinataire.

Le chercheur qui avait repéré cette brèche s'était également aperçu qu'il était possible de contourner les mécanismes d'authentification en faisant réaliser à la victime des actions à son insu. Par exemple, modifier les signatures en bas des e-mails et y intégrer du code malveillant.

A lire aussi :

Le service de messagerie anti-NSA, Protonmail, arrive en test

[MàJ] La messagerie ultra-sécurisée ProtonMail privée de compte Paypal

Crédit Photo : Ilin Sergey-Shutterstock