Firefox peine à se débarrasser de l'indésirable SHA-1

Décidément, la mise à la retraite de SHA-1, un algorithme utilisé dans les communications chiffrées HTTPS jugée vulnérable après plusieurs attaques démontrées par des experts, est plus compliquée à mettre en œuvre que prévue. Si la plupart des éditeurs de navigateurs web ont fixé un calendrier pour écarter définitivement SHA-1, certains comme la Fondation Mozilla ont décidé d'aller plus vite avec une échéance prévue au 1er juillet 2016. L'objectif étant d'adapter les navigateurs vers le support du successeur de SHA-1, SHA-2 jugé plus sécurisé.

Pour entamer l'année sur de bonnes résolutions, la version 43 de Firefox avait donc banni le support de SHA-1. Oui mais voilà, plusieurs internautes utilisent des antivirus ou des solutions d'analyse de trafic en tampon pour accéder à Internet. Or ces outils fonctionnent avec des certificats SHA-1 qui sont rejetés par le navigateur et bloque les pages web.

Une réintégration forcée, mais nécessaire

Devant ce problème de compatibilité, la Fondation a donc préféré réintégré le support de SHA-1 dans Firefox à travers une évolution de la version 43. Dans un blog, elle lance un appel aux éditeurs de solutions de sécurité de mettre à jour leurs produits. Elle confirme néanmoins sa volonté de supprimer SHA-1 de Firefox.

Des déboires qui s'ajoutent à la problématique de la base installée qui ne dispose pas de navigateur ou de terminaux susceptibles d'accepter les certificats SHA-2. Le CDN CloudFlare a estimé que que 37 millions de personnes devraient être touchées. Et de pointer certains pays comme la Chine, l'Iran, le Népal, le Vietnam et de nombreux pays africains. Une crainte partagée par Alex Stamos, RSSI de Facebook, qui milite pour la mise en place d'une solution de retrait alternatif : les sites web s'appuient par défaut sur SHA-2, mais quand les sites détectent que le navigateur est trop ancien, alors ils devraient proposer une version avec SHA-1. Les développeurs de Facebook ont déjà mis à disposition le code source pour mettre en place cette fonctionnalité sur le plan technique (serveur).

A lire aussi :

SHA-1 : un algorithme clef du chiffrement HTTPS n'est plus sécurisé

SHA-1 : Google, Microsoft et Firefox font le ménage dans le HTTPS

Crédit Photo : wk1003mike / shutterstock