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

Google s'apprête à bannir toute forme de chiffrement exploitant l'algorithme de hachage SHA-1, jugé insuffisamment sécurisé par les chercheurs. Le support de cette technologie sera définitivement retiré de Chrome, le principal navigateur du marché au 1er janvier 2017 « *au plus tard* ». D'ici là, un premier pas sera franchi avec Chrome 48, actuellement en bêta, qui affichera une erreur dès qu'il rencontrera un certificat SHA-1 émis par une autorité publique après le 1er janvier 2016. Les autorités de certification étant censées arrêter l'émission de certificats SHA-1 dès le début de l'année prochaine, Google estime que cette étape ne devrait pas poser trop de problèmes.

La rupture sera plus définitive quand Chrome mettra fin à toute forme de support des certificats basés sur SHA-1. Dès le 1er janvier 2017, tous les sites HTTPS utilisant ce type de technologies généreront alors **des erreurs sur le navigateur**. Google indique que cette étape pourrait être franchie bien plus tôt, soit dès le 1er juillet 2016. Cette avancée du calendrier est en ligne avec les annonces récentes de Microsoft, qui envisage de bloquer dans Windows les certificats SHA-1 dès juin 2016, et de la fondation Mozilla, qui veut leur fermer les portes de Firefox au 1er juillet prochain. Google ne fait pas mystère de sa volonté d'**aligner Chrome avec ses principaux concurrents**, Microsoft Edge et Firefox.

Windows XP et Android 2.2 sur la touche

Dès 2016, l'émission de nouveaux certificats SHA-1 est proscrite par le CA/Browser Forum, une organisation qui regroupe l'industrie logicielle et notamment les éditeurs de navigateurs. Reste à **migrer la base installée**, et en premier lieu environ un million de certificats SSL en circulation reposant sur SHA-1, selon les dernières estimations de Netcraft. De son côté, l'organisation Trustworthy Internet Movement (TIM) estime que 24 % des certificats SSL en circulation s'appuient sur la fonction réputée friable.

Problème : une partie de la base installée aura du mal à encaisser la transition vers SHA-2. Car une petite, mais tout de même significative, part des internautes ne dispose pas de navigateur ou de terminaux susceptibles d'accepter les certificats SHA-2. Autrement dit, ces utilisateurs, qui reposent sur des navigateurs, des téléphones ou des terminaux d'accès anciens, n'auront plus accès aux sites HTTPS. Cela concerne, par exemple, les internautes sous Windows XP SP2 et ceux sous Android 2.2 (ou versions précédentes). Or, selon Net Applications, en novembre, Windows XP motorisait toujours près de 12 % des PC de la planète. Bref, la retraite de SHA-1 va interdire l'accès des sites chiffrés à des dizaines de millions d'utilisateurs, surtout en Chine, en Afrique, en Inde, au Vietnam et autres pays en voie de développement.

Attaques par collision

L'an dernier, Mozilla avait déjà effectué la migration du site de téléchargement de son navigateur vers un nouveau certificat SSL utilisant un hachage SHA-2. Résultat : la mise à jour avait « *annihilé un million de téléchargements* », selon un responsable de l'éditeur, s'exprimant sur un forum en septembre 2014. Soit 5 % des téléchargements totaux, avait-il ajouté. Mozilla avait alors rétropédalé pour remettre en place un certificat avec hachage SHA-1.

Conçu par la NSA américaine en 1995, SHA-1 offre des fonctions dites de hachage qui prennent des données en entrée et les injectent dans une empreinte, servant de signature cryptographique au message de départ. Une fonction de hachage n'est utile que si deux messages en entrée, même très proches, aboutissent à des empreintes très différentes. Si tel n'est pas le cas, on parle alors d'un phénomène dit de collision, ce qui compromet la sécurité de l'algorithme tout entier. Un assaillant étant alors en mesure de créer une signature (une empreinte), autrement dit de se faire passer pour ce qu'il n'est pas, mettant en péril les communications chiffrées (e-commerce, banque en ligne…). La communauté scientifique estime désormais que SHA-1 n'est plus immunisé contre les collisions, et ce à des coûts tout à fait accessibles à une organisation cybercriminelle.

A lire aussi:

Thomé, Inria : « Les clefs de chiffrement de 768 bits ne suffisent plus »

Le chiffrement source de multiples failles de sécurité

Crédit photo : isak55 / Shutterstock