Chiffrement : la retraite de SHA-1 va rendre aveugles des millions d'internautes

Comme nous l'expliquions dans un article récent, SHA-1, un algorithme de hachage très répandu dans les protocoles chiffrés sur Internet, n'est jugé plus suffisamment sûr par la communauté scientifique. D'où l'urgence de la migration vers son successeur, SHA-2. 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 l'algorithme, 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 l'algorithme réputé friable.

Et là, une difficulté majeure va se faire jour, du côté de la base installée. 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, le 30 septembre dernier, Windows XP motorisait toujours environ 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.

Certificats SHA-1 : suspects dès 2017

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 aurait « *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.

Les utilisateurs concernés devraient commencer à rencontrer des difficultés de connexion dans le courant de l'année 2016, à mesure que les certificats utilisant l'ancien algorithme sont retirés. Les éditeurs de site n'ont guère d'autre choix : à partir de janvier 2017, les navigateurs Chrome et Firefox émettront des alertes de sécurité à chaque fois qu'ils rencontrent un certificat basé sur SHA-1. Firefox pourrait même commencer à lancer cet avertissement dès juillet 2016, si des attaques contre SHA-1 sont attestées, comme le laisse entendre une étude récente à laquelle a participé l'Inria et qui estime que les coûts d'une telle opération sont désormais à la portée d'une organisation cybercriminelle.

A lire aussi :

Failles NTP : la machine à détraquer le temps menace aussi le chiffrement
Comment la NSA a (probablement) cassé le chiffrement par VPN
Chiffrement : tous les navigateurs vont abandonner l'algorithme RC4

Crédit Photo : SergeyNivens-Shutterstock