Chiffrement : Microsoft va bannir le SHA-1 dans Windows 10 Anniversary Update

Le SHA-1 n'est plus en odeur de sainteté. Désormais jugé trop faible pour protéger efficacement les communications, notamment pour les connexions HTTPS, cet algorithme de chiffrement est voué à disparaître des navigateurs. Fin 2015, Google annonçait son intention de le bannir définitivement de Chrome au 1er janvier 2017 au plus tard. Après l'avoir un temps supprimé de Firefox, la Fondation Mozilla a remis l'algorithme en service pour maintenir l'accès aux sites qui utilisent toujours un certificat SHA-1. Et ils sont encore nombreux. Selon des chercheurs, l'algorithme de hachage créé par la NSA (National Security Agency) en 1993 constituait encore 28% des certificats web (notamment les certificats SSL) fin 2015. Mozilla a néanmoins annoncé qu'il fermera définitivement les portes de son navigateur à SHA-1 le 1er juillet prochain.

De son côté, Microsoft avait dans un premier temps annoncé le blocage dans Windows des certificats TLS exploitant le SHA-1 pour janvier 2017 avant, finalement d'avancer la date à juin 2016. L'éditeur de Redmond vient de préciser les modalités de l'arrêt du support de cette technologie vieillissante. Et d'en revoir encore une fois le calendrier.

Sites SHA-1 toujours supportés mais pas sécurisés

Dans une contribution de blog, les responsables développement Alec Oot et Mike Stephens annoncent que *« Edge et Internet Explorer ne considéreront plus les sites Web protégés par un certificat SHA-1 comme sûrs et l'icône de verrouillage de la barre d'adresse pour ces sites disparaîtra »*. Une mise à jour qui prendra effet avec les versions livrées dans Windows 10 Anniversary Update, la prochaine mise à niveau majeure de l'OS desktop et mobile de Microsoft attendu dans le courant de l'été (peut-être le 29 juillet pour la première bougie de Windows 10).

Autrement dit, les sites certifiés SHA-1 resteront accessibles par les navigateurs de Microsoft. Mais ils ne seront simplement plus considérés comme sécurisés. Redmond laissera donc à l'utilisateur final le soin d'assurer la propre sécurité de sa navigation en ligne. Les bêta-testeurs inscrits au programme Windows Insider pourront le constater lors d'une prochaine pré-version (*Preview*) de l'OS que Microsoft mettra prochainement à leur disposition.

Des millions de personnes impactées

Une situation qui ne perdurera néanmoins pas. Microsoft prévoit de bloquer, visiblement définitivement, les certificats signés TLS sous SHA-1 sur Edge et IE à partir de février 2017. Ce qui s'appliquera notamment aux utilisateurs de Windows 7 et 8.1 qui continuent de surfer avec IE11. Une période quelque peu décalée en regard de l'échéance fixée au 31 décembre 2016 à partir de laquelle les autorités de certifications n'émettront plus certificats SHA-1 qui expireraient au-delà de cette date butoir.

Le passage du SHA-1 vers le SHA-2 (et particulièrement le hash SHA-256), totalement hermétique à

ce jour aux risques de «collision» (qui permet de créer de faux certificats), ne se fera pas sans douleur. Selon Facebook, 3 à 7% des navigateurs aujourd'hui utilisés sont incapables de supporter le SHA2. *« Ce qui signifie que des dizaines de millions de personnes ne seront pas en mesure d'utiliser Internet en toute sécurité après le 31 décembre »*, notait Alex Stamos, directeur sécurité (CSO) de Facebook, en décembre 2015. Particulièrement les utilisateurs dans les pays émergents (6% en Chine notamment) et ceux utilisant encore Windows XP (et IE7). *« Nous pensons qu'il n'est pas juste que des dizaines de millions d'utilisateurs soient coupés des bénéfices de l'Internet chiffré »*, estime le CSO. Surtout s'ils ne peuvent plus se connecter au réseau social.

La possibilité d'une alternative?

Une alternative proposée par le CDN CloudFlare pourrait être mise en place. Il s'agirait de faire accepter au CA/B Forum, l'association d'industriels chargée de la politique des certifications électroniques, la création d'une nouvelle classe de certificat: la Legacy Verified (LV). Ces certificats estampillés «héritage vérifié» autoriseraient le support du SHA-1 et seraient attribuées aux organisations prêtes à supporter les navigateurs anciens. Outre Facebook et CloudFlare, Alibaba et Twitter soutiennent l'idée de maintenir le support du SHA-1 jusqu'en mars 2019. Un délai jugé suffisamment longs pour espérer voir la disparition complète des navigateurs incompatibles avec le SHA-256. Une disparition que les principaux éditeurs de navigateurs pourraient néanmoins accélérer dès l'année prochaine.

Lire également

SHA-1 : un algorithme clef du chiffrement HTTPS n'est plus sécurisé
Microsoft blackliste 20 autorités de certification, dont le Français Certigna
Le chiffrement par TLS victime de… la paresse