HTTPS : Google bannit les certificats Symantec de Chrome et Android

Depuis plusieurs mois, Google a affiché sa volonté de ne plus tolérer les errements des autorités de certification. En témoigne la liste d'exigences que le géant de la recherche a formulé à l'encontre de Symantec fin octobre, suite à un écart de conduite de l'autorité de certification de l'éditeur de sécurité (Thawte). Dans un billet de blog paru en fin de semaine dernière, Google annonce qu'il va désormais bannir les certificats émis par **la racine « Class 3 Public Primary CA »** (pour Certification Authority) de l'éditeur. Ces certificats ne seront bientôt plus considérés comme sûrs par Chrome, Android et les autres produits Google. Autrement dit, les utilisateurs verront s'afficher des **messages d'alerte anxiogènes** à chaque fois qu'un service (comme un site HTTPS) exploite ces outils de chiffrement.

Mountain View présente cette décision radicale comme la conséquence logique d'une notification de Symantec, en date du 1er décembre. Notification qui, aux yeux de Google, signe la fin du support par l'autorité de certification des critères de base du CA/Browser Forum, un consortium réunissant autorités de certification, éditeurs de navigateur, d'OS ou autres. « *Comme ces critères reflètent les bonnes pratiques de l'industrie et sont les bases des certificats reconnus publiquement comme sûrs, ne pas s'y conformer représente un risque inacceptable pour les utilisateurs des produits Google* », tacle Ryan Sleevi, un ingénieur de Mountain View dans un billet de blog.

Symantec : c'était prévu

Selon Google, Symantec explique que ce choix de ne plus se conformer aux critères du CA/Browser Forum par sa volonté d'utiliser l'autorité de certification Class 3 Public Primary CA pour des usages différents de ceux des certificats publiquement reconnus comme sûrs. Mountain View, qui assure que Symantec n'a pas souhaité lui préciser les nouveaux usages en question, en tire donc les conséquences. Ryan Sleevi écrit : « *Google n'est plus en mesure de garantir que cette autorité de certification ou que les certificats émis par cette dernière ne sont pas utilisés pour intercepter, dégrader la sécurité ou imiter les communications sécurisées des produits ou utilisateurs Google* ». Symantec n'a pas réagi sur son site à cette saillie du géant de la recherche, qui présente sa décision comme une punition.

Contacté, l'éditeur indique, toutefois, que la décision de Google est… des plus normales. « *En novembre, nous avons informé les éditeurs de navigateur qu'ils devraient retirer le certificat racine PCA3 G1 car il était basé sur des standards de sécurité anciens. Il n'était de toute façon plus utilisé depuis longtemps pour créer de nouveaux certificats* », explique un porte-parole de l'éditeur. Comme l'indique cette page répertoriant les différentes racines opérées par le groupe, il s'agit bien là de la racine Class 3 Public Primary CA, désignée à la vindicte publique par Google (voir la partie Root 2). Bref, l'éditeur explique que Google se serait contenté de **prendre acte des recommandations** qu'il a publiées concernant cette racine. Symantec indique par ailleurs vouloir désormais exploiter cette dernière pour « *offrir un support de transition pour les applications de certains clients, pour des usages strictement internes* ». Même si notre interlocuteur n'a pu nous le confirmer, il s'agit très certainement de

supporter le remplacement de l'algorithme SHA-1, dont la mise à la retraite a été anticipée récemment.

Escarmouches autour des certificats

En tout cas, le ton du billet de Google en dit long sur les relations entre les deux sociétés. Qui n'en sont pas à leurs premiers accrochages. En octobre dernier, après que Symantec a reconnu une faille mineure dans l'émission de ses certificats, Google avait expliqué que les mauvaises pratiques étaient en fait bien plus répandues que ce qu'indiquait l'éditeur d'outils de sécurité. Et ne s'était pas privé de **mettre la pression sur Symantec**, exigeant que son autorité de certification se conforme à toute une série de bonnes pratiques, faute de quoi ses certificats seraient bannis de ses produits en juin prochain. Mountain View avait notamment exigé que Symantec se conforme au protocole dit de Certificate Transparency, via lequel les autorités de certification doivent se soumettre à un système auditable et public d'enregistrement des émissions de certificats. Et ce pour tous les certificats émis par Symantec. Google avait par ailleurs réclamé une analyse indépendante des défaillances détectées chez Thawte.

A lire aussi :

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

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

Crédit photo : isak55 / Shutterstock