# Google bloque des certificats numériques corrompus… de l'Anssi

C'est une histoire de cordonnier mal chaussé. Google a bloqué, samedi 7 décembre, des **certificats numériques émis par une autorité de certification mandatée par l'Anssi**, l'Agence nationale de la sécurité des systèmes d'information. Ce qui fait pour le moins désordre.

Rappelons que les certificats numériques servent de carte d'identité des sites sécurisés (chiffrés) pour les navigateurs qui les visitent. Les précieux sésames, délivrés par des autorités certifiées (institutions, sociétés commerciales…), visent à **interdire les risques de détournement de trafic** à des fins de collecte de données privées (code banque, mot de passe…). Un système efficace sauf lorsqu'un certificat est corrompu et que celui-ci est alors exploitable par n'importe quel site de phishing qui se fera alors passer pour le vrai aux yeux du navigateur.

C'est à priori ce qui aurait pu se passer. Les certificats refoulés par Google permettaient d'**inspecter le trafic crypté de plusieurs domaines de l'éditeur**. Certes avec la connaissance des utilisateurs du réseau privé sur lequel il était exploité, indique l'entreprise de Mountain View. Mais la méthode viole totalement les procédures de l'Anssi.

## Une erreur humaine

Google s'est empressé d'alerter l'agence française. Laquelle a **révoqué les certificats en question**. *« Suite à une erreur humaine lors d'une action de renforcement de la sécurité au ministère des Finances, des certificats numériques correspondant à des domaines extérieurs à l'administration française ont été signés par une autorité de certification de la direction générale du Trésor rattachée à l'IGC/A. La branche considérée de l'IGC/A a été coupée à titre préventif »*, a expliqué l'Anssi.

L'IGC/A (Infrastructure de Gestion de la Confiance de l'Administration) est l'infrastructure gérant les clefs cryptographiques opérées par l'Anssi. Sur le site de l'agence, il est précisé que « *l'IGC/A permet d'instaurer un domaine de confiance interministériel et de faciliter l'authentification des téléservices de l'administration française*« . Et d'indiquer que les certificats en question « *permettent d'identifier officiellement les autorités de certification des administrations de l'État français* » et attestent « *de la qualité des pratiques de gestion des clés publiques mises en œuvre par ces autorités*« . Bref, le cœur du réacteur en ce qui concerne l'authentification des services en ligne de l'Etat.

Plus qu'un acte de piratage, c'est donc **une mauvaise manipulation** qui aurait mis en défaut l'intégrité des certificats. Un moindre mal, en théorie. Si *« cette erreur n'a eu aucune conséquence sur la sécurité des réseaux de l'administration ni sur les internautes »* selon l'Anssi, Google entend néanmoins *« étudier soigneusement d'éventuelles mesures complémentaires »*.

crédit photo © Pavel Ignatov – shutterstock

---

**Lire également**

Prism : « le révélateur de notre incapacité à gérer nos données » pour Thales
Sécurité des Scada : il est urgent d'agir, selon l'Anssi
Il est urgent de renforcer la cybersécurité en France