Google victime de faux certificats mandatés par la Chine

Google déclare avoir découvert que plusieurs de ses noms de domaine ont été associés à des certificats frauduleux. Les certificats en question auraient été délivrés par un organisme intermédiaire *« apparemment »* détenu par une société nommée **MCS Holdings**, basée en Egypte, et mandaté par le registre chinois **CNNIC**. Exposant aux attaques de type *« man-in-the-middle »* des échanges utilisant le protocole de sécurisation SSL (*Secure Sockets Layer*) ou son successeur TLS.

Tous les navigateurs et OS concernés, ou presque

Les certificats frauduleux concernés peuvent avoir été approuvés par *« presque tous les navigateurs web et systèmes d'exploitation »*, explique Google dans un billet de blog publié lundi 23 mars. Mais il existe **des exceptions** : Chrome (Google) sous Windows, OS X ou Linux, ChromeOS, ainsi que Firefox 33 et ses versions ultérieures, selon Google. La société assure avoir rapidement bloqué le certificat issu de MCS Holdings dans Chrome avec CRLSets, alerté ses concurrents et demandé des comptes au CNNIC (Centre d'information du réseau Internet de Chine).

Le mandataire, MCS Holdings, aurait agi comme un proxy ayant obtenu carte blanche d'une autorité de certification publique, *« ce qui constitue une violation grave du système »*, a affirmé Google. L'entreprise américaine n'hésite pas non plus à faire le parallèle avec l'affaire des certificats corrompus émis par une autorité de certification mandatée par l'Anssi française – l'Agence nationale de la sécurité des systèmes d'information – en 2013.

Lire aussi :
Superfish : Lenovo reconnaît avoir préinstallé un logiciel espion
Les certificats SSL contrefaits étudiés à la loupe