Nogofail : Google traque les failles de SSL et TLS

Google incite les webmasters à généraliser l'usage du HTTPS, des connexions utilisant un protocole de chiffrement. Si cette sécurisation des échanges apporte un niveau de confidentialité supplémentaire, elle n'est en rien infaillible. Les connexions HTTPS étant en particulier **exposées à des attaques dites de l'homme du milieu** (Man-in-the-middle)

Pour rassurer les utilisateurs, Google met aujourd'hui à disposition de la communauté **un outil de test baptisé Nogotofail**. Un logiciel diffusé sous forme de projet Open Source sur Github, ce qui signifie qu'il est ouvert aux contributions extérieures. Il fonctionne avec Android, iOS, Linux, Windows, Chrome OS, OS X et « *n'importe quel appareil permettant de se connecter à Internet* », précise Google dans une contribution de blog. Objectif de l'outil : **vérifier que les applications et terminaux ne renferment pas de vulnérabilités** connues SSL/TLS (les protocoles de chiffrement utilisés avec les connexions HTTPS) ou de mauvaises configurations.

Un outil de vérification qui fait suite à la découverte de toute une série de failles affectant les technologies de chiffrement, rappellent nos confrères de ITespresso. Cette année notamment, le protocole HTTPS (Hypertext Transfer Protocol Secure) a fait l'objet d'attaques exploitant des vulnérabilités dans la couche de sécurisation SSL/TLS.

Simuler une attaquer de l'homme du milieu

Le 14 octobre dernier, Google rendait ainsi public **Poodle**, une vulnérabilité logicielle trouvée au cœur du protocole SSL 3.0 (patchée avec Chrome 38, ce protocole disparaitra de Chrome 39). Et comment ne pas parler de **Heartbleed qui a fait trembler le web** en avril 2014 ? Présente dans le protocole OpenSSL, cette faille a fait peser une menace sans précédent sur les échanges Internet.

Ajoutons, en février 2014, la faille « Goto fail » découverte dans le code source de la librairie SecureTransport d'Apple et affectant la prise en charge du protocole SSL/TLS sur iOS et Mac OS X. L'outil rendu public par Google tire d'ailleurs son nom de cette vulnérabilité.

Il est déjà possible de tester en ligne un site web utilisant le protocole HTTPS via **un outil comme Qualys Lab Tool**. Mais « Nogotofail » est présenté comme plus complet et permettant de tester toutes les failles découvertes à ce jour. L'outil de Google va simuler une attaque de type Man-in-the-middle et peut être **déployé en tant que routeur, VPN ou proxy**.
Si Google clame sa volonté altruiste d'éradiquer les failles dans le protocole SSL/TLS, il s'agit également de restaurer un climat de confiance sur Internet, suite aux révélations sur les écoutes de la NSA. Avec pour principe clef : tout ce qui bénéficie à Internet bénéficie à Google.

A lire aussi :
5 questions pour comprendre le déchiffrement SSL
5 mois après : le bilan de la faille Heartbleed

Crédit photo : © Sergej Khackimullin / Fotolia.com