Comment le ministère des finances espionne le trafic web de ses collaborateurs

Une « erreur humaine » dans la gestion de la sécurité informatique a mis en évidence un système de surveillance pour déchiffrer les flux SSL entrants et sortants. Une pratique qui existe... dans toutes les grandes entreprises.

Gilbert Kallenborn | 01net | le 11/12/13 à 18h57 | 1 réaction

Le Minefi décrypte tous les échanges SSL de ses collaborateurs.

agrandir la photo

Pour Ralf Skyper Kaiser (RSK), membre du collectif de hackers « The Hackers Voice », il n'y a pas de doute possible : le ministère français de l'Economie et des Finances (Minefi) espionne les flux web chiffrés en SSL de ses collaborateurs. Et il est tellement remonté qu'il a même averti la Commission européenne pour l'inciter à mener une enquête.

L'affaire remonte en fait à quelques jours. Google avait mis la main sur un faux certificat de chiffrement SSL, émis et utilisé par le Minefi pour chiffrer les échanges avec le domaine google.com. En d'autres termes, le Minefi a endossé le rôle d'un tiers de confiance reconnu pour garantir la sécurité des échanges entre les utilisateurs internes et les sites web de Google. Ce qui est, évidemment, totalement anormal. C'est pourquoi Google a immédiatement sonné l'alarme, en épinglant non pas le Minefi, mais l'ANSSI. En effet, si le Minefi a pu créer un tel faux certificat, c'est parce que l'ANSSI - qui est une autorité de certification dite « racine » - lui a donné ce pouvoir selon un processus de délégation définie dans le cadre de l'IGC/A (infrastructure de gestion de la confiance de l'administration).

Tous les échanges SSL sont passés au peigne fin

L'ANSSI a réagi au quart de tour, en révoquant les faux certificats et en publiant un communiqué qui fait référence à une *« erreur humaine »* dans l'utilisation des certificats. Mais selon RSK, l'affaire est beaucoup plus malsaine que cela. Selon lui, l'usage de ces faux certificats ne peut pas se faire par erreur et prouve l'existence d'une technologie de surveillance appelée « proxy SSL ». Celle-ci se place dans l'enceinte d'une organisation et intercepte le trafic entre l'utilisateur et le site web en question.

Grâce au faux certificat, ce dispositif fait croire à l'utilisateur qui souhaite accéder aux sites web externes que sa liaison est bien sécurisée. Mais en réalité, cela lui permet de déchiffrer les échanges, d'analyser son contenu, avant de les chiffrer à nouveau avec un vrai certificat et de les réexpédier vers l'extérieur. Du point de vue de Google, tout se passe donc normalement. Mais ce n'est pas tout. Doté d'une délégation de la part de l'ANSSI, le Minefi pouvait en réalité créer un faux certificat pour n'importe quel site. *« Il est probable que le Minefi ait surveillé les échanges vers tous les sites »*, souligne RSK.

Un espionnage qui se fait depuis des années

Mais pour Bruno Bonfils, consultant en sécurité indépendant, il n'y a rien de vraiment nouveau sous le soleil dans cette histoire. *« Les proxy SSL sont déployés dans toutes les grandes entreprises. Elles veulent déchiffrer les flux SSL entrants et sortants pour éviter que des informations sensibles ne sortent. C'est la stratégie dite du Data Leakage Prevention »*, explique l'expert. Cet espionnage se fait en toute douceur, depuis des années. Mais personne ne s'en aperçoit, car ces dispositifs utilisent des certificats à usage strictement interne, qui ne sont rattachés à aucune autorité de certification. *« Si le Minefi s'est fait épinglé, c'est justement parce qu'il n'a pas utilisé de certificat local, mais un certificat qui était validé par une autorité officielle. Ce qui est contraire aux principes de sécurité des autorités de certification »*, poursuit le consultant.

Une telle surveillance serait d'ailleurs légale, à partir du moment où elle est notifiée aux utilisateurs par le biais d'une charte informatique. Mais la plupart des salariés n'en ont pas

conscience : personne ne lit jamais les chartes informatiques et le décryptage des données SSL est rarement indiqué de manière explicite.

L'ANSSI confirme

Interrogé par 01net, l'ANSSI admet d'ailleurs l'existence de ce dispositif de surveillance au sein du Minefi. *« La direction générale du Trésor, étant particulièrement sensibilisée aux attaques informatiques, a mis en place un dispositif de filtrage (un web application firewall - WAF) en périphérie d'une partie de son système d'information pour détecter des attaques potentielles,* nous explique l'autorité par email. *C'est sur ce dispositif qu'étaient utilisés les certificats. L'emploi d'équipements de sécurité de type WAF, lorsqu'il est réalisé dans les règles de l'art, n'est pas un problème en soi. En revanche, les certificats utilisés sur de tels équipements ne doivent impérativement pas être rattachés à une autorité de certification reconnue (telle que l'IGC/A). »* En effet, un tel mauvais usage entache la crédibilité de l'ANSSI en tant qu'autorité de certification racine.

L'ANSSI tient par ailleurs à préciser qu'il ne faut pas parler d'espionnage des collaborateurs. *« Ces technologies largement utilisées (que l'on retrouve dans la plupart des firewall applicatifs) sont destinées à inspecter le trafic chiffré entrant et sortant d'une entreprise, d'une administration...pour analyser l'activité potentielle de codes malveillants. Ce genre de technologies est justement là pour détecter d'éventuelles traces d'espionnage et pas le contraire. »*

En tous les cas, si vous êtes salarié dans une grande entreprise, sachez désormais qu'il ne suffit pas d'être connecté en SSL pour se sentir à l'abri vis-à-vis de son employeur. Et qu'il est préférable de faire ses virements bancaires depuis chez soi...