Comment Gemalto a été piraté par le GCHQ britannique

Dans un long article paru en fin de semaine dernière, *The Intercept* dévoile, sur la base de documents exfiltrés par Edward Snowden, comment le GCHQ britannique a mis en place une surveillance de masse des activités de millions d'internautes. Basée sur une collecte de métadonnées réalisée directement sur le trafic passant par les câbles en fibre optique, notamment les câbles transatlantiques, l'outil développé par les espions britanniques – baptisé Karma Police – relie des adresses IP à des services que ces internautes ont utilisés ou visualisés. Selon un document transmis par Edward Snowden, en 2012, le GCHQ stockait 50 milliards de métadonnées par jour, total qu'il avait prévu de porter à 100 milliards à la fin de l'année. Rappelons que la Grande-Bretagne est une plaque tournante du trafic Internet, notamment transatlantique (voir carte ci-dessous), conférant au GCHQ une place de choix dans l'espionnage de masse mis en place par la NSA avec la complicité de ses alliés des Five Eyes.

Dans leur entrepôt de données, poétiquement appelé Black Hole, les espions britanniques stockent aussi des cookies, ces petits fichiers présents sur les postes de travail et permettant aux sites Web de garder une trace des habitudes de chacun. Ces cookies, qui renferment des noms d'utilisateurs, des e-mails, des adresses IP, les préférences des utilisateurs en matière de navigateur et parfois même des informations relatives aux mots de passe, servent au GCHQ à créer une passerelle entre l'adresse IP et des informations nominatives. Une passerelle établie via un outil appelé **Mutant Broth**.

La patience du GCHQ

Selon *The Intercept*, c'est cet outil qui aurait été exploité dans le cadre du piratage de Gemalto, le leader de la production de cartes SIM dans le monde. Le mécanisme serait le suivant : le GCHQ aurait utilisé Mutant Broth pour analyser des cookies Facebook interceptés qu'il pensait associés à des employés de Gemalto en France et en Pologne. Ce serait donc l'infection de ces utilisateurs, dont les adresses IP auraient été isolées via leurs usages personnels, qui aurait permis aux espions britanniques de s'infiltrer sur le réseau Gemalto pour y dérober des clefs de chiffrement servant à protéger les communications téléphoniques mobiles. Rappelons, en effet, que ce hack visait, *in fine*, à compromettre la sécurité des échanges sur les réseaux mobiles, sans avoir besoin de demander l'assistance des opérateurs ou de gouvernements étrangers. Et sans laisser la moindre trace sur les réseaux… Au passage, la technique utilisée démontre une nouvelle fois la patience des espions du GCHQ et de leurs compères de la NSA, capables, pour parvenir à leurs fins, de passer par des biais détournés pour trouver la faille. Rappelons que Gemalto avait reconnu avoir été victime d'une attaque sévère en 2010 mais avait alors écarté tout vol massif de clefs de chiffrement.

Selon *The Intercept*, un mécanisme similaire a été mis en œuvre lors du piratage de Belgacom, l'opérateur belge fournissant des services notamment aux administrations européennes. Le GCHQ aurait entré des adresses IP associées à Belgacom dans Mutant Broth afin de découvrir des informations sur des employés de la société, technique qui lui a permis d'identifier les profils

Google, Yahoo et LinkedIn de trois ingénieurs de l'opérateur. Trois employés dont les ordinateurs ont été ensuite infectés, afin d'infiltrer le réseau de Belgacom. Rappelons qu'à l'époque, le GCHQ était parvenu à s'immiscer jusqu'au cœur du réseau de l'opérateur, ce qui lui permettait de récupérer directement les communications y transitant.

A lire aussi :

Le Royaume-Uni, allié de la NSA, pirate les clefs de chiffrement de Gemalto
Espionnage de Belgacom : ce serait un coup des services britanniques

Crédit photo : Gil C / Shutterstock