

Gemalto a bien été attaqué, mais ses réseaux sécurisés seraient restés étanches



Gemalto a bien été attaqué,
mais ses réseaux sécurisés
seraient restés étanches

Oui des attaques ont bien été détectées, mais Gemalto précise que ses réseaux sécurisés n'ont pas été pénétrés. Le vol massif de clés de SIM ? Impossible en 2010 du fait du chiffrement des échanges avec les opérateurs. Et d'autres facteurs permettent de pondérer les conséquences de ces attaques.

Un peu moins d'une semaine après la publication par The Intercept de documents décrivant des attaques contre des fournisseurs de cartes SIM, Gemalto, un des acteurs ciblés, a présenté les conclusions de ses investigations.

Et cette analyse semble effectivement confirmer le scénario d'une opération conjointe de deux agences de renseignement étrangères, la NSA et le GCHQ.

Des attaques « graves et sophistiquées », mais sur des réseaux périphériques

« Nous avons analysé la méthode décrite dans les documents et les tentatives d'intrusion sophistiquées que nous avons détectées sur notre réseau en 2010 et 2011 rendent l'information qui est décrite probable » déclare Olivier Piou, le directeur général de Gemalto.

Pour étayer cette conclusion, l'entreprise s'appuie sur la détection de « deux attaques particulièrement sophistiquées qui pourraient effectivement être liées à cette opération ». Le directeur de la sécurité de Gemalto, Patrick Lacruche, décrit ces deux attaques précises en 2010.

La première a été identifiée en juin de cette année. « Nous avons identifié une activité suspecte sur un de nos sites français. Un tiers a essayé de se connecter à un de nos réseaux que nous appelons Office, c'est-à-dire le réseau de communication des employés entre eux et avec le monde extérieur. »

Toujours en 2010, un second incident est détecté par l'équipe de sécurité : « Il s'agissait de faux emails envoyés à un de nos clients opérateurs mobiles en usurpant des adresses email authentiques de Gemalto. Ces faux emails contenaient un fichier attaché qui permettait le téléchargement d'un code malveillant. » Le client sera alerté et l'attaque signalée aux autorités.

Suivront sur la « même période » plusieurs « tentatives d'accès aux ordinateurs » de salariés de l'entreprise, ciblés en raison vraisemblablement de leurs « contacts réguliers » avec les clients de Gemalto.

Des vols de clés ? Possibles dans des « cas exceptionnels »

Si les attaques, qualifiées de « graves et sophistiquées », semblent avérées, le fournisseur de cartes SIM exclut en revanche qu'elles aient pu aboutir à la compromission de ses produits de sécurité ou à l'interception massive de clés de chiffrement.

Patrick Lacruche l'assure, ces attaques n'ont affecté « que des parties externes des réseaux Gemalto ». Or les « clés de cryptage et plus généralement les données clients ne sont pas stockées sur ces réseaux ».

Car, poursuit-il, « nous n'avons rien détecté d'autre, que ce soit dans les parties internes du réseau de notre activité SIM » ou « dans les parties du réseau sécurisé d'autres produits comme les cartes bancaires ». Ces « réseaux sont isolés entre eux et ne sont pas connectés au monde extérieur » indique encore le responsable sécurité.

L'entreprise reconnaît cependant que des interceptions de clés ont pu, dans des « cas exceptionnels », éventuellement être réalisées. Pour le justifier, Gemalto fait savoir qu'il avait « dès avant 2010 », mis en place un système d'échange sécurisé avec ses clients. Ce chiffrement empêcherait donc que les clés, en cas d'interception, puissent être exploitées ensuite pour des écoutes.

Au pire, seuls les réseaux 2G seraient affectés par des écoutes

Serge Barbe, le vice-président de Gemalto en charge des produits et services, a apporté d'autres informations permettant selon lui de relativiser les conséquences de ces attaques et les risques d'espionnage pour les clients des opérateurs.

Ainsi, si des clés de chiffrement de SIM avaient effectivement été dérobées, celles-ci ne permettraient de procéder à des écoutes que sur des communications 2G. Or, la faiblesse de cette technologie, « pensée dans les années 80 », était déjà connue.

« Donc si les clés de cryptage de cartes SIM 2G étaient interceptées par des agences de renseignement, il leur était techniquement possible d'espionner les communications » reconnaît Serge Barbe, qui précise toutefois que ces cartes étaient pour la plupart des cartes prépayées, c'est-à-dire dont le cycle de vie était réduit.

Mais qu'en est-il alors des SIM des générations suivantes ? Le vol auprès du fournisseur ou de l'opérateur des clés permet-il des opérations d'espionnage des communications ? Non selon Gemalto pour qui la faiblesse des carte 2G a été « éliminée » par la suite.

La sécurité a « encore été largement renforcée, je dirais même repensée, avec l'arrivée des cartes SIM de troisième et quatrième générations » revendique Serge Barbe. « L'interception et le décryptage en cours d'échange entre le fournisseur et l'opérateur ne permettrait pas aux pirates de se connecter aux réseaux 3G ou 4G et donc par conséquent d'espionner les communications ».

« Les cartes 3G et 4G ne pouvaient pas être affectées par l'attaque qui est décrite » dans les documents attribués aux GCHQ. Malgré tout, « ces produits plus récents ne sont toutefois pas utilisés universellement dans le monde » tient à préciser le représentant de Gemalto.

Pour le patron de Gemalto, Olivier Piou, une conclusion s'impose dans cette affaire d'espionnage : « L'encryptage systématique des échanges et l'utilisation de cartes de dernière génération, couplés à des algorithmes personnalisés pour chaque opérateur, sont la meilleure réponse à ce genre d'attaque. » Bref, une bonne opportunité finalement pour l'entreprise de faire la promotion de ses produits et pratiques de sécurité.

Après cette lecture, quel est votre avis ?

Cliquez et laissez-nous un commentaire...

Source : <http://www.zdnet.fr/actualites/gemalto-a-bien-ete-attaque-mais-ses-reseaux-securises-seraient-restes-etanches-39815336.htm>

Par Christophe Auffray