Cartes SIM : le mea culpa maîtrisé de Gemalto sur le piratage des clés

Gemalto s'est livré ce matin à un exercice de communication de crise face aux accusations livrées par « *The Intercept* » d'un piratage massif des clés de chiffrement des cartes SIM par les agences de renseignements anglaise (**GCHQ**) et américaine (**NSA**). Le leader mondial a donc mené un audit pour définir la réalité des accusations et a livré les conclusions de son enquête au Pavillon Gabriel à Paris juste devant l'ambassade des États-Unis et de celle d'Angleterre.

Pour mémoire, ces allégations proviennent des documents transmis par le lanceur d'alertes Edward Snowden. Dans ces présentations, l'infiltration du réseau de Gemalto serait à l'origine l'œuvre du GCHQ. La méthode reposerait au départ sur l'espionnage des communications privées (mails et comptes Facebook) de salariés Gemalto ainsi que de salariés d'opérateurs non identifiés pour voler les clés de chiffrement lors des échanges entre les deux. Ces clés permettent ensuite d'accéder à des informations transitant par le réseau des opérateurs.

Attaques confirmées contre le réseau externe de Gemalto

Sur cette première révélation, Olivier Piu, directeur général de Gemalto a répondu que « ***des attaques ont été effectivement menées en 2010 et 2011*** *qui nous montrent que l'opération citée dans les documents est probable* ». Le vice-président en charge des opérations et de la sécurité, Patrick Lacruche, est revenu plus en détail sur le *modus operandi* des attaques : « *nous avons eu deux vagues d'attaques. La première a été perpétrée en juin 2010 et a visé la branche que nous nommons Office (le réseau bureautique) qui est celle en contact avec l'extérieur. Un second incident en juillet 2010 a concerné l'envoi de faux emails avec des adresses Gemalto à des opérateurs, l'objectif était de cliquer sur un fichier joint qui contenait du code malveillant. En parallèle plusieurs tentatives d'intrusion ont été constatées* ».

Olivier Piu rajoute que « ***la seconde attaque était très sévère*** *et nous nous sommes rendu compte que ce n'était pas un hacker de base qui était derrière. Il fallait des ressources* ». Pour autant, le groupe basé en Hollande ne connaissait pas l'identité de l'attaquant, « *nous avons découvert comme vous la semaine dernière les informations dévoilées par Intercept* », souligne Patrick Lacruche. Les dirigeants admettent qu'à l'époque « *nous n'avions pas réussi à identifier les commanditaires des attaques* ». Ils écartent aussi le facteur humain comme maillon faible de la sécurité, « *ils ont utilisé un système de surveillance automatisée et non un ciblage humain* ».

Pas de vol massif et impact limité à la 2G

Si les attaques sont confirmées, il en va tout autrement du caractère massif de vol des clés de chiffrement. **Gemalto réfute les allégations** des documents publiés par *The Intercept*. « *Les seules clés interceptées l'ont été dans des cas exceptionnels, sur des questions de maintenance, d'urgence ou de test avec des opérateurs dont les échanges n'intégraient pas des processus hautement sécurisés que nous avions*

mis en place bien avant 2010 », indique Patrick Lacruche. Par contre impossible de connaître **le chiffre exact du nombre de clés volés**, la communication de crise a ses limites que la transparence ignore. Sur les clients touchés, aucun nom d'opérateurs n'a été donné.

Après « *le oui, mais* », l'autre étage de la communication de crise est de rassurer les clients et de vanter les mérites sécuritaires de la carte SIM notamment pour les réseaux 3G et 4G. « *Les clés interceptées ne sont exploitables que sur le réseau 2G et les opérateurs connaissent depuis longtemps les faiblesses de la technologie 2G* », constate Serge Barbe, vice-président chargé des produits et services. « *Nous avons proposé à l'époque d'intégrer des mesures de sécurité supplémentaire aux opérateurs* », précise le responsable. On peut néanmoins s'interroger sur les risques concernant les réseaux M2M qui embarquent souvent des cartes SIM 2G et utilisent encore le réseau 2G des opérateurs mobiles.

Par contre, il écarte l'idée que les cartes 3G et 4G puissent avoir été impactées, « *elles bénéficient d'un système de sécurisation différent et sont dotées d'une protection par chiffrement additionnelle* ». Le constructeur fait l'article par la même occasion de ces cartes de dernière génération avec algorithmes personnalisés.

Un agacement très diplomatique

Enfin, le dernier acte de cette communication a visé les commanditaires supposés du piratage, la NSA et le GCHQ. Olivier Piu s'est déclaré « *préoccupé que des autorités d'Etat aient pu lancer de telles opérations contre des sociétés privées non coupables d'agissements suspects* ». A-t-il été surpris de l'absence de réaction de la part des officiels français, le dirigeant botte en touche, « le gouvernement a d'autres choses à s'occuper », mais il en profite pour lancer une petite pique, « *les Américains et les Anglais sont déjà aux 21ème siècle sur les questions cyber, il y a une faiblesse en France avec peu d'outils juridiques* ».

C'est pour cela qu'**il ne compte pas lancer une action judiciaire** contre les agences de renseignement britannique et américaine. « *Les faits sont difficiles à prouver au sens juridique et attaquer un Etat est coûteux, long et assez aléatoire. La conclusion est que, non, on ne va pas prendre d'action juridique* ». Il ajoute même « *ce serait une perte de temps* ».

Au final, Gemalto a réussi à en dire un peu sans en dévoiler beaucoup sur cette affaire qui comporte quelques zones d'ombres : le nombre de clés réellement volées, leurs usages, le ou les opérateurs touchés, quelles ont été les motivations des agences de renseignement (surveillance, intelligence économique, etc), la raison de l'absence de réactions des autorités de l'Etat, les investigations n'ont concerné que la période 2010-2011 et après…

A lire aussi :

Gemalto se lance dans la sécurisation des documents… en polycarbonate

Gemalto lance une plate-forme universelle de paiement mobile clé en main