pressrelease

Gemalto présente les conclusions de ses investigations sur l'allégation de piratage de clés d'encryptage de cartes SIM

- L'analyse de la méthode décrite dans les documents et les tentatives d'intrusion sophistiquées détectées par Gemalto en 2010 et 2011 rendent cette opération probable.
- Les attaques contre Gemalto n'ayant touché que des réseaux bureautiques, elles n'ont pas pu résulter en un vol massif de clés d'encryptage de cartes SIM.
- La technique utilisée étant d'intercepter les clés lors de l'échange entre l'opérateur telecom et ses fournisseurs, et Gemalto ayant avant 2010 déjà largement déployé un système d'échange sécurisé avec ses clients, seuls quelques cas exceptionnels ont pu aboutir à un vol.
- Les données éventuellement volées par cette méthode ne sont exploitables que dans les réseaux de deuxième génération (2G). Les réseaux 3G et 4G ne sont pas vulnérables à ce type d'attaque.
- Aucun autre produit de Gemalto n'est concerné par cette attaque.
- L'encryptage systématique des données et des échanges, l'utilisation de cartes de dernières générations et d'algorithmes personnalisés pour chaque opérateur sont les meilleures réponses à ces attaques.

Amsterdam, le 25 février 2015 – Suite à la publication de documents par un site web le 19 février 2015, Gemalto (Euronext NL0000400653 GTO) a mené une investigation approfondie sur la base de deux éléments : les documents censés émaner de la NSA et du GCHQ rendus publics par ce site, et les outils de surveillance interne, avec leurs registres de tentatives d'intrusion.

L'article suppose que les documents publiés sont réels et qu'ils décrivent précisément des événements qui se sont produits en 2010 et 2011. Notre publication ci-dessous n'a pas pour but de confirmer partiellement ou entièrement ni de fournir des éléments permettant de réfuter partiellement ou entièrement le contenu des documents publiés par ce site web.

En tant qu'acteur de la sécurité numérique, Gemalto est régulièrement la cible d'attaques. Ces tentatives d'attaques sont plus ou moins sophistiquées et nous sommes habitués à y faire face. La plupart échouent mais quelques-unes parviennent parfois à pénétrer la partie externe de notre réseau qui est architecturé pour être très sécurisé.

Si nous regardons en arrière, sur la période couverte par les documents de la NSA et le GCHQ, nous confirmons avoir fait face à plusieurs attaques. En 2010 et 2011 précisément, nous avons détecté deux attaques particulièrement sophistiquées qui pourraient être reliées à cette opération.

En juin 2010, nous avons remarqué une activité suspecte sur l'un de nos sites français où un tiers a essayé d'espionner le réseau que nous appelons « office », c'est-à-dire le réseau de communication des employés entre eux et avec le monde extérieur. Des mesures ont été prises immédiatement pour éradiquer la menace.

En juillet 2010, notre équipe de sécurité a détecté un second incident. Il s'agissait de faux emails envoyés à l'un de nos clients opérateur mobile en usurpant des adresses email authentiques de Gemalto. Ces faux emails contenaient un fichier attaché qui permettaient le téléchargement de code malveillant. Nous avons immédiatement informé le client concerné et signalé l'incident aux autorités compétentes, en leur communiquant l'incident lui-même et le type de programme malveillant identifié.

Au cours de la même période, nous avons également détecté plusieurs tentatives d'accès aux ordinateurs de collaborateurs de Gemalto ayant des contacts réguliers avec des clients.
A l'époque, nous n'avons pas pu identifier les auteurs de ces attaques mais maintenant nous pensons qu'elles pourraient être liées à l'opération du GCHQ et de la NSA.

Ces intrusions n'ont affecté que des parties externes des réseaux de Gemalto, c'est-à-dire les réseaux bureautiques qui sont en contact avec le monde extérieur. Les clés de cryptage et plus généralement les données client ne sont pas stockées sur ces réseaux. Il faut imaginer l'architecture de notre réseau un peu comme le croisement entre un oignon et une orange. Il est composé de couches multiples et de nombreux quartiers qui permettent de cloisonner et d'isoler les données.

Bien que ces intrusions décrites précédemment aient constitué des attaques sophistiquées et graves, nous n'avons rien détecté d'autre, que ce soit dans les autres parties internes des réseaux de notre activité SIM, isolées du monde extérieur, ou dans les autres parties du réseau sécurisé qui gèrent d'autres produits, tels que les cartes bancaires, les cartes d'identité et les passeports électroniques. Ces réseaux sont isolés les uns des autres et ne sont pas connectés au monde extérieur.

La difficulté d'attaquer à distance un grand nombre de cartes SIM individuellement et l'architecture sécurisée de nos réseaux expliquent le choix de cibler plutôt la phase d'échange de clés entre l'opérateur et ses fournisseurs comme décrit dans les documents de la NSA et du GCHQ.

Le risque d'interception de données lors de l'échange avec nos clients a été grandement réduit avec la généralisation des processus d'échanges hautement sécurisés que Gemalto avait mis en place bien avant 2010. Les documents dévoilés indiquent que les tentatives d'interception de clés ont ciblé des opérateurs en Afghanistan, au Yémen, en Inde, en Serbie, en Iran, en Islande, en Somalie, au Pakistan et au Tadjikistan. Ils disent aussi que lorsque la méthode d'échange des données était forte, la technique d'interception ne fonctionnait pas. Le rapport le souligne en déclarant par exemple que cette technique d'interception « ... a été infructueuse sur les réseaux pakistanais ». Nous pouvons confirmer que les échanges entre Gemalto et ses clients opérateurs du Pakistan étaient déjà hautement sécurisés à cette époque.

En 2010 cependant, ces méthodes n'étaient pas généralisées et certains opérateurs ou certains fournisseurs ne souhaitaient pas les utiliser. Dans le cas de Gemalto, la non utilisation du protocole d'échange sécurisé était exceptionnelle.
L'analyse des documents démontre aussi que les attaques de la NSA et du GCHQ ont eu de nombreuses autres cibles que Gemalto. La position de leader du marché de Gemalto a pu en faire la cible de prédilection présumée de services de renseignement pour atteindre le plus grand nombre de téléphones, mais nous avons relevé plusieurs éléments qui ne concernent pas Gemalto, par exemple :

- Gemalto n'a jamais vendu de cartes SIM à quatre des douze opérateurs cités dans les documents, en particulier l'opérateur somalien auquel 300 000 clés d'authentification auraient été volées.
- Une liste censée localiser nos centres de personnalisation de cartes SIM indique une présence au Japon, en Colombie et en Italie, alors que Gemalto n'avait pas de centre de personnalisation dans ces pays à l'époque.
- La table 2 indique que les fournisseurs de cartes SIM ne représentent que 2% des sources de clés d'encryptage (38/1719), et que l'usage de méthodes d'encryptage fortes par les fournisseurs de SIM fait que les autres groupes (98%) sont nettement plus vulnérables à des tentatives d'interception.

En 2010-2011, la plupart des opérateurs des pays visés utilisaient encore des réseaux 2G. Le niveau de sécurité de la technologie 2G, élaboré dans les années 1980, était déjà considéré comme faible en 2010 et très largement dépassé. Si les

clés de cryptage de cartes SIM 2G étaient interceptées par les services de renseignement, il leur était techniquement possible d'espionner des communications lorsque la carte était utilisée dans le téléphone mobile de l'abonné. C'est une faiblesse connue de l'ancienne technologie 2G et pendant longtemps, nous avons recommandé aux opérateurs le déploiement de mécanismes sécuritaires supplémentaires. En supposant, que les clés aient été interceptées, la capacité à intercepter les appels aurait toutefois été limitée dans le temps, car la plupart des cartes SIM 2G en service à l'époque dans les pays ciblés étaient des cartes prépayées avec un cycle de vie très court, généralement entre 3 et 6 mois.

Cette faiblesse connue des normes 2G a été éliminée avec l'introduction d'algorithmes propriétaires, utilisés à ce jour comme deuxième niveau de sécurité par les grands opérateurs de réseaux. La sécurité a encore été renforcée avec l'arrivée des cartes SIM 3G et 4G dotées d'une protection par cryptage additionnelle. L'interception de clés de cryptage en cours d'échange entre le fournisseur de carte SIM et l'opérateur ne permettrait pas aux pirates de se connecter aux réseaux 3G ou 4G et, par conséquent, ne leur permettrait pas d'espionner des communications. En conséquence, les cartes 3G et 4G ne pouvaient donc pas être affectées par l'attaque décrite. Ces produits plus récents ne sont toutefois pas utilisés universellement dans le monde car ils sont un peu plus onéreux, et parfois, pour l'opérateur, le principal critère d'une décision d'achat peut être le prix.

La sécurité numérique n'est pas statique. Les technologies de pointe perdent de leur efficacité avec le temps, à mesure que des contre-attaques sont mises au point et que la recherche et la puissance de calcul évoluent. Ainsi, les fonctionnalités et les capacités de tous les produits de sécurité réputés sont régulièrement modifiées et mises à niveau. Les cartes SIM ne dérogent pas à la règle et ont constamment été mises à jour au fil du temps, en particulier avec des modifications majeures pour les réseaux 3G et 4G.

La sécurité est encore plus grande pour les opérateurs mobiles qui choisissent de collaborer avec Gemalto pour mettre des algorithmes personnalisés dans leurs cartes SIM. La variété des profils et la fragmentation des technologies algorithmiques employées par nos clients contribuent à augmenter de façon significative la complexité et le coût du déploiement de systèmes d'écoute à l'échelle mondiale. C'est l'une des raisons pour lesquelles nous sommes opposés aux technologies alternatives qui limitent la capacité des opérateurs à déployer des mécanismes sécuritaires personnalisés. Une telle technologie faciliterait l'organisation d'une surveillance de masse si la technologie choisie était malheureusement victime d'une brèche ou d'une défaillance.

Gemalto voudrait réitérer son engagement à fournir le meilleur niveau de sécurité possible pour les applications civiles. Nos produits, notre infrastructure et nos processus sont conçus pour assurer le plus haut niveau de sécurité dans un environnement commercial, ouvert et global. Ceux-ci sont régulièrement audités et certifiés par des tierces parties privées et par des organisations publiques.

Toutefois, Gemalto est bien conscient du fait que les plus éminentes agences d'espionnage, surtout lorsqu'elles font équipe, possèdent des ressources et des appuis juridiques qui dépassent de loin les moyens à la disposition des pirates et autres organisations criminelles ordinaires. Nous restons néanmoins préoccupés par le fait que des autorités d'État aient pu lancer de telles opérations contre des sociétés privées non coupables d'agissements suspects.

Notre priorité actuelle est d'être à l'écoute de nos clients. Nos équipes ont tout particulièrement apprécié le soutien dont ils nous ont fait preuve en cette période inédite, et ces événements ne font que stimuler nos collaborateurs pour travailler encore plus étroitement avec eux à l'élaboration et au déploiement d'applications toujours plus sophistiquées pour répondre au besoin des utilisateurs.

Dans le monde d'aujourd'hui, toute organisation peut être visée par une cyber attaque. Il n'a donc jamais été plus important d'implémenter les bonnes pratiques de sécurité, et d'adopter les technologies comme l'encryptage fort des données qui permet, en cas d'intrusion dans les réseaux, de rendre l'information volée inutilisable par les hackers.

Gemalto continue à surveiller ses réseaux et à améliorer ses processus. Nous n'anticipons pas de communication supplémentaire à ce sujet, à moins que de nouveaux éléments majeurs apparaissent.

À propos de Gemalto

Gemalto (Euronext NL0000400653 GTO) est le leader mondial de la sécurité numérique avec un chiffre d'affaires 2013 de 2,4 milliards d'euros. Présent dans 44 pays, Gemalto emploie plus de 12 000 salariés travaillant depuis 85 bureaux et 25 centres de Recherche et de Développement logiciel.

Nous nous développons au coeur du monde numérique en évolution rapide et constante. Des milliards de personnes à travers le monde revendiquent de plus en plus la liberté de communiquer, acheter, voyager, faire des transactions bancaires, se divertir et travailler – à tout moment et en tous lieux - de façon agréable et sûre. Gemalto répond à leurs demandes croissantes en matière de services mobiles personnels, paiement sécurisé, authentification des accès au « cloud », protection de l'identité et de la vie privée, services d'e-santé et d'e-gouvernement performants, billettique des transports urbains facile d'utilisation et applications M2M fiables. Nous développons des logiciels embarqués et des produits sécurisés que nous concevons et personnalisons. Nos plateformes logicielles et nos services gèrent ces produits, les données confidentielles qu'ils contiennent et les services sécurisés qu'ils rendent possibles pour les utilisateurs finaux.

Nos innovations permettent à nos clients d'offrir des services numériques de confiance et faciles d'utilisation à des milliards de personnes. Gemalto continue de croître avec le nombre grandissant d'utilisateurs de ses solutions pour interagir dans le monde numérique et mobile.

Pour plus d'informations, visitez nos sites www.gemalto.com/france, www.justaskgemalto.com, blog.gemalto.com, ou suivez @GemaltoFrance sur twitter.

Communication financière

Gabriel Rangoni
M. : +33(0) 6 14 26 69 56
gabriel.rangoni@gemalto.com

Communication Corporate

Isabelle Marand
M. : +33(0) 6 14 89 18 17
isabelle.marand@gemalto.com

Agence Relations Media

Catherine Durand-Meddahi
M. : +33(0) 6 08 14 49 70
c.meddahi@agence-influences.fr

Contacts media Gemalto:

Nicole Williams
North America
+1 512 758 8921
nicole.williams@gemalto.com

Vanessa Viala
Europe & CIS
+49 89 210 299 129
vanessa.viala@gemalto.com

Vivian Liang
大中华地区 (Greater China)
+86 1059373046
vivian.liang@gemalto.com

Ernesto Haikewitsch
Latin America
+55 11 5105 9220
ernesto.haikewitsch@gemalto.com

Kristel Teyras
Middle East & Africa
+33 1 55 01 57 89
kristel.teyras@gemalto.com

Pierre Lelievre
Asia Pacific
+65 6317 3802
pierre.lelievre@gemalto.com