【欧州連携センター情報】

2015 年 3 月 3 日

英米諜報機関、ジェムアルトの SIM カード暗号キーを収集

米調査報道サイトの The Intercept は、米国家安全保障局（NSA）による違法個人情報収集を暴露したエドワード・スノーデン氏が新たに明らかにした文書に依拠し、NSA と英情報機関の GCHQ（政府通信本部）が 2010 年と 2011 年に仏ジェムアルト（IC カード）製の SIM カード暗号キーを大量に違法収集していたと報じた。暗号キーは、暗号キーが通信事業者に送信されるところで奪取された模様だという。

それぞれの SIM カードは、通信事業者との通信を暗号化するため、暗号キーを搭載している。データを傍受しても、暗号キーがないと、通信内容の解読は極めて難しい。報道によれば、英米の情報機関は、通信事業者への暗号キーの送信を担当していたジェムアルト従業員を特定し、次いで、その行動を分析することにより、暗号キーの送信が電子メールか FTP プロトコルにより送信されていることを把握した。FTP プロトコルの暗号化は簡単なもので（暗号化されていない場合さえあった）、この経路上で容易に奪取されたという。ある証券アナリストはこれについて、ジェムアルトの暗号キー技術そのものが破られたわけではないが、ジェムアルトの管理体制には問題があったと指摘している。また、The Intercept が明らかにした文書は 2010 年と 2011 年だけを対象としたもので、その後も収集が続けられていた可能性は大きい。英米情報機関による暗号キー収集は、ジェムアルトだけを対象としたものではないのは明らかだが、ジェムアルトは年に 20 億枚の SIM カードを生産し、世界 85 ヵ国の 450 社の通信事業者に納入しており、影響は大きい。

Les Echos 2015-02-23

＜続報＞英米諜報機関の SIM カード暗号キー違法収集問題：ジェムアルトは独自調査を実施

米調査報道サイトの The Intercept が、米国家安全保障局（NSA）と英諜報機関の GCHQ（政府通信本部）が 2010 年と 2011 年に仏 IC カードのジェムアルト製の大量の SIM カード暗号キーを違法収集していたと報じた件について、ジェムアルトは 2 月 23 日、24 日朝に開く記者会見で、社内での独自の調査結果を明らかにすると発表した。24 日朝という設定は、調査に必要な時間を考慮したものだと説明した。同時に、ジェムアルトは、社内調査により、同社の SIM カードそのものは安全だという結果が出ているとし、SIM カード暗号キーの管理体制には問題があったが、同社の技術には問題がないとの見方を強調した。株式市場では、ジェムアルト株価は、2 月 20 日に 3.7%下落したが、23 日には 0.6%の下落に留まり、ジェムアルトからの説明待ちという状況。

通信事業者の側では、ジェムアルトの SIM カードを使用している世界 450 社近くの事業

者のうち多くが既に、ジェムアルトに説明を求めており、例えば、仏通信ブイグ・テレコムは、ジェムアルトによる調査結果の発表を待っているとした。また、ドイツ・テレコムも問題の全貌に関する報告書提出を求めている。NTT ドコモは、問題がユーザーに与えた影響について調査すると示唆した。仏通信オレンジでは、違法収集が行われた時期から見て、対象となったのは 2G 向けカードだが、現在では 2G 向けカードは仏国内にはほとんど存在していない上、現在のセキュリティ措置から見て、同様の事件の再発はあり得ないとの見方を明らかにしている。

Les Echos 2015-02-24

【原文】

Gemalto promet de faire la lumière après son piratage

A. C. ET R. G.

Le groupe livrera les conclusions de son enquête interne mercredi.

Se donner du temps pour mener sa propre enquête. C'est la stratégie adoptée par Gemalto, après les révélations vendredi du site The Intercept, qui, se basant sur de nouveaux documents dévoilés par Edward Snowden, a indiqué que la NSA et le GCHQ, les agences de surveillance américaine et britannique, auraient piraté en masse, autour de 2010, des cartes SIM fabriquées par le groupe français. Celui-ci a promis, dans un communiqué publié hier, de faire toute la lumière sur l'affaire à l'occasion d'une conférence de presse qui se tiendra mercredi matin. 《 Le délai nécessaire pour pouvoir communiquer des choses tangibles 》, indique-t-on dans l'entourage de Gemalto.

Marchés dans l'expectative

Dans l'intervalle, le groupe cherchait hier à relativiser la portée de l'affaire. Les conclusions préliminaires de l'enquête interne《 montrent déjà que les produits SIM de Gemalto […] sont sûrs 》, précisait-il. En conséquence, 《 la société ne s'attend pas à subir un préjudice financier significatif 》. De fait, la technologie de Gemalto serait moins en cause que ses procédures internes.

La sécurité des produits fabriqués par le groupe n'aurait été percée par les services secrets qu'en récupérant les clefs de chiffrement qui équipent les cartes SIM, après avoir espionné les salariés de Gemalto chargés de ces fameuses clefs. Avant de connaître les résultats complets de cette enquête interne, les marchés semblaient encore hier dans l'expectative. Le titre limitait sa chute à 0,6 %, à 69,53 euros à la clôture, après avoir reculé de 3,70 % vendredi.

Chez les opérateurs télécoms, on reste prudent. Près de 450 groupes dans le monde s'équipent en cartes SIM auprès du leader du secteur. Nombre d'entre eux ont pris contact avec Gemalto pour en savoir plus sur l'étendue du piratage.《 On attend les

résultats des analyses qu'ils sont en train de mener 》, confie-t-on chez Bouygues Telecom. Deutsche Telekom a demandé un rapport complet auprès de son fournisseur sur ce qui s'est réellement passé. De l'autre côté de la planète, NTT DoCoMo, le premier opérateur japonais, a indiqué qu'il regardait à quel point ses clients auraient pu être affectés par ce piratage.

Orange tente, quant à lui, de déminer l'affaire.《 Nous avons pris connaissance des informations [publiées]. La période citée concerne les années 2009-2010 et les cartes SIM en question seraient des cartes 2G. Elles sont quasi inexistantes en France à l'heure actuelle. 》En outre, complète un porte-parole,《 les processus de sécurité actuels déployés en France ne permettent pas la réplicabilité d'un tel incident 》. Il n'empêche, l'affaire reste préoccupante pour les opérateurs télécoms qui tentent de pérenniser la relation de tiers de confiance qu'ils entretiennent avec leurs abonnés, en leur garantissant, tant que faire se peut, la sécurité de leurs données privées.

Les Echos-P.22

＜続報＞

Des négligences humaines à l'origine du piratage de Gemalto

SANDRINE CASSINI

La NSA a piraté à grande échelle le fabricant de cartes SIM. Son objectif : écouter les communications interceptées.

Voilà qui donne un sérieux coup de canif à la réputation de celui qui se présente comme le《 leader de la sécurité numérique 》. La NSA et l'agence de surveillance britannique, le GCHQ, auraient piraté en 2010 et en 2011 des quantités industrielles de cartes SIM fabriquées par Gemalto, qui équipent les téléphones portables, a indiqué le site The Intercept, se basant sur de nouveaux documents dévoilés par Edward Snowden. Chaque carte SIM est, en effet, équipée d'une clef de chiffrement, que Gemalto remet à l'opérateur téléphonique. Ce dernier installe ces clefs sur ses équipements, afin de sécuriser les communications. Sans ces clefs, il est très difficile de déchiffrer une communication même si elle est interceptée. Les fichiers contenant les fameuses clefs auraient ainsi été dérobés par les deux agences de renseignements anglo-saxonnes. Celui qui possède ces clefs est ensuite en mesure de facilement déchiffrer les conversations interceptées, ou de lire tous les documents et autres SMS qui transitent sur les mobiles. Pour capter les communications à grande échelle, la NSA passerait par des satellites.

Espionnage des salariés du groupe

Chez Gemalto, l'heure était à la stupéfaction vendredi. 《 Gemalto prend cet article très au sérieux et met en oeuvre tous les moyens nécessaires pour enquêter et comprendre l'étendue de ces techniques sophistiquées 》, s'est contentée de dire l'entreprise dans un communiqué. 《 L'enseignement de l'affaire, c'est que les agences ont profité de la négligence des acteurs 》, se désole Eric Laubacher, directeur innovation- sécurité chez Ercom, fournisseur de produits de sécurité pour les télécommunications.

De fait, les agences ont commencé par repérer puis espionner les salariés de Gemalto chargés de ces fameuses clefs de sécurité. Elles se sont ensuite rendu compte que les fabricants de cartes SIM transféraient les fichiers 《 par e-mail ou via un protocole FTP protégé par une simple méthode de cryptage, qui peut être facilement cassée... voire, occasionnellement sans protection du tout 》, indique le document publié par The Intercept.

Bonne nouvelle, les technologies de Gemalto n'ont donc pas été corrompues par la NSA. En revanche, 《 cela pose la question des procédures de contrôle 》, note Exane. Si les documents dévoilés portent sur les années 2010 et 2011, il n'y a pas de raison que ce piratage à grande échelle se soit arrêté. Les agences auraient ainsi réussi à espionner l'Iran, l'Afghanistan, le Yémen, l'Inde ou la Serbie, mais pas le Pakistan.

Gemalto n'était visiblement pas le seul fabricant visé. Mais c'est un acteur majeur du secteur. Il produit 2 milliards de cartes SIM par an, opère dans 85 pays et fournit 450 opérateurs télécoms, parmi lesquels AT&T, T-Mobile et Verizon.

Les Echos-P.23