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 avions 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

Espionnage Industriel par le Net : nouvelle victime

	Espionnage Industriel par le Net : nouvelle victime

La fuite sur Internet d'emails sur la stratégie et les acquisitions de Snapchat a porté un coup sévère au moral de son patron et fondateur, Evan Spiegel.

Evan Spiegel, le PDG de Snapchat, est une victime collatérale du piratage de Sony Pictures et des fuites de données consécutives. Des emails du dirigeant du studio de cinéma ont été divulgués. Or, celui-ci, en tant qu'administrateur de Snapchat, avait accès à des données confidentielles, qui depuis ne le sont plus tellement.
Et Evan Spiegel a semble-t-il du mal à digérer. Le patron de l'application mobile s'est dit à la fois en colère et dévasté que des informations relatives à la stratégie et au plan de développement de la startup aient ainsi été dévoilées sur Internet.

Le secret indispensable à une startup
« J'ai eu le sentiment que j'allais pleurer toute la matinée, alors je suis sorti marcher et penser à certaines choses » écrit le dirigeant de Snapchat dans un mémo adressé aux salariés de l'entreprise américaine – puis mis en ligne ensuite sur Twitter.
Mais aux Etats-Unis, tout finit presque à ressembler à un scénario hollywoodien… « J'ai même rencontré un de mes professeurs de design du secondaire. Elle m'a serré très fort dans ses bras. J'en avais vraiment besoin » ajoute ainsi Evan Spiegel.
Les fuites sur Snapchat révélaient donc notamment que l'entreprise avait refusé une offre de rachat de trois milliards de dollars de Facebook, mais aussi qu'elle avait procédé à plusieurs acquisitions pour plusieurs millions de dollars, notamment dans le domaine des objets connectés.
« Nous gardons le secret car nous arrivons à faire notre travail libre de tout jugement – jusqu'à ce que nous soyons prêts à le partager. Nous avons des secrets car cela vous donne la possibilité de changer d'avis jusqu'à ce que vous soyez sûr d'avoir fait le bon choix » commente encore le PDG de Snapchat.

Keeping Secrets

I've been feeling a lot of things since our business plans were made public last night. Definitely angry. Definitely devastated.

I felt like I was going to cry all morning, so I went on a walk and thought through a couple of things. I even ran into one of my high school design teachers. She gave me a huge hug. I really needed it.

And I really need to tell you that I'm so proud of all of you. I want to give you all a huge hug because keeping secrets is exhausting.

Keeping secrets means coming home late, after working all day and night. Curling up with your loved ones, hanging out with your friends, and not being able to share all of the incredible things you're working on. It's painful. It's tiring.

Secrets also bring us together.

We keep secrets because we love surprising people. We keep secrets because it's the best way to keep showing the world that growth is not only possible, it's necessary. We keep secrets because it's the right thing to do, not because it's the easy thing to do.

We keep secrets because we get to do our work free from judgment – until we're ready to share it. We keep secrets because keeping secrets gives you space to change your mind until you're really sure that you're right.

We care about taking the time to get things right. Secrets help us do that.

Secrets keep the space between our community and the public – space that we need to feel safe in our expression and creativity.

I am so sorry that our work has been violated and exposed.

A couple of people have asked me what we're going to do.
First we're going to be really mad and angry and upset. And that's ok.

It's not fair that the people who try to build us up and break us down get a glimpse of who we really are. It's not fair that people get to take away all the hard work we've done to surprise our community, family, and friends.

It's not okay that people steal our secrets and make public that which we desire to remain private.

When we're done being mad and angry and upset we're going to keep doing exactly what we are doing. And then we're going to do it ten times better.

We're going to change the world because this is not the one that we want to live in.

Evan Spiegel
December 17, 2014

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.zdnet.fr/actualites/le-patron-de-snapchat-en-colere-et-devaste-39811579.htm

Vol de données : tous les coups sont permis pour piller l’économie française

Vol de données : tous les coups sont permis pour piller l’économie française

Vol d'ordinateur dans des chambres d'hôtel, disparition de brevets dans le Thalys entre Paris et Bruxelles, pénétration d'agents à l'occasion d'une visite, piratage de technologies… Alors qu'une crise endémique tenaille le pays et réveille les appétits les plus féroces, des fleurons de l'économie française font l'objet d'un pillage vertigineux. Animé par un cynique théâtre d'ombres que ne renierait guère John le Carré, il prendrait même depuis vingt ans une forme industrielle. Cet édifiant état des lieux émane d'un rapport choc de la délégation parlementaire au renseignement, composée de parlementaires tous habilités au «secret-défense» et emmenés par le président de la commission des lois à l'Assemblée, le député (PS) Jean-Jacques Urvoas, qui vient d'effectuer une plongée au cœur des services de renseignements et de la sécurité nationale. Ce document de 175 pages, porté à notre connaissance, pointe une «plurivoracité de la prédation économique» liée à une «technicisation de l'espionnage» mais aussi l'«utilisation croissante du vecteur Internet».

Ainsi, l'année dernière, la seule Direction générale de la sécurité intérieure (DGSI) a recensé des «cas d'ingérence», notamment dans le domaine de «la recherche fondamentale, où la culture de la protection est particulièrement faible, mais également dans l'aéronautique et la santé». Dès septembre 2011, les policiers spécialisés de la sous-direction de la protection du patrimoine économique, basée à Levallois-Perret, avaient révélé dans nos colonnes l'existence de près de 5 000 «cas» en quatre ans. Durant cette période, 3 189 entreprises ont été visées. À ce petit jeu, une cohorte de prédateurs occultes pilotée en sous-main par des agences étatiques ou des multinationales s'attaquait à la grande entreprise comme à la plus petite «pépite».

À ce titre, rappelle le rapport de la DPR, «nos principaux partenaires peuvent aussi être nos meilleurs adversaires dans le domaine économique». Sans les citer, les spectres de grandes puissances comme la Chine ou la Russie se profilent entre les lignes. En février dernier, le groupe Safran a été contraint d'épaissir sa cuirasse après des cyberattaques des sites d'une de ses filiales, le motoriste Snecma. «D'une ampleur limitée» et vite décelée, l'intrusion d'origine indéterminée avait conduit les services de sécurité à neutraliser puis retirer une dizaine d'ordinateurs du réseau de l'entreprise. L'Île-de-France, où 144 cas d'ingérence ont été mis au jour en 2013, concentre près de 20 % des attaques. Les secteurs les plus ciblés étant l'aéronautique, l'énergie nucléaire, les télécommunications, l'aérospatiale, la robotique et les machines-outils.

Le droit, un outil de prédation

«Au-delà de cet espionnage industriel dont l'existence est connue, mais dont les méthodes continuent malheureusement de surprendre des entreprises et des administrations insuffisamment armées, il serait naïf d'oublier que les principales ingérences empruntent aujourd'hui des voies légales», précise le rapport, qui brocarde sans détour les États-Unis, lesquels – ce ne sont pas les seuls – utilisent le «droit comme un puissant instrument de prédation». Ainsi, le rapport détaille la redoutable procédure Discovery, fondée sur le principe fondamental de la common law américaine permettant à un «plaignant d'adresser des demandes de pièces au défendeur afin de cibler son action en justice». Or, les demandes s'avèrent bien souvent extraordinairement vastes (d'où leur surnom de fishing expeditions, «parties de pêche») et peuvent procéder d'une volonté de profiter de cette procédure pour se livrer légalement à de l'espionnage économique. Il en est de même pour le deal of justice, qui permet au Department of Justice (DOJ) d'éperonner de grandes entreprises pour infraction aux lois états-uniennes en matière de corruption qui «s'appuie principalement sur le Foreign Corrupt Practices Act de 1977 et sur les lois de sanctions économiques contre des pays (Cuba, Iran, Libye, Soudan, Syrie…)».

Cette fine mouche peut recopier la comptabilité, lire les échanges de mails, compulser la documentation stratégique, exiger de savoir à quoi correspond chaque dollar dépensé en frais professionnels par un cadre à l'étranger.

«Dans 90 % des cas, il s'agit d'entreprises étrangères, dont certains grands groupes français, à l'image de la récente affaire impliquant BNP Paribas», souligne le rapport. La banque, accusée de transactions avec des pays sous embargo économique américain, avait accepté le 30 juin, devant un tribunal de New York, deux chefs d'accusation: «falsification de documents commerciaux» et «collusion» avant d'écoper de 6,5 milliards d'euros d'amende. «L'entreprise doit reconnaître sa culpabilité et négocier le montant de l'amende infligée. En contrepartie, le DOJ renonce aux poursuites pour une période de trois ans, période pendant laquelle l'entreprise doit faire preuve d'un comportement exemplaire, note le rapport. Pour prouver sa bonne foi, et là réside le principal problème, elle doit accepter la mise en place d'un moniteur en son sein, moniteur qu'elle choisit mais dont la désignation définitive est soumise à l'approbation des États-Unis. Le moniteur aura accès à l'intégralité des informations de l'entreprise afin de rédiger un rapport annuel extrêmement détaillé.»

Cette fine mouche peut recopier la comptabilité, lire les échanges de mails, compulser la documentation stratégique, exiger de savoir à quoi correspond chaque dollar dépensé en frais professionnels par un cadre à l'étranger. Ou encore, ce qui n'est pas la moindre affaire, dévoiler les démarches concurrentielles à l'étranger. Or, révèle la délégation parlementaire, les services secrets américains peuvent «solliciter toute information nécessaire, y compris les rapports de monitorat» en invoquant le Foreign Intelligence Surveillance Act. En clair, le droit sert de bélier pour forcer la protection et les espions passent derrière pour siphonner le savoir-faire français. Selon nos informations, un grand groupe énergétique français et un tycoon pétrochimique allemand ont récemment subi pareil traitement après avoir versé plusieurs milliards de dollars. Alors qu'aux États-Unis les services secrets et le business entretiennent des relations fusionnelles et souvent consanguines, au point que la CIA a créé et gère le fonds d'investissement In-Q-Tel permettant de capter de précieuses informations concurrentielles. Une source informée confie qu'une PME française développant un logiciel performant a été «tamponnée», sans succès, par cette structure qui lui proposait d'entrer dans son capital.

Proposition de loi sur le secret des affaires

Parmi les propositions très concrètes formulées pour défendre le système immunitaire des entreprises françaises, la Délégation parlementaire au renseignement suggère de jeter enfin les bases d'un dispositif national protégeant le secret des affaires. Évoquée de façon éparse et fragmentaire dans la charte des droits fondamentaux de l'Union européenne, le Code du commerce ou celui des postes et télécommunications, cette notion «n'a pas d'existence juridique stabilisée ni de définition uniforme», note le rapport. Ainsi, en droit, la définition du vol n'intègre pas les biens immatériels. Et, pour l'heure, le délit de révélation d'un secret de fabrique ne concerne que les seuls salariés de l'entreprise. Face à un arsenal répressif lacunaire, Jean-Jacques Urvoas a donc concocté une proposition de loi, déposée en juillet dernier et présentée mercredi devant le Medef, permettant d'inscrire dans le Code du commerce un titre en neuf articles sur le «secret des affaires». Protégeant le potentiel scientifique et technique, les positions stratégiques, les intérêts commerciaux et financiers ainsi que la capacité concurrentielle des entreprises, cette loi prévoit des sanctions pouvant aller jusqu'à sept ans d'emprisonnement et 750.000 euros d'amendes dès lors que la souveraineté nationale est en jeu.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.lefigaro.fr/conjoncture/2014/12/18/20002-20141218ARTFIG00005-espionnage-comment-on-pille-l-economie-francaise.php
par Christophe Cornevin