Le régulateur mondial d’internet victime d’une attaque informatique

Le régulateur mondial d’internet victime d’une attaque informatique

Le régulateur mondial d’internet, l’Icann, a annoncé que des pirates informatiques avaient réussi à pénétrer dans ses ordinateurs.

Une attaque par « hameçonnage » a en effet visé l’agence américaine et plusieurs de ses employés ont reçu des courriels destinés à ressembler à ceux envoyés par un de leurs collègues avec une adresse se terminant en « icann.org », selon le blog de l’Icann.

« Plusieurs employés ont vu leurs références dérobées », a précisé l’agence.
L’attaque a, semble-t-il, commencé en novembre. Typiquement, les attaques par hameçonnage sont destinées à duper les gens en les conduisant à cliquer sur des pages factices où ils rentrent leurs adresses et mots de passe, qui sont ainsi récupérés par les pirates informatiques.
Cette ruse a permis aux hackers de récupérer les adresses et mots de passe de plusieurs employés de l’Icann. Ils ont donc pu s’introduire plus avant au sein du système informatique de l’organisation.
Ils ont ainsi pu pénétrer dans des serveurs sécurisés où ils ont récupéré des dossiers sur des noms de domaines, des adresses et des mots de passe d’utilisateurs, a encore indiqué l’Icann.
Le blog et l’annuaire n’ont pas été trafiqués, a encore noté l’Icann sans préciser qui pourrait être à l’origine de l’attaque.
L’Icann, dont la mission est d’attribuer les noms de domaines des sites internet, devrait quitter le giron américain en fin d’année prochaine. Washington a en effet annoncé en mars qu’il pourrait ne pas renouveler son contrat avec la société basée à Los Angeles si un système de contrôle indépendant est en place pour assurer la fiabilité du système d’attribution des adresses.

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

Source : http://www.7sur7.be/7s7/fr/4134/Internet/article/detail/2156470/2014/12/18/Le-regulateur-mondial-d-internet-victime-d-une-attaque-informatique.dhtml

---

Live streaming illégal : un coût considérable pour

l’économie mondiale

	**Live streaming illégal : un coût considérable pour l’économie mondiale**

Une étude du Center for Strategic and Internationals Studies (CSIS) faisait grand bruit lors de sa sortie, en juin dernier. Elle évaluait à 445 milliards de dollars, soit 327 milliards d'euros, le coût global de la cybercriminalité sur l'économie mondiale. S'il semble compliqué de lutter contre ce fléau sans visage, la limitation de certains comportements à risque permettrait de réduire substantiellement la note pour les industries du secteur, mais aussi et surtout pour les internautes. Ainsi en va-t-il du live streaming illégal, plébiscité mais toxique.

Radiographie de la cybercriminalité mondiale

Sans surprise, les pays les plus exposés aux méfaits des cybercriminels sont les grandes puissances. A eux seuls, Etats-Unis, Chine et Allemagne concentrent 200 milliards de pertes dues à des piratages en tout genre, même si essentiellement par vol de propriété intellectuelle.

L'importance des dégâts commis par les hackers est inversement proportionnelle au nombre d'entre eux capables de conceptualiser des programmes permettant d'exploiter des failles logicielles connues (exploits). Selon le Centre de lutte contre la Cybercriminalité d'Europol, seule une centaine de personnes serait responsable de la cybercriminalité dans le monde. Autrement dit, si d'innombrables réseaux cybercriminels s'approprient les kits d'exploits et malwares créés par d'autres, ils ne sont qu'une poignée à pouvoir être considérés comme les cerveaux du hacking international.

Europol précise que ces kits et malwares sont à ce point élaborés qu'ils peuvent facilement être adaptés aux cibles spécifiques des cybercriminels. Des cibles qui sont souvent des entreprises dont les solutions de sécurité laissent à désirer, mais aussi des particuliers, notamment via leur utilisation du live-streaming illégal, véritables supermarchés pour les hackers, qui n'ont qu'à se pencher pour se servir.

Le live streaming illégal, tête de pont de la cybercriminalité mondiale

Début octobre, l'Association of Internet Security Professionals (AISP) se fendait d'un rapport alarmant. Intitulé « Illegal Streaming and Cyber Security Risks : a dangerous status quo ? » il montrait que 500 millions d'ordinateurs étaient infectés dans le monde, soit une infection toutes les 18 secondes.

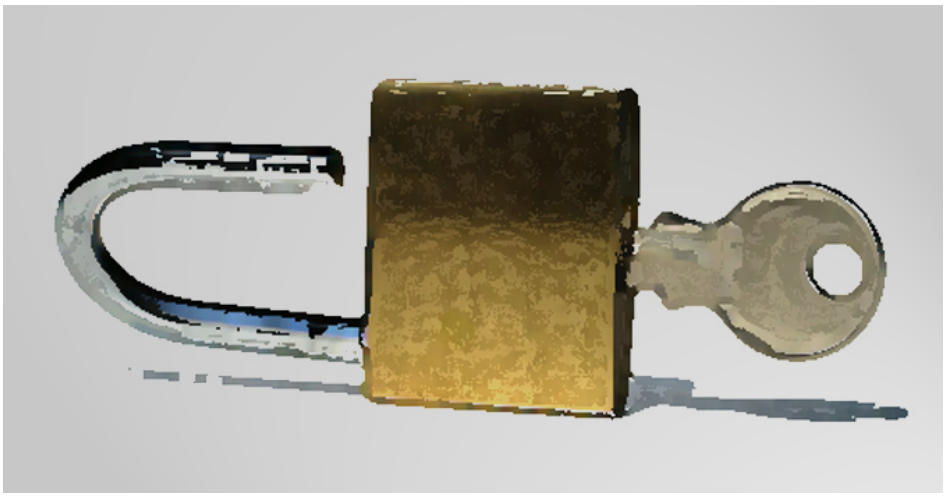
Concernant les sites de live streaming illégaux, type retransmission de matchs de sport, le rapport de l'AISP se fait très précis. Selon lui, 80 % de ces plateformes hébergeraient des malwares, visant à subtiliser des données confidentielles aux personnes les fréquentant. Avec pour but, in fine, de bombarder leurs boites mails de spams, de subtiliser leurs codes bancaires ou encore d'usurper leur identité.

67 milliards de dollars sont dépensés par an en achat de services de sécurité sur Internet. Cette somme pourrait être considérablement réduite si les internautes prenaient conscience des risques encourus en surfant, par exemple, sur des sites de live streaming illégaux.

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

Source : http://www.actu-economie.com/2014/12/18/live-streaming-illegal-cout-considerable-leconomie-mondiale/
Par Christophe Fourrier

Les Français choisissent très mal leurs mots de passe



Les Français choisissent très mal leurs mots de passe

Selon Dashlane qui a réalisé une étude statistique basée sur 70 000 utilisateurs dans le monde, les Français seraient en Europe ceux qui choisissent le moins bien leur mot de passe, du point de vue des recommandations sur la sécurité.

Le prestataire Dashlane, qui propose un gestionnaire de mots de passe, a publié les résultats d'une étude réalisée en analysant la robustesse des mots de passe choisis par 70 000 clients sur les différents sites internet où ils s'inscrivent et s'identifient. En moyenne, les Français obtiennent la pire note d'Europe avec 58 points sur 100, loin derrière les 67 points obtenus par les Allemands. La France fait cependant mieux que les Etats-Unis, qui ferme la marche du classement mondial avec seulement 52 points.
Le score est calculé en prenant en compte différents critères positifs ou négatifs comme sa longueur (plus c'est long plus c'est bon), la présence de caractères spéciaux qui évitent les attaques par dictionnaire de mots, ou encore le choix de mots de passe à fuir comme 12345, motdepasse, azerty, etc.
En tirant un peu fort sur les conclusions, la société y voit la manifestation d'une différence culturelle entre des Allemands préoccupés par la protection de leur vie privée du fait de leurs souvenirs de la Stasi, alors que les Américains chercheraient avant tout l'efficacité et la rapidité. « Outre-Rhin, la sensibilité à la sécurité et à la vie privée est très développée tandis qu'aux Etats-Unis les risques sont minimisés au profit des opportunités », analyse Guillaume Desnoes, directeur de Dashlane pour l'Europe.

L'INTERNAUTE N'EST PAS LE COUPABLE
« Concernant la France, outre ses particularités culturelles, il est nécessaire de pointer du doigt le manque de pragmatisme des pouvoirs publics qui agissent peu sur le front de la sécurité en ligne se contentant surtout de publier des alertes. On est loin du modèle britannique où le gouvernement a investi 5M£ par an dans les campagnes « Cyber Streetwise » et « Get Safe Online ! » », dénonce-t-il.
Statistiquement, les femmes en France veilleraient légèrement mieux que les hommes à choisir un mot de passe plus sûr (60 points), et surtout les jeunes semblent mieux sensibilisés, avec un score de 65 points pour les moins de 25 ans. Les scores sont toutefois relativement proches, et dénotent une faiblesse générale dans le choix des mots de passe.
Or c'est une autre étude de Dashlane, beaucoup plus intéressante à nos yeux, qui montrait en juillet dernier la responsabilité des éditeurs de sites internet eux-même dans le choix des mots de passe. Résumée par l'infographie ci-dessous, elle montrait que des sites pourtant très réputés et très sensibles comme Amazon (qui stocke le numéro de carte bleue), Meetic ou ShowroomPrivé avaient une politique beaucoup trop laxiste face aux choix de leurs utilisateurs, alors qu'Apple et Microsoft étaient les meilleurs élèves.

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

Source : http://www.numerama.com/magazine/31636-les-francais-choisissent-tres-mal-leurs-mots-de-passe.html

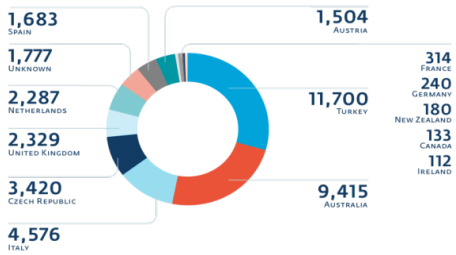
Détection d’une grande famille de malware et découverte de son mode opératoire

	Détection d’une grande famille de malware et découverte de son mode opératoire

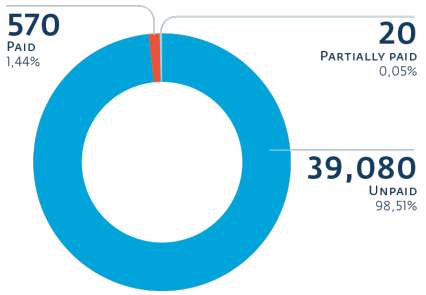
La nouvelle variante de ransomware TorrentLocker atteint en 2014 plus de 40 000 systèmes informatiques européens.

Quelles sont les caractéristiques de cette nouvelle variante ?
L'équipe de chercheurs canadienne ESET, spécialisée en menaces cybercriminelles, a découvert que depuis le début de l'année 2014, des attaques de ransomware du nom de TorrentLocker se propageaient partout en Europe. Cette variante identifiée par ESET comme Win32/Filecoder.Dl, appartient à la famille des ransomware. Il paraîtrait que les acteurs cachés derrière ce malware seraient de la même famille que le cheval de Troie bancaire : Hesperbot. Sa méthode change en revanche, puisque qu'il passe de la norme AES (Advanced Ecryption Standards) du chiffrement basé sur un compteur (CTR) au chiffrement d'enchaînement des blocs (Cipher Block Chaining, CBC)..
Le logiciel malveillant s'introduit malicieusement dans le système d'exploitation de sa victime, via des liens infiltrés eux-mêmes dans des e-mails frauduleux. Le logiciel crypte ensuite les données de l'ordinateur. Les documents, photographies et autres fichiers sont alors inutilisables pour le propriétaire. Le hacker peut aussitôt demander à la victime de payer une rançon si elle ne veut pas que ses données soient détruites. Les sommes demandées sont considérables, pouvant atteindre les 1200€. Pour déverrouiller ces données, la victime a besoin d'un code de déchiffrement que seul le pirate peut lui fournir et sans garantie.

Des techniques de persuasion toujours plus performantes
Les propriétaires de ces logiciels malveillants savent être de plus en plus convaincants en ciblant le message en fonction des pays qu'ils convoitent. Ils savent de mieux en mieux personnaliser et adapter leur message sur leurs cibles. Par conséquent, ils sont de plus en plus dangereux, car ces « faux » e-mails sont de plus en plus difficile à détecter pour les victimes.
Les acteurs de ce logiciel malveillant utilisent de nombreuses ruses pour convaincre les internautes. Ils envoient des messages personnalisés, en mimant la provenance d'un organisme certifié. Ils en profitent ensuite pour réclamer le paiement d'une fausse facture. Ils arrivent même à troubler les internautes en allant jusqu'à insérer des images de CAPTCHA.



Nombre de victimes ayant payé les cybercriminels pour le logiciel
Des conséquences irrémédiables, attention à ne pas les encourager !
La dernière vague de TorrentLocker a atteint 40 000 ordinateurs, représentant 280 millions de documents chiffrés en Europe, Canada, Australie et Nouvelle-Zélande. Près de 600 victimes ont payé la rançon, ce qui a fait gagner 481 578€ aux malfaiteurs en Bitcoins! En France, Torrentlocker a intercepté 2 170 247 fichiers avec une demande de rançon d'au minimum 830€.



Nombre de victimes ayant payé les cybercriminels pour le logiciel
L'équipe de chercheurs canadiens ESET a su démanteler TorrentLocker en localisant le malware grâce aux serveurs C&C qui généraient des URL pour les pages d'échanges d'argent avec les victimes.
La première règle à prendre en considération est qu'il faut d'une part protéger ses appareils que ce soit un PC, un Mac, un smartphone ou une tablette sous Android. Ensuite il faut veiller à ne pas ouvrir des e-mails inconnus ou paraissant suspects et surtout ne pas cliquer sur un lien trop rapidement ni ouvrir la pièce jointe. Le conseil à retenir est de ne pas payer les rançons demandées, ce qui encourage les pirates et les entraîne à développer leurs logiciels malveillants.

Les actualités sur Torrentlocker
Le logiciel malveillant est en constante évolution, l'équipe de sécurité ESET a mis en place un livre blanc, où elle publie régulièrement leurs analyses et informe sur les nouvelles apparences que prend le logiciel au fil du temps, disponible sur www.welivesecurity.com.
Pour plus d'informations sur TorrentLocker, vous pouvez consulter le livre blanc sur
http://presse.marketing-land.com/r/?F=23e5g9n2ctsdr5hy9tpgyh7gqgazh6hj3y38q6ds3xp5zm8q23sfj4q-5686679

Au travers de conférences ou de formations, Denis JACOPINI vous propose de vous sensibiliser, responsable de la stratégie de l'entreprise qui DOIT désormais intégrer le risque informatique comme un fléau à combattre et à enrayer plutôt qu'une fatalité.
Contactez-nous

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

Source : https://mail.google.com/mail/u/0/?hl=fr&shva=1#inbox/14a6329542c28f29

Reprenez le contrôle de votre identité en ligne

Reprenez le contrôle de votre identité en ligne

Quand on s'inscrit avec un des géants du web comme Google ou Facebook. On souscrit à beaucoup plus qu'un seul service. On peut par exemple utiliser les mêmes identifiants pour s'enregistrer partout sur le web. C'est très pratique. Sauf que si votre compte se fait un jour pirater ou supprimer, vous perdez votre mail et tous les accès aux différents services que vous utilisez. IndieHosters veut vous aider à reprendre le contrôle de votre identité en ligne sans perdre le côté pratique.

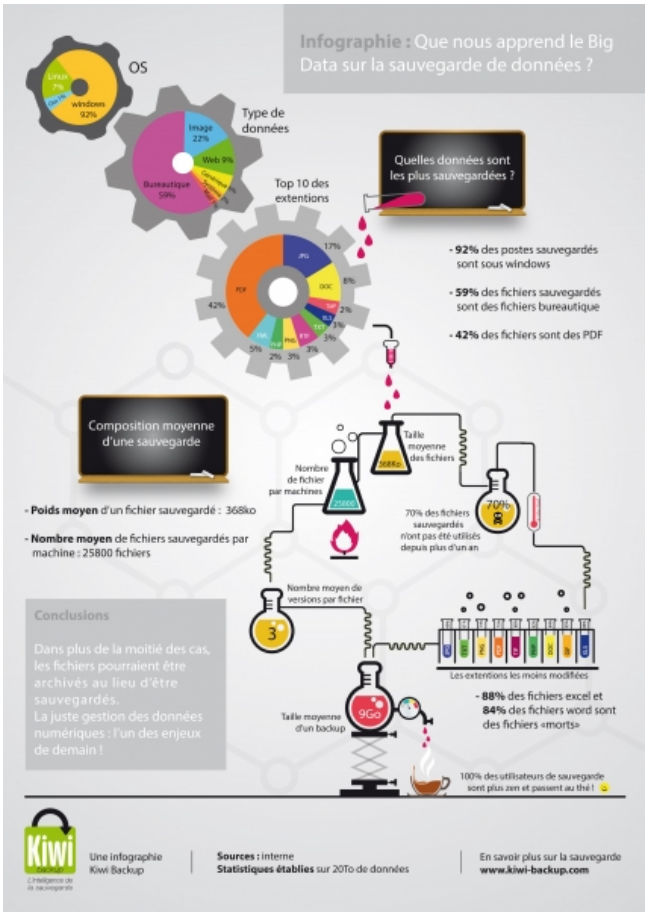
Il existe de nombreuses alternatives aux identifications de Facebook et Google. Elles s'appellent OpenID ou Mozilla Personna. Le problème avec ces outils, c'est qu'ils demandent d'être hébergés sur un serveur en ligne et qu'ils doivent être régulièrement mis à jour. Les compétences techniques demandées dépassent bien souvent les bases des internautes avertis et c'est une galère qui décourage même les utilisateurs les plus motivés.
Aujourd'hui, si vous allez chez un hébergeur connu comme OVH ou Gandi, vous aurez droit en un seul clic à une adresse mail, un hébergement pour un site web, une base de données et WordPress ou quelques logiciels libres.
IndieHosters veut aller encore plus loin en proposant tous les outils qui vous permettent de gérer votre identité en ligne. Et pour garantir la confidentialité des données, ils vous offrent en prime un certificat TSL (identique à celui utilisé pour les opérations bancaires en ligne par exemple). Vos données vous appartiennent et elles ne sont pas accessibles pour l'hébergeur. Et comme vous bénéficiez d'un serveur chez IndieHosters, vous pouvez également en profiter pour créer votre blog.

Lire la suite….

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

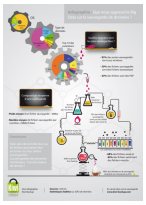
Source : http://www.gizmodo.fr/2014/12/18/reprenez-le-controle-de-votre-identite-en-ligne-avec-indiehosters.html

Sauvegarde des données et Big Data



Sauvegarde des données et Big Data

Infographie réalisée à partir de l'analyse de 20 To de données sauvegardées.
Que nous apprend le Big Data sur l'usage de la sauvegarde de données ?Des chiffres instructifs sont issus de cette analyse :
92 % des postes sauvegardés sont sous Windows,
Près de 60 % des fichiers sont des fichiers bureautiques (excel, word, PDF…),
42 % des fichiers sont des PDF,
70 % des fichiers sauvegardés n'ont pas été modifiés depuis plus de 1 an,
80 % des fichiers Excel et 84 % des fichiers Word n'ont pas été modifiés depuis plus de 1 an,
368 Ko : c'est le poids moyen d'un fichier sauvegardé,
9 Go : c'est le volume moyen d'un back-up.



Quelles conclusions peut-on tirer de cette infographie ?
Dans bien des cas, l'archivage serait plus approprié que la sauvegarde. Car pourquoi sauvegarder en incrémentiel un fichier qui ne bouge pas pendant des mois et peut être considéré comme un fichier « mort » ?
Le poids des PDF est extrêmement important et pourrait être réduit en sauvegardant les fichiers source uniquement et les PDF ayant une valeur juridique (contrats signés, devis,…)
Nous produisons beaucoup de fichiers bureautiques qui deviennent rapidement obsolètes et qui pourraient faire l'objet d'un « toilettage » plus régulier
La sauvegarde en ligne incrémentale est un outil puissant et complexe, permettant de sauvegarder plusieurs versions d'un même fichier sans augmenter l'espace de stockage nécessaire. Mais est-elle toujours utilisée à bon escient ? Une révision des critères de sauvegarde devrait être réalisée à intervalle régulier afin de ne pas engorger le cloud de fichiers qui ne seront jamais restaurés.

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

Source : http://www.journaldunet.com/solutions/expert/59471/sauvegarde-de-donnees-et-big-data.shtml

---

Denis JACOPINI et son équipe considère la sauvegarde comme la colonne vertébrale du système informatique. En ces temps quasiment 100% numériques, en cas de sérieux problème (panne, erreur de manipulation, acte malveillant, sinistre), la sauvegarde deviendra la source d'information la plus précieuse au monde.
Selon Denis JACOPINI, une sauvegarde de données doit être :
Automatisée : Pour ne plus oublier de sauvegarder, pour que la machine, bête comme une machine, y pense à notre place.

Contrôlée : J'ai rencontré trop de cas ou pendant des années des professionnels, avaient des systèmes de sauvegardes sur lesquels rien ne se sauvait, une panne avait interrompu le processus de sauvegarde depuis plusieurs mois ou pire, ne sauvegardaient que les raccourcis.
C'est la raison pour laquelle nous accordons beaucoup d'importance à notre audit des besoins, en communication rapprochée avec les éditeurs des différents logiciels créeant de la donnée dans l'entreprise, pour mettre en corrélation le « A sauver », le « Sauvé ».
Nous formons ensuite le client sur l'interprétation des rapports de sauvegarde qu'il va lui même contrôler (s'il ne souhaite pas souscrire à notre offre de contrôle des sauvegardes par nos services). l devient alors à même de savoir que ça fonctionne parfaitement.
Lorsqu'un dysfonctionnement apparait, il en est immédiatement informé. Cette rapidité d'alerte permet ensuite d'avoir du temps pour analyser le problème et le résoudre.

Externalisée : Un vol de l'ensemble de votre matériel informatique et du système de sauvegarde ne , vous met pas à l'abris d'une perte de vos données, de même qu'un sinistre…
Externaliser vos sauvegarde tout en y apportant la sécurité adaptée, vous permettra, même en cas de perte ou de destruction totale de votre système informatique, d'avoir accès à vos données à distance et de pouvoir recommencer à travaille en un temps record.

Historisée : En sauvegardant vos données sur plusieurs supports que vous faites tourner (le nombre de support dépendra du niveau de sécurité souhaité), vous pourrez, selon les paramètres choisis, retrouver un fichier effacé depuis plusieurs mois, qui ne se trouve évidemment plus sur les sauvegardes récentes. Cette fonction est très utile lorsque des données sont régulièrement effacées des systèmes informatiques. Il permet de retrouver le contenu d'une sauvegarde antérieure.

Parmi l'ensemble des logiciels gratuits et payants testés, nous avons à ce jour trouvé un produit qui non seulement regroupe l'ensemble des exigences répertoriées ci-dessus, mais également a été testé sur des nombreuses installations, plateformes et ne nous a toujours donné satisfaction.
Il peut sauver sur n'importe quel support, local réseau, ftp, cloud… et vous envoie le rapport de sauvegarde par e-mail. Des solutions existent même pour que vous soyez alerté des sauvegardes par SMS.
En plus, pour moins de 50 euros, je ne peux que vous conseiller ce produit : SyncBack

---

Confidentialité des donnés : 71 % des employés déclarent avoir accès à des informations qu'ils ne devraient pas voir

Confidentialité des donnés : 71 % des employés déclarent avoir accès à des informations qu'ils ne devraient pas voir

Une enquête de Ponemon Institute pour la société Varonis systems Inc révèle que les employés disposant d'accès excessifs aux données de l'entreprise représentent un risque de fuites. Cependant, moins d'un collaborateur sur quatre estime que leur entreprise accorde une priorité très élevée à la protection de ses données.

Une étude* commandée par Varonis Systems Inc, une société qui fournit des solutions logicielles pour les entreprises, et réalisée par le Ponemon Institute, un centre de recherche sur la confidentialité, la protection des données et les politiques de sécurité de l'information, révèle que la plupart des entreprises rencontrent des difficultés à trouver l'équilibre entre un besoin de sécurité renforcée et les exigences de productivité des salariés. L'étude précise que les employés qui disposent de privilèges excessifs d'accès aux données représentent un risque croissant pour les entreprises en raison de l'exposition accidentelle et intentionnelle d'informations sensibles ou critiques. 71 % des utilisateurs finaux indiquent avoir accès à des données de l'entreprise qu'ils ne devraient pas pouvoir consulter et 54 % de ces utilisateurs caractérisent ces accès comme fréquents ou très fréquents.

Productivité contre sécurité

Les informaticiens comme les utilisateurs finaux témoignent d'un manque de contrôle en ce qui concerne l'accès aux données et leur utilisation par les employés. Les deux groupes conviennent généralement du fait que leur entreprise préférerait négliger les risques de sécurité plutôt que sacrifier la productivité. Seulement 22 % des collaborateurs ayant participé à l'enquête estiment que leur entreprise accorde une priorité très élevée à la protection de ses données. Moins de la moitié des employés pensent que leur société applique des politiques de sécurité strictes en ce qui concerne l'utilisation et l'accès aux données.

Des fuites dues à la malveillance des collaborateurs

Les conclusions de l'enquête indiquent également que les informaticiens et les utilisateurs finaux s'accordent sur le fait que les comptes d'employés détournés pouvant conduire à des fuites de données sont très probablement le fait de collaborateurs internes disposant d'accès excessifs et souvent inconscients des risques que ceux-ci représentent. 50 % des utilisateurs finaux et 74 % des informaticiens estiment que les erreurs, les négligences ou la malveillance d'employés sont fréquemment ou très fréquemment à l'origine des fuites de données. Et seulement 47 % des informaticiens indiquent que les employés de leur entreprise prennent des mesures appropriées pour protéger les données auxquelles ils accèdent.

Dans le même temps, 76 % des utilisateurs finaux indiquent que leur travail exige l'accès et l'emploi d'informations de l'entreprise telles que des données relatives aux clients, des renseignements sur les collaborateurs, des rapports financiers et des documents commerciaux confidentiels. Et, 76 % des utilisateurs finaux jugent qu'il est parfois acceptable de transférer des documents de travail sur leurs périphériques personnels, alors que seulement 13 % des informaticiens en conviennent.

*Le rapport d'étude intitulé "Données : actifs protégés ou bombe à retardement ?" se fonde sur des entretiens menés en octobre 2014 auprès de 2 276 employés aux États-Unis, au Royaume-Uni, en France et en Allemagne.

Source : http://www.courriercadres.com/carriere/internet-et-l-entreprise/securite-des-donnes-71-des-employes-declarent-avoir-acces-15122014

Par Audrey Pelé

Votre smartphone vous épie à

votre insu

Votre smartphone vous épie à votre insu

Une nouvelle étude de la Cnil publiée ce lundi souligne que deux tiers des applications pour smartphones collectent des informations personnelles auxquelles elles ne devraient pas avoir accès et sans que les utilisateurs en aient conscience. L'étude démontre que nos téléphones sont devenus de vrais petits espions domestiques.

Un nouveau rapport de la CNIL (Commission nationale de l'informatique et des libertés) publié ce lundi montre que les accès aux données personnelles des utilisateurs sont massifs et peu visibles par le citoyen mal informé. Deux applications sur trois captent des informations personnelles à l'insu des utilisateurs. Et l'augmentation du temps passé par les citoyens (de 2 à 4 heures par jour) sur leur portable augmente les risques de fuites de ce type de données.
La CNIL appelle de nouveau les éditeurs d'applications et leurs fournisseurs de services ou partenaires commerciaux à intensifier leur effort d'information des utilisateurs, sans s'abriter derrière des contraintes techniques. Apple, Google, Microsoft, Mozilla seraient les premiers visés.
La CNIL soulignait déjà en 2011 que la confidentialité des données personnelles des internautes n'est pas respectée par les géants du Web. Mais la tendance se renforce. La CNIL a conduit cette nouvelle étude avec l'aide de l'Inria, qui a installé l'outil d'analyse Mobilitics sur des Smartphones que des agents de la CNIL ont utilisé à la place de leurs téléphones personnels. L'étude, menée pendant trois mois, a passé au crible 121 applications Android (plus de 70% du marché des smartphones en France). Et les résultats sont édifiants.
L'étude a permis de dégager trois éléments majeurs. Les identifiants techniques, matériels ou logiciels sont utilisés à des fins publicitaires dans plus de 50% des cas. Les smartphones sont également de vrais « GPS de poche » et certaines applications ne se privent pas d'accéder à ces données qui dévoilent où nous nous trouvons, même lorsque l'abonné n'est pas en train d'utiliser l'application en question. La géolocalisation représente 30% des données collectées chez les utilisateurs. Parmi les 121 applications scrutées par la Commission, cinq ont même accédé au numéro de téléphone de l'utilisateur et deux ont pu récupérer la liste des identifiants des points d'accès WiFi à portée de l'utilisateur.
Si vous croyez encore que le maître à bord de votre smarthpone c'est vous, ce dernier élément va achever de vous convaincre. L'éditeur du système d'exploitation définit ce que les éditeurs d'applications sont autorisés à collecter ou non. Et si la CNIL condamne de nouveau les utilisations outrancières qui sont faites des données personnelles, elle a en réalité peu d'influence face au poids économique que représente pour les géants du Web la collecte de nos données personnelles.

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

Source : http://www.francesoir.fr/societe-science-tech/votre-smartphone-vous-epie-votre-insu
par la rédaction de FranceSoir.fr

La protection des données médicales web 3.0

La protection des données médicales web 3.0

Par Murielle CAHEN – Avocat

L'avènement du web dit 3.0 laisse place à un constat évident : la quasi-totalité des objets disposent aujourd'hui d'une connexion à l'Internet. Dans cette ère du tout connecté où les flux sont incessants, une catégorie de données reste cependant sujette à une attention particulière : les données dites personnelles, regroupant en leur sein les données médicales.

Avant toute chose, il apparait plus aisé de définir plus précisément ce que l'on entend par une donnée médicale. Dans un premier temps, cette dernière n'est pas nécessairement informatique : une donnée peut en effet être archivée sous la forme d'un écrit. Il en va ainsi des certificats médicaux ou des ordonnances. Ainsi, le terme de donnée médicale englobe tout ce qui a attrait à une méthode de conservation de l'état de santé d'un patient : la question de la protection des données médicales, avec les règles de déontologie et de respect de la vie privée s'y afférant, n'est donc pas récente.

Or l'évolution fulgurante des technologies informatiques peuvent constituer un danger pour la protection des données de santé. Ainsi, ces dernières peuvent se voir perdues, corrompues, détruites voire même détournées. Ainsi, le récent cas de suicide du prévenu suspecté d'avoir volé le dossier médical de Michael Schumacher rappelle que les données médicales, du fait de leur caractère éminemment personnel, restent des données sensibles devant faire l'objet d'une protection particulière.

La France est pionnière en la matière puisqu'elle dispose de ce fait d'un régime juridique protégeant l'ensemble des données personnelles. Ce régime date de la loi du 06 janvier 1978. L'objectif principal de cette loi est d'assurer la sécurité du traitement des données à caractère personnel. Parmi ces dernières on y trouve les données médicales qui font également l'objet de dispositions particulières : le code de la santé publique protège les données médicales, et notamment leur traitement par les professionnels de santé.
Cependant, une donnée informatique est, par définition, immatérielle. Elle suppose donc une localisation sur un serveur. Hélas, dans le cas où un ressortissant français tombe malade dans un pays étranger et est soigné là bas, ses données médicales ne seront pas situés sur le territoire national. La loi française ne s'appliquant que sur le territoire français, le régime de protection des données médicales pourra se voir alors modifié, et certaines atteintes à la confidentialité de données de santé seront peut être tolérées alors qu'elles constituent une infraction au droit français. Dès lors, quelle est la réelle portée juridique de la protection des données médicales à la fois au plan national et international? L'évolution récente de certaines technologies informatiques peut elle rentrer en contradiction avec la confidentialité de données si sensibles?

I. Une protection des données médicales encadrée au plan national.
Il en va de soit, mais la France possède un régime juridique particulier sur la protection des données médicales, ce dit régime étant particulièrement efficace. De plus, la CNIL assure une surveillance particulière des dites données et elle délivre régulièrement des informations pratiques destinés à renseigner les professionnels de la santé.

A. Un cadre juridique et réglementaire efficace.
Comme dit précédemment, la France s'est dotée la première d'un régime juridique spécifique aux données personnelles et à l'utilisation des données personnelles. En effet, la loi dite Informatique et Liberté promulguée le 06 janvier 1978 a pour objet spécifique de protéger le traitement des données à caractère personnel. Comme indiqué ci-dessus, le caractère sensible de cette catégorie de données, qui permet ainsi de catégoriser les individus en fonction de leur ethnie, sexe, état de santé, etc., justifie à lui seul la mise en place d'une protection. Si cette loi s'attache à traiter de la protection de l'ensemble des données dites à caractère personnel, la loi dite « Kouchner » promulguée le 4 mars 2002 a pour objet de s'intéresser particulièrement aux données médicales. Ainsi, l'article L1111-7 du Code de la santé publique met en place pour les patients les conditions d'accès à leurs données relatives à leur santé. Lorsqu'un individu souhaite avoir accès à n'importe quel document dont le contenu est relatif à son état de santé (par exemple une feuille de consultation ou une ordonnance médicale), ce dernier peut demander directement ou par le biais d'un médecin l'accès à ce document.
Cependant, l'article L1111-8 du Code de la santé publique s'attache plus précisément à la licéité de l'hébergement et du traitement de données de santé. Ainsi, dans le cadre d'opérations de soins ou de diagnostic, les données de santé récupérées peuvent uniquement être hébergées auprès de personnes physiques ou morales qui sont agréées à cet effet. De plus, cet hébergement de donnée de santé ne peut être effectué qu'après consentement exprès de la personne concernée. Enfin, les dispositions du code de la santé publique rappellent que le traitement de telles données doivent évidemment respecter les conditions posées parla loi Informatique et Libertés. Les professionnels de la santé sont encadrés lorsqu'ils sont amenés à traiter avec des données médicales. De plus, le secret médical imposé par la déontologie des professions relatives au milieu de la santé interdit toute divulgation de donnée médicale à autrui sans accord de ce dernier ou au détriment des conditions posées par la loi.

B. Des recommandations pratiques délivrées par la CNIL.
La CNIL accorde une attention particulière à la manière dont sont effectuées des traitements de données à caractère personnel. Pour se faire, la CNIL utilise souvent des recommandations faites aux entreprises ou aux professionnels concernés afin de rappeler les pratiques idéales à effectuer suivant la situation. Dans le cas de la protection des données médicales, la CNIL s'est prononcé sur les modalités optimales à adopter dans le cas où un professionnel de santé héberge ou traite des données médicales.
La CNIL commence par rappeler la nécessité première de maintenir le degré de confidentialité des données de santé au même rang que celui du secret médical. Pour se faire, la CNIL donne des indications d'ordre technique qui, si elles peuvent paraître acquises pour de plus en plus de gens aujourd'hui au regard de l'ouverture du milieu informatique au grand public, restent nécessaires, voire indispensables dans certains cas, pour s'assurer d'un minimum de sécurité sur les données hébergées : un mot de passe doit être mis en place sur l'ordinateur et ce dernier doit faire l'objet d'un arrêt complet à chaque absence du professionnel de santé. De plus, il est recommandé par la CNIL de ne jamais faire de copie de son mot de passe pouvant être lue ou interceptée par un tiers non autorisé à accéder au système informatique. A ce titre, rappelons simplement que la simple intrusion dans un système informatique sans autorisation constitue à lui seul un délit pénal. De plus, la CNIL recommande pour le professionnel médical de disposer de supports de sauvegardes externes permettant d'éviter la perte de données.
Dans le cas où un traitement de données médicales fait l'objet d'une mise en réseau, la CNIL recommande alors une gestion plus poussée des mots de passe : ces derniers doivent être distincts suivant l'utilisateur qui utilise l'ordinateur et trois erreurs consécutives doivent, à l'instar des erreurs lors de l'entrée d'un code PIN erroné, bloquer le système. De plus, la CNIL ne recommande pas à ce qu'un compte d'un utilisateur puisse être ouvert sur plusieurs postes différents : cela signifie ainsi que le professionnel médical n'est pas présent devant l'un de ses postes, ce qui rend accessible les données à un tiers. De plus, les données médicales doivent faire l'objet d'un cryptage : c'est obligatoire pour les données personnelles. Ainsi, outre une intégrité des données qui doit constamment être vérifiée au plan informatique, la confidentialité de ces dernières doit être assurée par un chiffrement total ou partiel des données nominatives en fonction des cas. Enfin, dans le cas où l'accès au réseau se fait via Internet, un système de pare-feu est hautement recommandé pour prévenir de toute tentative d'interception des données médicales lorsque ces dernières font l'objet d'un flux.

II. Une protection des données médicales incertaine au plan international.
La loi française n'est applicable en France, et certaines législations internationales semblent ne pas accorder autant d'importance à la protection des données personnelles. De plus, l'ouverture des réseaux au monde entier amène à un risque : le législateur n'a pas le temps d'adapter la loi à la technique informatique.

A. Une absence de concertation internationale préjudiciable.
Avant toute chose, il est à noter que la majorité des autres états étrangers n'adopte pas de position hostile par rapport à la protection des données personnelles, bien au contraire. Ainsi, concernant les états européens, la plupart de ces derniers ont adopté une CNIL (ou un équivalent) permettant ainsi une certaine uniformisation de la protection des données personnelles, et donc par ce biais des données médicales. De plus, lorsqu'un traitement de données personnelles d'un citoyen français doit être effectué dans un pays étranger, un accord de la CNIL est obligatoire. Il existe ainsi des cas de figure où des données médicales d'un ressortissant français peuvent être amenées à être traitées dans un pays étranger à l'européenne.
L'exemple des États-Unis constitue peut-être le meilleur exemple de risque potentiel d'atteinte à la protection des données médicales d'un citoyen français. Prenons le cas où lors du séjour d'un français aux États-Unis, ce dernier doit subir une hospitalisation imprévue dans un établissement de santé américain. Théoriquement, et dans la grande majorité des cas, les données médicales des patients français n'ont aucune raison d'être détournées de leur utilisation. Or il existe un principe en droit américain nommé le « Patriot Act ». Ce dernier permet au gouvernement américain de disposer librement des données personnelles d'un individu sur le fondement d'une seule suspicion de terrorisme ou d'espionnage. Si l'existence d'un tel principe est hautement compréhensible au regard de l'importance accordée par le gouvernement américain à tout ce qui concerne la sécurité nationale, le fondement d'une seule suspicion sans autre preuve apparait bien léger pour assurer une protection des données médicales. De plus, la cybercriminalité est un rempart à une bonne protection des données médicales lorsque des pare-feu ne sont pas suffisamment élaborés pour prévenir de telles attaque. Ainsi, entre les mois d'avril et juin 2014, Community Health Systems, un spécialiste de la gestion d'hôpitaux américains, a subi des cyber-attaques qui ont subtilisé plusieurs millions de données personnelles. S'il n'est fait état d'aucune subtilisation de données médicales au sein des données volées, cette possibilité relance la nécessité d'une protection informatique nécessaire pour se prémunir de ce genre de piratage.

B. Un état technique avancé, ou le risque d'un retard juridique.
Aujourd'hui, il apparait pratiquement impossible de faire disparaitre la carte vitale du système médical français : la gestion des données de santé apparait bien trop longue au regard du nombre de patients à gérer. A ce titre, l'évolution informatique mêlée à des impératifs de gestion médicale ne pose pas de problème juridique en soit. Toutefois, des technologies nouvelles ne sont pas encore appréhendées parla loi. Il en va par exemple du Cloud computing : aucun stockage physique n'est effectué sur le disque dur de l'ordinateur et tout se retrouve localisé dans des datacenters qui peuvent être localisés dans des pays étrangers. Certaines entreprises louent d'ailleurs des services de cloud à des professionnels. Or dans le cas où un professionnel médical stockerait des données de santé de cette manière, outre un accord de la CNIL nécessaire, que se passe-t-il dans le cas où un patient souhaite avoir accès à ses données de santé ? De plus, lorsque des données, notamment personnelles, se retrouve massivement stockées en un point physique fixe, les risques de cyber-attaques se retrouvent augmentées. En 2009, le gouvernement français avait élaboré le projet « Andromède » qui prévoit de stocker sous la forme d'un « cloud souverain » les données nationales du gouvernement, de son administration et d'autres entreprises. Ce projet permettrait ainsi d'alléger considérablement les risques associées à une « volatilité » des données que l'on peut constater aujourd'hui. En effet, ces dernières se retrouveraient toutes sous l'égide de la loi française, aucun problème de localisation des serveurs ne pourrait être relevé et le travail de surveillance de la CNIL serait considérablement allégé. Pour autant, si les données médicales ne semblent pas faire l'objet d'un stockage massif dans des serveurs cloud étrangers, la question mérite néanmoins réflexion en ce que les dispositions relatives au bon traitement des données médicales par le droit français se voit d'un coup quasiment réduites à néant. Enfin, une législation numérique européenne serait la bienvenue puisque les données médicales se verraient enfin asservies à un régime juridique dans l'ensemble de l'Europe.
Par Me Murielle CAHEN
Sources :
http://www.cnil.fr/documentation/fiches-pratiques/fiche/article/un-imperatif-la-securite/

http://www.ordre.pharmacien.fr/content/download/123311/645012/version/1/file/J23-Dossier-CommentGarantirSecuriteDonneesSante.pdf

http://www.ordre.pharmacien.fr/Le-patient/La-protection-des-donnees-de-sante

http://www.linformaticien.com/actualites/id/33884/4-5-millions-de-donnees-medicales-derobees-aux-etats-unis.aspx

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

Source : http://www.juritravail.com/Actualite/fichiers-libertas/Id/176621
Par Murielle CAHEN – Avocat

La France, terrain de jeu privilégié des espions chinois

La France, terrain de jeu privilégié des espions chinois

Au début du mois, « l'Obs » dévoilait l'existence d'un centre d'écoutes des services de renseignement chinois en banlieue parisienne. Si la Chine a démenti les affirmations de l'hebdomadaire, l'exécutif français n'a absolument pas réagi. Une passivité qui dit bien la liberté d'action dont bénéficient en France les espions chinois. Impossible de prendre le risque d'une brouille diplomatique avec Pékin pour une vague affaire d'espionnage compte tenu des enjeux commerciaux.

Lors de la visite du président chinois, Xi Jinping, à Paris en mars 2014 – Orban Thierry-POOL/SIPA

Une annexe de la « NSA chinoise » en banlieue parisienne ! Au début du mois de décembre, l'Obs dévoilait l'existence de ce que l'hebdomadaire croyait être un centre d'écoutes des services de renseignements chinois.

« C'est une totale invention !, tonne Monsieur Wu, chargé de communication de l'ambassade de Chine en France, Ces installations ne font qu'assurer le système de communication de l'ambassade. Cela permet des connexions sécurisées. Cela a été fait en totale conformité avec la législation française. Nous respectons les lois françaises. J'ai sous les yeux les papiers datés du 11 octobre 2002 qui attestent de l'autorisation donnée par l'Autorité de régulation des télécoms qui est parfaitement au courant de ces installations. Il n'y a là bas que des diplomates, aucun militaire. Tout est transparent ». Quand nous lui demandons, si la totale transparence et la bonne volonté chinoise pourraient aller jusqu'à nous laisser visiter ces installations, Monsieur Wu hésite tout de même… avant de répondre par la négative ! La transparence a des limites…

Paradoxalement, du côté français, on est encore moins prolixe. Interrogé sur l'existence supposée d'un bâtiment des renseignements chinois sur le territoire français, le quai d'Orsay répond « pas de commentaires ». En théorie, le ministère de l'Intérieur, les Affaires étrangères et les services de renseignement français sont parfaitement au courant de l'existence de cette annexe de l'ambassade de Chine et les autorités françaises auraient même validé l'installation de ces antennes.

Les « grandes oreilles » de Pékin en France… *par LeNouvelObservateur*

Si l'Obs surévalue sans doute en partie la menace représentée par les trois paraboles perchées sur ce bâtiment de Chevilly-la-Rue au point d'en faire une annexe de la « NSA chinoise » – on « souhaite » à Pékin de disposer d'autres moyens pour espionner Paris –, l'article de l'hebdomadaire, que l'on sent largement alimenté par la DGSI, dit bien toute la frustration et l'impuissance du contre-espionnage français face au pillage d'informations exercées par l'Empire du Milieu en France. Compte tenu du poids économique que représente la Chine pour la France, les espions chinois opèrent en effet relativement tranquillement sur le territoire français au grand dam du contre-espionnage français.

La France n'a tout simplement pas les moyens de se payer une brouille diplomatique avec Pékin au prétexte de trois paraboles installées en banlieue parisienne. Les milliards de contrats commerciaux signés avec les Chinois valent bien quelques sacrifices… Ce laisser-faire relève néanmoins de l'humiliation permanente pour les services français, contraints d'avaler toutes les couleuvres chinoises.

Non que Pékin ne possède pas, comme les Américains, mais aussi comme la France, de « grandes oreilles » un peu partout dans le monde, et prioritairement dans les pays et les dictatures amies du régime. En 2008, dans son ouvrage Les services secrets chinois, Roger Faligot estimait déjà que la Chine jouait dans la cour des grands avec les Etats-Unis et la Russie en matière de renseignement électro-magnétique. Six ans plus tard, les budgets du renseignement chinois ont explosé et les techniciens ont progressé, formés depuis les années 80 par le BND allemand et même jusque dans les années 90 par… la NSA américaine.

Selon Roger Faligot, la Chine a mis en place au fil des ans une « armée populaire des cyberguerriers » : « Ce service dépend de l'armée populaire de libération. Il est organisé en deux départements qui travaillent sur le renseignement de guerre et l'interception des communications. Ils procèdent en envoyant des virus qui permettent de pirater des informations ou de bloquer des sites gênants. Ils opèrent également en mode "testing" en piratant des systèmes pour étudier la capacité de réaction de l'ennemi. Nous sommes ici en plein volet de guerre psychologique et idéologique ».

Une guerre surtout économique désormais, comme l'avait illustré en septembre dernier une enquête de Franck Renaud et Hervé Gattegno parue dans Vanity Fair. Les journalistes avaient mis la main sur un rapport de la délégation interministérielle à l'intelligence économique (D2IE) sur les objectifs et méthodes chinoises pour piller les innovations technologiques françaises. Un espionnage d'une toute autre ampleur que le renseignement d'origine électro-magnétique. Cette instance signale chaque année plusieurs dizaines de vols ou tentatives de vols de données par captation ou indiscrétion. Toutes les techniques d'espionnage seraient utilisées. De la simple « oreille baladeuse » chinoise dans les trains Thalys ou Eurostar largement fréquentés par les industriels, aux « agents de charme » chargés de séduire les élites industrielles, à l'organisation de voyage de tourisme industriel, l'infiltration d'étudiants chinois dans les universités françaises, le vol de matériels informatiques ou bien encore des méthodes de « phishing » très sophistiquées. Il faut aussi ajouter l'incroyable « pouvoir de persuasion » des Chinois pour imposer à leurs partenaires des transferts de technologies lors de la signature de contrats commerciaux ou la création de joint-ventures, de filiales communes.

« La Chine est déterminée à devenir indépendante de l'Occident en matière d'innovation technologique. Elle est donc avide de connaissances, de savoir-faire et de procédés à faire venir en Chine ou à absorber à l'étranger » précisait le rapport de la D2IE. De leur côté, « les entreprises françaises, attirées par ce marché qu'elles envisagent immense (…) et par les coûts de main-d'œuvre locaux inférieurs aux coûts européens, sont souvent prêts à transférer leur technologie et leur savoir-faire, fournissant ainsi un avantage à leurs concurrents chinois ».
Paris se rassure en estimant que Pékin n'a pas encore les capacités d'exploiter à plein les renseignements politiques, économiques ou industriels qu'ils obtiennent, la Chine se limitant pour l'instant à du rattrapage technologique et à des copies de mauvaise qualité. Mais les énormes moyens affectés à la cyberguerre servent aussi le renseignement économique notamment par le biais de piratages informatiques massifs ainsi que le vol de propriété intellectuelle.

Derrière chaque touriste chinois, un espion potentiel ?
En 2013, la société de sécurité américaine Mandiant publiait un rapport documenté (accessible librement http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf) sur l'unité 61398 du renseignement chinois. Chargée du « suivi » des pays de langue anglaise, l'unité aurait compromis jusqu'à 141 entreprises dans vingt grands secteurs industriels, en dérobant un volume considérable d'informations relevant de la propriété intellectuelle. L'infrastructure de commandement et de contrôle de cette unité compterait de 850 à 1 000 machines situées dans 13 pays. Le coût de ce pillage informatique des entreprises américaines était estimé à au moins 24 milliards de dollars en 2012. L'unité 61046, chargée notamment du suivi de l'Europe, fonctionne sans doute sur le même principe avec la même efficacité, mais est moins connue.
Elle a néanmoins permis aux espions chinois d'accéder aux ordinateurs du président de la Commission européenne, du ministère français des Finances en mars 2011et même de l'Elysée en juillet 2012, causant à l'époque une panique certaine dans les couloirs de la présidence. Chaque attaque est l'occasion pour les services occidentaux d'identifier les priorités des services chinois ainsi que les commanditaires pour mieux connaître leur organisation encore très nébuleuse.
Un an plus tard, dans une mise à jour de son rapport, la société Mandiant disait avoir constaté une « mise en sommeil » pendant quelques mois des activités de l'Unité 61398 suite à la publication de son rapport et aux protestations américaines. De même, toutes les adresses IP des cyberattaques chinoises qui ont frappé les Etats-Unis depuis ont été modifiées, suggérant un changement de stratégie des renseignements chinois.
Mais l'espionnage informatique continue. En octobre dernier, une société américaine de cybersécurité privée identifiera une nouvelle unité de espions informatiques chinois baptisée « groupe Axiome » : « Axiome est chargé de diriger les opérations de cyberespionnage très sophistiquées contre de nombreuses grandes entreprises, des journalistes, des groupes écologistes ou pro-démocratie, des sociétés de logiciels, des établissements universitaires et des organismes gouvernementaux dans le monde entier ». Cibles prioritaires : les Etats-Unis, l'Europe et les voisins asiatiques.
Le Washington Post dévoilera quelques jours plus tard une note du FBI destinée aux industriels américains les alertant sur cette unité de cyberpirates que le FBI considérait comme directement liée aux services de renseignements chinois et jugeait plus performante que l'unité 61398.

Une forme d'espionnite aigüe qui oblige les services français à une attention de tous les instants. Très récemment la lettre spécialisée Intelligence online rapportait l'escapade à Saint-Nazaire d'une équipe du service culturel de l'ambassade de Chine, venue célébrer l'anniversaire de la construction d'un bateau de croisière chinois. La délégation se serait tellement attardée à « mitrailler » le porte-hélicoptères Mistral destiné à la Russie que cela aurait fini par éveiller les soupçons de la DGSI. De la surveillance à la paranoïa, il n'y a parfois pas loin…

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

Source : http://www.marianne.net/La-France-terrain-de-jeu-privilegie-des-espions-chinois_a243309.html
par Régis SOUBROUILLARD – Marianne