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.

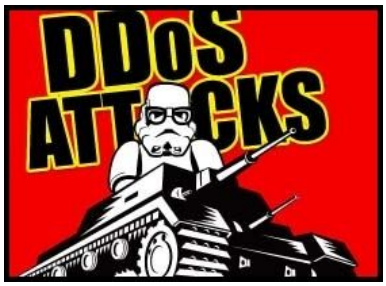
Derrière chaque touriste chinois, un espion potentiel ?
En 2013, la société de sécurité américaine Mandiant publiait un rapport documenté (accessible librement http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf) sur l'unité 61398 du renseignement chinois. Chargée du « suivi » des pays de langue 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

DDoS : les hébergeurs doivent prendre d’urgence des mesures pour défendre leurs clients

	DDoS : les hébergeurs doivent prendre d’urgence des mesures pour défendre leurs clients

Faisant chaque jour la une des journaux, les attaques par DDoS se multiplient. De ce fait, de nombreuses entreprises s'interrogent : leur stratégie de mitigation des DDoS les protège-t-elle suffisamment ? Aujourd'hui, elles se tournent vers leurs fournisseurs de cloud et leurs hébergeurs pour avoir la bonne réponse.

Malheureusement, l'hébergement procure aux hackers une surface d'attaque incroyablement attrayante. En effet, la taille et l'ampleur des infrastructures réseaux des data centers des opérateurs et l'importante base de clients que cela représente, présentent de multiples points d'entrée et se traduisent une énorme bande passante globale qui offre un véritable boulevard aux attaques DDoS perturbatrices et destructrices. En s'appuyant de plus en plus sur l'hébergement pour leurs services et leurs infrastructures critiques, les entreprises s'exposent elles-mêmes au risque de subir des cyber-menaces dévastatrices – même en tant que cibles indirectes.
L'aspect multi-tenant des centres de données du cloud peut expliquer la confiance relative des locataires. Une attaque DDoS volumétrique contre un des 'tenants' peut engendrer des répercussions désastreuses envers les autres : un effet « domino » de latence, de dégradation du service et d'interruption des activités de longue durée, avec de lourds dommages potentiels. Un trafic malveillant excessif qui bombarde un seul locataire au cours d'une attaque DDoS volumétrique, peut avoir des effets négatifs sur d'autres locataires et sur l'ensemble des opérations du centre de données. Il est en fait, de plus en plus fréquent qu'une attaque visant à l'origine un seul locataire ou un seul service, étouffe complètement les ressources partagées, en infrastructure et en bande passante. Ceci provoque de sévères ralentissements allant parfois jusqu'à la mise hors service du centre de données tout entier. En quelque sorte les effets secondaires du DDoS.

La technique du trou noir est un moyen de défense brut, utilisé couramment lors des attaques pour atténuer les effets secondaires des DDoS. Par cette technique, les fournisseurs de cloud et d'hébergement bloquent tous les paquets destinés à un domaine, le trafic étant re-routé vers un itinéraire nulL pour l'adresse (ou les adresses) IP sous attaque. Ce mode de défense contre les attaques DDoS pose un certain nombre de problèmes. En particulier, quand plusieurs locataires partagent une gamme d'adresses IP publiques. Dans ce cas, ils verront leur accès supprimé à l'ensemble des services, qu'ils soient ou non la cible spécifique de l'attaque. En pratiquant cette technique, l'opérateur du data center achève en fait lui-même le travail de l'attaquant en dosant complètement ses propres clients ! De plus, l'injection de routes nulL est un processus manuel qui nécessite des analystes humains, des processus workflow et des autorisations. On augmente alors les temps de réponse à l'attaque et on laisse tous les locataires du data center partagé en subir les conséquences sur des périodes pouvant atteindre plusieurs heures.
La dépendance croissante à Internet rend les effets – financiers ou autres – des attaques DDoS réussies de plus en plus douloureux pour les fournisseurs de services, les entreprises et les administrations. Et l'arrivée de nouveaux outils DDoS toujours plus puissants promettent le déclenchement d'attaques encore plus destructrices dans les mois et les années à venir.

Il est temps que les entreprises qui s'appuient sur des infrastructures ou des services hébergés commencent à se poser les bonnes questions, comme se demander si leurs fournisseurs d'hébergement ou de centres de données les protègent correctement quand une attaque DDoS frappe. Comme cela s'est vu à maintes reprises, les clients hébergés comptent en fait tout simplement sur leur fournisseur pour « s'occuper » des attaques quand elles surviennent, sans appréhender pleinement le danger et les conséquences de fermer les yeux face à ce type de comportement malveillant.

Voici trois étapes-clés pour que les fournisseurs protègent mieux leur propre infrastructure et celle de leurs clients.

1. Éliminer les délais entre le moment où les dispositifs de surveillance traditionnels détectent une menace et génèrent une alerte et le moment où un opérateur est en mesure d'y répondre. Initialement de quelques heures, l'effet de l'attaque sera réduit à quelques secondes. Ceci est possible par le déploiement d'appliances qui surveillent et atténuent automatiquement les menaces DDoS. La solution de mitigation doit pouvoir mettre à disposition des rapports d'alertes et d'événements en temps réel, avec une infrastructure de maintenance opérationnelle en arrière-plan pour des temps de réaction rapides, et fournir toute la visibilité indispensable pour comprendre l'état de la menace et améliorer pro-activement la défense anti-DDoS.

2. Déployer la mitigation DDoS inline. Si des périphériques out of band sont en place pour nettoyer le trafic, il convient de déployer rapidement des équipements de détection des menaces inline qui pourront inspecter, analyser et contrer les DDoS en temps réel.

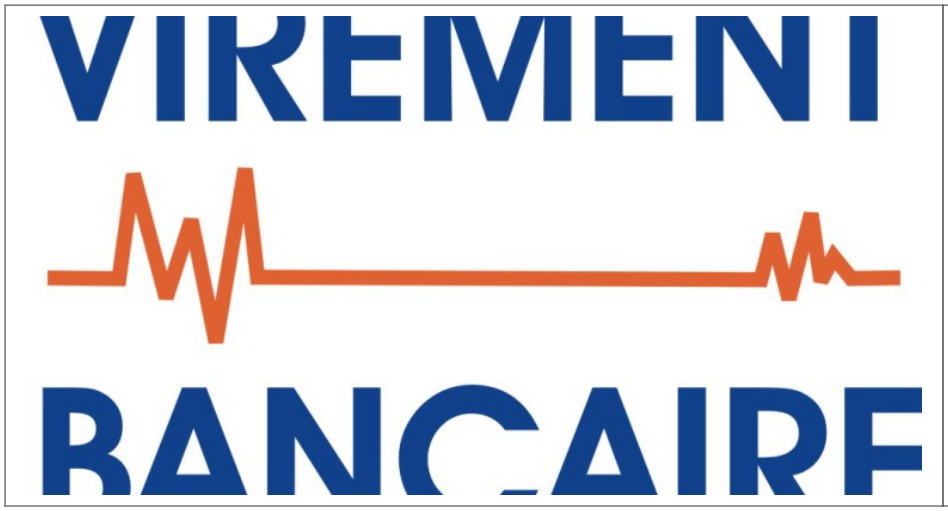
3. Investir dans une solution de mitigation DDoS architecturée pour ne jamais abandonner le bon trafic. Les prestataires de services hébergés doivent impérativement empêcher que l'équipement de sécurité ne devienne un goulot d'étranglement pour les services rendus et toujours permettre au trafic légitime de passer, sans aucune interruption ; voilà une approche de défense anti-DDoS réussie et sans dommage collatéral.

Les entreprises font confiance à leurs fournisseurs pour assurer la disponibilité de leurs services et, finalement, leur protection contre les cyber-menaces et les attaques par DDoS. Le déploiement d'une première ligne de défense complète contre les attaques DDoS permet de protéger pleinement les clients contre les menaces volumétriques dommageables, qu'elles soient dirigées vers les réseaux, qu'elles en proviennent ou qu'elles y transitent.

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

Source : http://www.programmez.com/avis-experts/ddos-les-hebergeurs-doivent-prendre-durgence-des-mesures-pour-defendre-leurs-clients-21827
par Adrian Bisaz

Virements bancaires frauduleux, découvrez les dernières techniques d’escroquerie



Virements bancaires frauduleux, découvrez les dernières techniques d’escroquerie

Les entreprises sont de plus en plus souvent victimes d'escroqueries bancaires, en particulier celles touchant les virements internationaux. C'est ainsi près de 250 millions d'Euros qui sont détournés, le plus souvent au profit d'organisations criminelles. 16% des entreprises reconnaissent ainsi avoir été touchées. A côté de la classique escroquerie qui consiste à usurper la signature d'un dirigeant de l'entreprise visée, puis à transmettre un ordre de virement falsifié à la banque, trois autres sont principalement utilisées.

Jean-Marc Souvira, commissaire principal à l'Office central de la répression de la grande délinquance financière révèle dans une vidéo (ci-dessous) destinée à sensibiliser les responsables d'entreprises sur les risques encourus qui sont chaque jours plus grands. Ces fraudes touchent tous les secteurs d'activité, elles visent majoritairement le commerce, en raison du très grand nombre de transactions réalisées dans ce secteur. Il faut rappeler aussi l'exposition des fraudes a la carte bancaire comme nous en parlions ici.

Prévenir les escroqueries aux ordres de virements internationaux dans les entreprises

Virements bancaires frauduleux : les nouvelles techniques des escrocs
La première d'entre elles est appelée «escroquerie à la nigériane»: L'escroquerie à la nigériane, ainsi appelée car les auteurs procèdent depuis l'Afrique de l'ouest, consiste à envoyer un mail informant la société destinataire d'un changement de coordonnées en raison de dysfonctionnements. Les auteurs y expliquent que le paiement des prochaines factures devra s'effectuer sur un nouveau compte bancaire, mieux sécurisé. Elle touche principalement les entreprises exerçant dans le secteur du commerce, les escrocs se faisant passer pour leurs sous-traitants asiatiques.

virements bancaires frauduleux
Une autre technique l'«escroquerie au président» : L'escroquerie au Président consiste à obtenir un virement en se faisant passer pour le PDG de l'entreprise, en arguant d'une quelconque urgence pour qu'il soit immédiat. Une personne de l'entreprise est appelée par le prétendu P-DG, qui explique qu'il est en déplacement et a besoin d'un virement pour une opération confidentielle, telle qu'une OPA ou un contrôle fiscal. Très compliquée puisqu'elle nécessite une bonne connaissance de l'entreprise et de ses codes, ainsi qu'un certain aplomb, cette escroquerie est très lucrative : les sommes détournées peuvent atteindre plus d'un million d'euros pour chaque ordre.
La dernière arnaque en vogue est celle qui profite de la norme Sepa : Plus récemment, une nouvelle escroquerie exploite les failles de la norme SEPA. Les escrocs contactent les entreprises, en se faisant passer pour un informaticien de leur banque, afin de les convaincre de se connecter sur un site pour des mises à jour ou des tests de sécurité. Ce faux site leur permet de prendre le contrôle à distance du réseau interne de l'entreprise. Des ordres de virement sont alors passés, sans surveillance puisque les banques ne vérifient plus si l'ordre émane bien de l'entreprise.

La Chine, principale plateforme de réception
Pour faire face à ces arnaques, il faut avant tout du « bon sens ». Mais il faut aussi ne pas tarder à se rendre compte de l'arnaque, car les opérations de virement ne peuvent être annulées après un délai, très court. Dans leur grande majorité c'est en Chine que l'on trouve l'origine des escrocs et vers ou l'argent est ensuite versé. La police et de la justice françaises doivent d'ailleurs très prochainement rencontrer leurs homologues chinois pour étudier ce problème qui ne touche pas seulement la France mais l'ensemble de l'Europe.

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

Source : http://www.lesnewseco.fr/techniques-escroquerie-virements-bancaires-01609.html

Smartphones : deux applis sur trois nous espionnent, révèle la Cnil

Smartphones : deux applis sur trois nous espionnent, révèle la Cnil

Pour savoir si les applications installées sur nos téléphones portables se montrent respectueuses de nos données personnelles, la Cnil a élaboré, avec l'aide de l'Inria, un logiciel de contrôle et l'a fait tourner sur 121 applications Android pour vérifier la collecte éventuelle d'informations de localisation, du carnet d'adresses, du calendrier ou même des numéros de téléphone.

Le résultat est édifiant, révèlent nos confrères d'Europe 1 : 66 % des applications communiquent sur le type de réseau Internet (Wi-Fi, 3G, 4G) auquel l'utilisateur est connecté, 24 % accèdent à la géolocalisation, le plus souvent à l'insu de l'utilisateur, cinq applis ont accédé au numéro de téléphone de l'utilisateur et deux ont été jusqu'à récupérer la liste des identifiants des points d'accès Wi-Fi présents autour de l'utilisateur.

Une application qui n'est pourtant pas dédiée à la recherche d'itinéraire, Google Play, boutique de téléchargement d'applications pour Android, a même accédé à plus d'un million de fois à la géolocalisation d'un smartphone unique en trois mois !

La Cnil assortit ses conclusions de quelques conseils. La meilleure façon de se protéger consiste à éviter les téléchargements inutiles, et à faire régulièrement le tri dans celles qui sont installées sur son appareil. On peut également régler les paramètres de son téléphone (menu Paramètres Google, option « désactiver annonces par centres d'intérêt ».)

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

Source : http://www.industrie-techno.com/smartphones-deux-applis-sur-trois-nous-espionnent-revele-la-cnil.35111
Par Muriel de Véricourt

Cyberviolence : les parents ne sont pas désarmés

Cyberviolence : les parents ne sont pas désarmés

Un collégien sur cinq déclare avoir été insulté ou humilié sur internet ou par des SMS. Pour répondre à ce phénomène en augmentation, les parents d'élèves ont à leur disposition des outils pour prévenir et agir avant un drame.

«Demain, à l'arrêt de bus, t'es morte ». La violence des mots est inouïe. Ils ont été envoyés par SMS à une collégienne de cinquième vivant en région parisienne. Insultée également sur Facebook, la jeune fille s'est suicidée après deux années d'enfer où les insultes sur internet se sont ajoutées à un harcèlement « classique » au collège. Car la cyberviolence peut pousser un jeune à commettre l'irréparable. « Les suicides sont rares, fort heureusement, tempère Catherine Blaya, présidente de l'Observatoire international de la violence à l'école, mais mettez-vous à la place d'une jeune fille de 14 ans qui voit sur un réseau social une photo d'elle trafiquée à moitié nue avec un message qui la traite de ''chaudasse''. Quand elle retournera au collège, toutes les personnes qu'elle croisera seront susceptibles d'être au courant ».

Un collégien sur trois ne dit rien

Si, selon une enquête du ministère de l'Éducation nationale publiée le 27 novembre 2014, la cyberviolence est en progression et a touché en 2013 un collégien sur cinq en France, les parents se sentent souvent désarmés pour répondre aux souffrances de leurs enfants et réagir.
Encore faut-il que les parents soient au courant. Un collégien sur trois ne dit rien à personne sur sa situation, selon l'enquête du ministère. « Tous les parents n'ont pas accès au profil Facebook de leur enfant. Certains ne savent même pas qu'ils en possèdent un », souligne Christine Sené, la présidente de l'association Noélanie qui combat toutes les violences à l'école.
En prévention, pour en parler avec ses enfants, il existe plusieurs outils, comme le site internet créé par Facebook « takethislollilop.com ». « On y visionne un clip très dissuasif qui montre une sorte de psychopathe qui cherche et vole des informations sur le compte Facebook de sa victime. C'est un clip interactif. Pour les enfants, les adolescents, cela a beaucoup d'impact », insiste Catherine Blaya.

« Il existe aussi des outils pédagogiques très intéressants sur le site ''agircontreleharcelementalecole.gouv.fr''. Les parents peuvent s'en servir pour entamer un dialogue », souligne Eric Debarbieux, le délégué ministériel chargé de la prévention et de la lutte contre les violences en milieu scolaire.

Il est également possible de faire stopper rapidement certains actes de cyberviolence. « Le plus efficace pour supprimer une vidéo dégradante est le site internet-signalement.gouv.fr », conseille Christine Sené dont l'association a un forum rassemblant près de 3500 familles. Alertée, l'association « e-enfance » peut aussi réagir rapidement pour faire suspendre une page Facebook dans les 24 heures.

« Reste que seuls les parents peuvent porter plainte », rappelle Eric Debarbieux. « Pour les aider dans leurs démarches juridiques, par expérience, les gendarmes de la Brigade de prévention de la délinquance juvénile sont très précieux et efficaces », conseille Christine Sené.

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

Source : http://www.ledauphine.com/faits-divers/2014/12/14/cyberviolence-les-parents-ne-sont-pas-desarmes
Par Patrice BARRÈRE

Nouveau tournant pour la protection de la vie privée au Maroc

Nouveau tournant pour la protection de la vie privée au Maroc

La Commission nationale de contrôle de la protection des données à caractère personnel (CNDP) publie son premier rapport d'activité 2010-2013. Installée fin août 2010, cette autorité administrative se charge de préserver le respect de la vie privée. Elle s'appuie sur la loi 09-08 relative à la protection des personnes physiques du traitement des données personnelles (Bulletin officiel en français n°5714 du 15 mars 2009).

«Les plaintes qui nous parviennent sont en hausse d'année en année. Ce qui signifie que la culture de la protection des données personnelles commence à se répandre. Certes, cette culture n'est qu'à ses débuts, mais les résultats réalisés (…) sont franchement encourageants», relève avec optimisme le président de la CNDP, Saïd Ihraï. Une seule plainte en 2011, 7 en 2012 et 43 en 2013. Qu'est-ce qui explique cette progression? L'accessibilité de la procédure joue: dans 83% des cas, les plaintes sont enregistrées en ligne (www.cndp.ma). Elles sont aussi déposées sur place ou envoyées par fax. «Toutefois, le nombre de réclamations reste limité à cause notamment d'une grande réticence à les faire par écrit», selon le rapport.

Les SMS indésirables arrivent en tête des plaintes, suivis par les Spam… «Près de la moitié des cas ont été réglés. Pour les envois abusifs de SMS, les contacts pris avec le régulateur télécoms et les trois opérateurs ont permis de mettre en place une stratégie de lutte…». Sauf que le business illégal des bases de données se poursuit. C'est pourquoi nos boîtes électroniques sont bombardées par des publicités intempestives. Avec un pourcentage relativement modeste (voir illustration), l'usage abusif de données biométriques et de la vidéosurveillance interpellent (voir encadré). Toutes rubriques confondues, les 51 plaintes déposées jusqu'à fin 2013 émanent surtout de Casablanca et de Rabat (88%). Cette concentration géographique a une cause. Regroupant les grands centres économiques et administratifs, les deux métropoles centralisent par conséquent une masse significative de données personnelles et les responsables des traitements: patronyme, numéro de la carte d'identité et de téléphone, email, photo, empreinte digitale, ADN, relevé d'identité bancaire… Ces données permettent «d'identifier directement ou indirectement» salariés, actionnaires, clients, visiteurs, fournisseurs, administrés…

La CNDP veille à ce que le traitement des informations liées à nos vies privées ait «des finalités précises, claires et légitimes». Conformément à la loi du 18 février 2009, le responsable du traitement doit notifier son activité à la Commission (voir page 6), avoir l'autorisation préalable des personnes concernées, veiller au respect de la confidentialité des données… Le non-respect de la loi expose à des amendes et des sanctions pénales. Vous voilà avertis.

Contrôles inopinés

Rappelons à bon entendeur les termes de la Délibération adoptée par la Commission nationale de contrôle de la protection des données à caractère personnel (CNDP) fin mai 2013 à Rabat. Celle-ci porte sur «les conditions nécessaires à la mise en place d'un système de vidéosurveillance dans les lieux de travail et dans les lieux privés communs» (cf. L'Economiste du 15 novembre 2013). Malgré son importance, la Délibération n° 350-2013 demeure largement ignorée par les personnes physiques et morales (entreprises, établissements publics, ministères…).

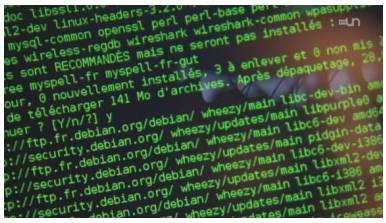
Particuliers, entreprises et administrations doivent s'attendre à des contrôles inopinés d'agents assermentés. La collecte et le traitement d'images des lieux surveillés constituent une manipulation de données personnelles. L'utilisation de caméra de surveillance doit être notifiée préalablement à la CNDP.

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

Source : http://www.leconomiste.com/article/962774-donnees-personnelles-nouveau-tournant-pour-la-protection-de-la-vie-privee
par Faiçal FAQUIHI

Réseaux Wifi: gare aux

pirates!

	**Réseaux Wifi: gare aux pirates!**

Aujourd'hui, on se déplace avec son Smartphone dans la poche, et de plus en plus souvent avec son ordinateur portable sous le bras. On veut pouvoir surfer sur le Net dans les gares, les aéroports, les cafés ou les chambres d'hôtel. Plusieurs grandes villes offrent même un accès wifi public et gratuit. Nos cartes bancaires sont aussi équipées de puces permettant le paiement sans contact. Mais attention, ce sont autant de nouvelles possibilités offertes aux pirates informatiques !

Le piratage informatique augmente
De l'aveu des experts, les antivirus ne savent pas s'adapter à toutes les nouvelles menaces. Il faut d'abord subir une attaque et ses conséquences avant de trouver la parade. Les criminels ont donc pratiquement toujours un temps d'avance. Et les portes d'entrée vers vos données confidentielles se multiplient. Les accès wifi « malicieux », ou encore les virus et autres applications permettant de récupérer vos données de carte de paiement sans contact (NFC)sont des méthodes récentes de piratage qui viennent s'ajouter à une liste déjà longue. Démonstrations.

Votre wifi peut vous rendre suspect
Un soir, madame T. a la mauvaise surprise d'être accueillie par des inspecteurs de la police judiciaire lors de son retour à son domicile. Des images pédopornographiques ont transité par son accès wifi! Bien que protégé, l'accès wifi a été piraté puis utilisé par un cybercriminel. Madame T a rapidement été mise hors de causes, mais reste choquée par cette aventure. Témoignage.

Wifi gratuits: Attention! Le point avec Luc Mariot, journaliste et producteur d'ABE

Les wifi gratuits contrôlés: CFF (en gare de Genève), Aéroport (GVA), Ville de Genève, Ville de Lausanne, Ville de Vevey, Starbucks, Mc Donald, Manor, Centre La Praille.

Vos données intéressent les cybercriminels
Les cybercriminels peuvent utiliser vos données de plusieurs manières. Certains rendent vos documents illisibles puis vous rançonnent en vous vendant la clé de décryptage. D'autres s'emparent tout simplement de vos coordonnées bancaires, pour ensuite les revendre ou consommer à vos frais sur la Toile. Enfin, certains s'invitent carrément chez vous ou à votre bureau, en suivant vos faits et gestes à travers votre micro et votre webcam intégrés. Comment se protéger?
Le Département du Trésor américain et l'Union Européenne annonçaient il y a 5 ans déjà que les profits générés par la cybercriminalité dépassent désormais ceux de la vente de drogue dans le monde ! Un phénomène qui ne va faire que s'amplifier dans les décennies à venir.

LE reportage qui vous dit tout

La principale faille dans les entreprises est le manque de connaissance de ces risques.
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 : http://www.rts.ch/emissions/abe/6205697-reseaux-wifi-gare-aux-pirates.html

Infographie du vol de données en 2014

Infographie du vol de données en 2014

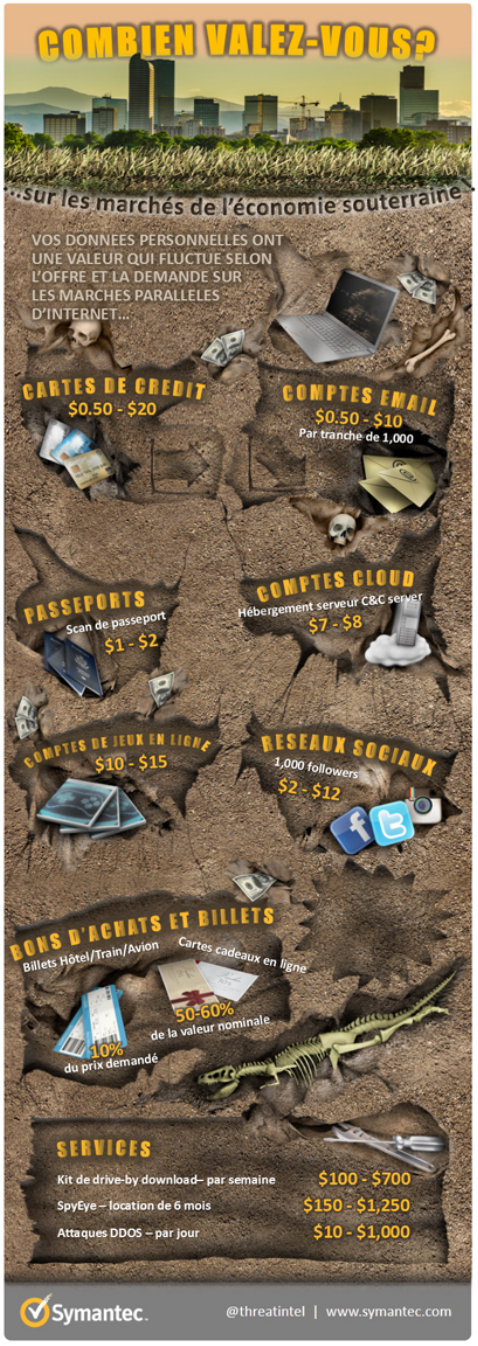
2014: une année record !
Cette année 2014 restera dans les mémoires en ce qui concerne le vol de données informatiques. En effet, l'entêtement des cybercriminels n'a fait qu'augmenter au cours de ces douze derniers mois et 2014 restera comme l'année record en terme de quantité d'informations piratées. A Bon Escient vous partage ce soir une infographie provenant de Silicon sur le vol de données personnelles. Les temps changent, le sabotage n'est plus le but ultime d'un cyberpirate. En effet, le vol de données est dorénavant la source première de motivation pour ce type d'attaque. A ce petit jeu, le gang Russe Cybervor a frappé fort, ce dernier a revendiqué le vol de plus d'1,2 milliards de noms et mots de passe, auquel il faut ajouter pas moins de 500 millions d'adresses e-mail, tout ce butin ayant été collecté sur pas moins de 420 000 sites. Il ne faut pas non plus oublier les deux autres scandales, subis quant à eux par l'industrie américaine de la grande distribution, à savoir les affaires Target et Home Depot, les pirates ayant profité de plusieurs failles dans les lignes de caisses.

Concernant le paysage digital français, deux attaques ont marqué les esprits et concernent l'opérateur Orange, qui s'est respectivement fait pirater 800 000 et 1,3 millions de comptes. Ces attaques numériques ont un impact négatif sur l'image de l'entreprise et font baisser la réputation ce celle-ci. De plus, elles ont des répercussions économiques avec une perte de confiance de la part des clients.

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

Source : http://www.abonescient.fr/le-fil-infographique/le-vol-de-donnees-infographie/

Données volées ! Services d’attaques ! Quels sont prix sur le marché de la cybercriminalité ?

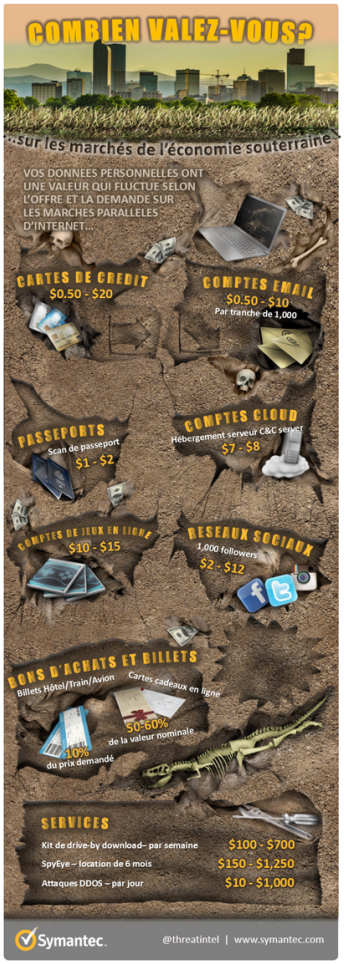


Données volées ! Services d’attaques ! Quels sont prix sur le marché de la cybercriminalité ?

Sur les marchés de l'économie souterraine sur Internet, combien valent les données personnelles volées lors des récentes violations de données massives ? A combien sont proposés les services d'attaques ?

Les chercheurs de Symantec ont mené une étude empirique sur les marchés souterrains florissants de l'Internet et déterminé comment les données volées ou les services d'attaques varient selon la loi de l'offre et de la demande. Si la valeur des emails a diminué de façon significative, le spam ne faisant plus vraiment recette, la valeur d'autres biens et services illicites reste stable.
A titre d'exemples (illustrés via l'infographie ci-dessous) :

– Les scans de passeport coûtent entre 1$ et 2$ et sont utilisés pour les vols d'identités
– Les comptes de jeux en ligne volés se monnaient entre 10$ et 15$, puisqu'ils peuvent rapporter gros dans le monde virtuel
– Les malwares customisés se paient entre 12$ et 3,500$, comme par exemple des outils pour voler des bitcoins en détournant les flux de paiement vers les cybercriminels
– 1 000 followers sur les réseaux sociaux coûtent entre 2$ et 12$
– Les comptes cloud volés sont à 7$ ou 8$. Ils peuvent être utilisés pour héberger des serveurs de commandes et contrôles



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

Source : http://www.infohightech.com/donnees-volees-services-dattaques-quels-sont-prix-sur-le-marche-de-la-cybercriminalite/