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

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

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

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

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

Le droit, un outil de prédation

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

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

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

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

Proposition de loi sur le secret des affaires

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

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

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

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.

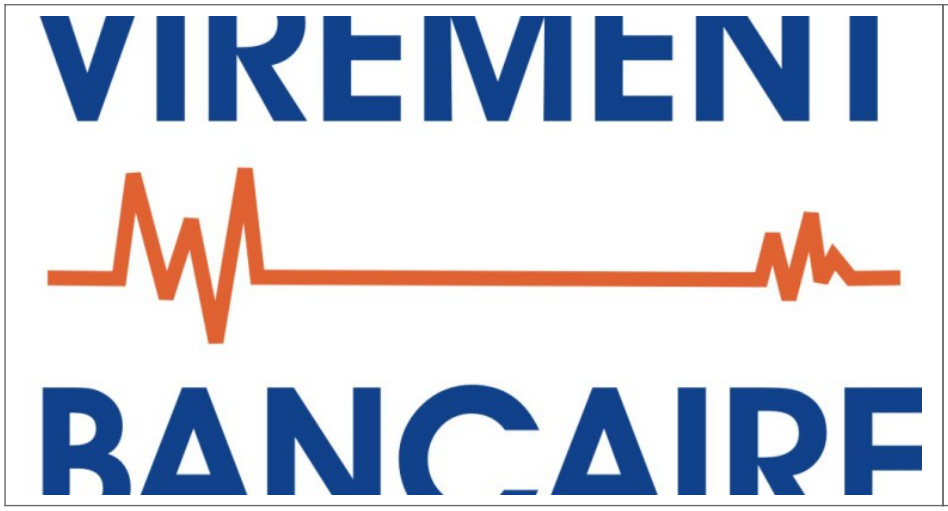
Derrière chaque touriste chinois, un espion potentiel ?
En 2013, la société de sécurité américaine Mandiant publiait un rapport documenté (accessible librement http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf) sur l'unité 61398 du renseignement chinois. Chargée du « suivi » des pays de langue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

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.

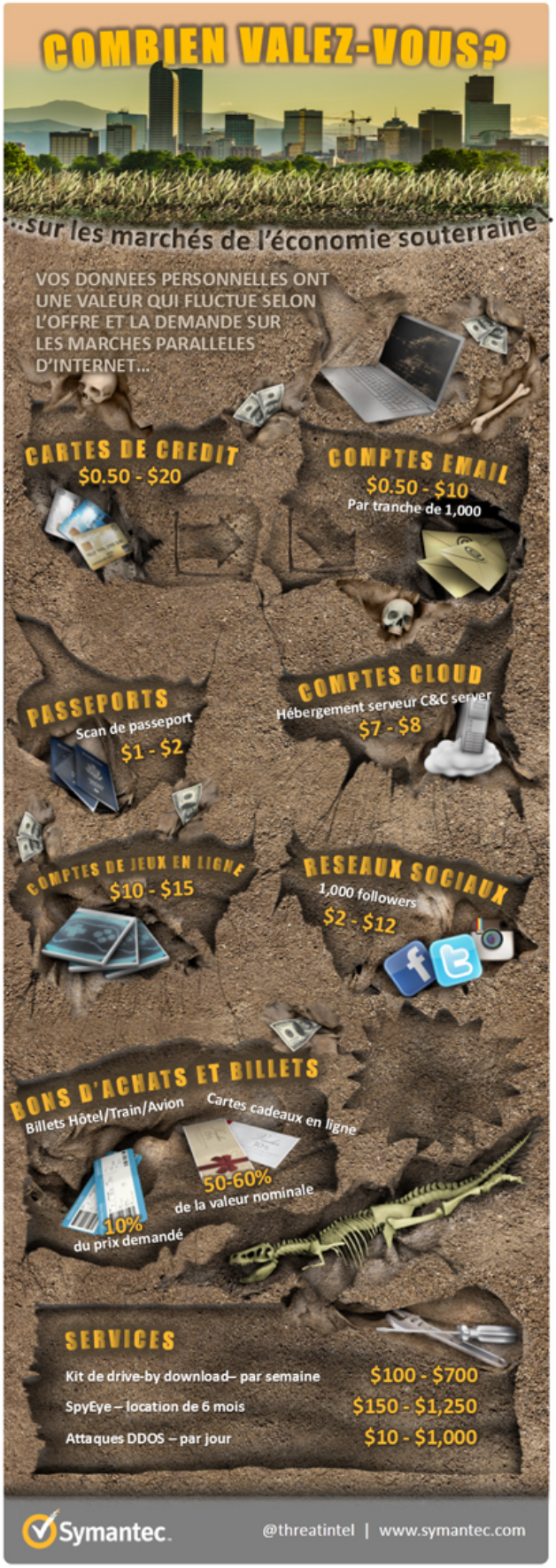
La Chine, principale plateforme de réception
Pour faire face à ces arnaques, il faut avant tout du « bon sens ». Mais il faut aussi ne pas tarder à se rendre compte de l'arnaque, car les opérations de virement ne peuvent être annulées après un délai, très court. Dans leur grande majorité c'est en Chine 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

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

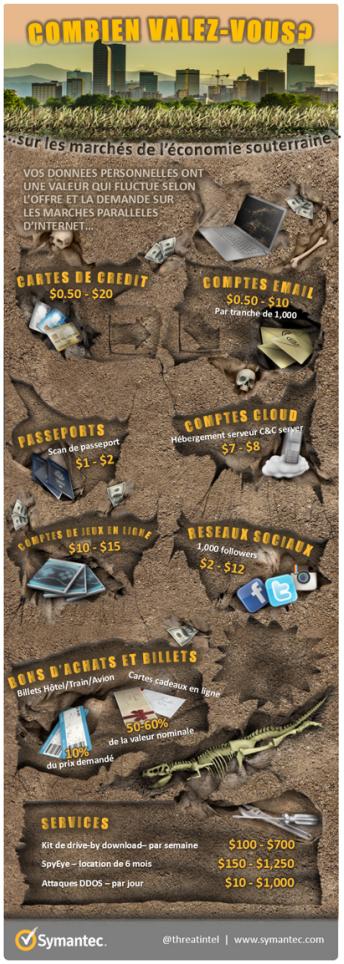
Données volées ! Services d'attaques ! Quels sont prix sur le marché de la cybercriminalité ?



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/

Les pirates capables de voler des données même si votre ordinateur n’est pas connecté à Internet (ou pire, éteint !)

	Les pirates capables de voler des données même si votre ordinateur n’est pas connecté à Internet (ou pire, éteint !)

Lorsque des institutions gouvernementales ou des entreprises souhaitent stocker des informations confidentielles, elles utilisent le plus souvent un réseau en « air-wall », déconnecté d'internet, et isolé de toute connexion extérieure. Récemment pourtant, plusieurs chercheurs de l'université Ben-Gurion en Israël ont démontré qu'il était possible, une fois ce réseau contaminé par un virus spécifique, d'en récolter les données.

Les pirates informatiques peuvent voler les données de votre ordinateur même s'il est déconnecté et éteint.
Atlantico : Bien que les particuliers soient sans doute moins la cible de ce type d'attaque informatique, sont-ils tout aussi vulnérables ?
Michel Nesterenko : Tout ordinateur est potentiellement vulnérable. Mais les connaissances et la technologie nécessaire pour réussir un tel vol de données font que seules les ordinateurs dans lesquels sont stockés des données stratégiques ou des données commerciales de grande valeur sont vraiment à risque. Donc le consommateur normal n'a pas de grand souci à se faire.
Du temps de la Guerre Froide dans les années 60 les espions américains et russes pouvaient voler toutes les informations passant sur l'écran d'un ordinateur à partir du van stationné dans la rue.
C'est pour cela que certains ministères à Washington avaient blindés l'enveloppe extérieure des ordinateurs détenant des données sensibles de façon à empêcher toute émanation électromagnétique.

Jean-Paul Pinte : En tant que particulier, nous sommes encore plus vulnérables à ce type d'attaque ou d'infiltration qui, une fois installé sur une machine, permet d'y revenir et de se servir. Nous avons en effet moins pensé la sécurité de nos données par rapport à une entreprise par exemple, mais le risque demeure le même, il est même plus grand. Le ver installé sur un PC, il est en effet possible de faire ce que l'on veut, de s'installer confortablement et d'y revenir à sa guise. Une des seules façon de pirater un PC éteint serait d'être en rapport avec la C-MOS et nécessiterait donc un accès physique à la machine. Ce n'est donc à la portée du premier venu.
Comme pour votre Webcam éteinte, il est tout aussi possible d'en prendre la main à distance et certains vont même jusqu'à utiliser un cache ou collant qu'ils posent sur la Webcam pour s'en protéger. Un ordinateur quand il est éteint, c'est juste la boite d'alimentation qui est éteinte mais la carte mère continue à recevoir de l'énergie (un voyant lumineux au niveau de la carte mère est toujours présent). Il est donc toujours plus prudent de débrancher totalement son ordinateur et surtout de ne pas le laisser en mode veille ou veille prolongée. Il est également possible si l'on veut se protéger totalement de fermer son boîtier Wifi mais attention aux mises à jour qui se font parfois la nuit sur ces matériels.

Quelles données peuvent être récupérées ? Quelles sont les marges de manoeuvre des pirates informatiques avec pareil procédé ?
Michel Nesterenko : Potentiellement tout peut être récupéré à terme car le vol des données prends du temps, compte tenu des limitations de la bande passante. Ce type de procédé est fort utile dans un contexte militaire ou d'espionnage industriel. Les informations peuvent être revendues aux concurrents ou utilisées dans des manipulations boursières par exemple.

Jean-Paul Pinte : Une fois dans la machine, on peut tout faire avec quelques manipulations que connaissent bien ces hackers. A la base il y a quelques années, le but était simplement d'avoir pu infiltrer ou craquer une machine.
Aujourd'hui, ce sont tous vos contacts de messagerie, les fichiers stockés, les mots de passe qui peuvent être récupérés par exemple au même titre que tous les documents personnels. Il n'y a donc pas de limites.
Tous ces éléments pourraient se retrouver un jour sur la toile et servir par exemple dans le cas d'adresses de messagerie à des banques de données réutilisées par la suite pour faire des envois en masse comme cela se pratique dans le cas des mails nigérian.
Prendre la main sur votre machine revient à avoir la clé de votre domicile, le code de votre alarme et tout peut alors être envisagé en vue de vous voler des informations et des accès à des sites que vous utilisez et sur lesquels vous passez des actes d'achat par exemple.
Aujourd'hui, on parle même de vol de données qui pourraient vous faire chanter.

Comment savoir si notre ordinateur est infecté par ce type de virus ? Comment s'en apercevoir ?
Michel Nesterenko : Pour tout virus connu, il existe un antidote. Encore faut il que les anti-virus et parre-feu soient mis à jour constamment sur chacun des ordinateurs du réseau indépendamment.

Jean-Paul Pinte : Assurez-vous tout d'abord d'avoir la bonne dernière version officielle de vos logiciels et pensez à utiliser des solutions comme Anti Hacks qui détectera les problèmes de configuration et les logiciels obsolètes sur votre machine et qui, surtout, se chargera de configurer automatiquement les logiciels et vous aidera à les mettre à jour.
Ensuite un anti-virus que vous mettrez à jour tous les jours et pas à la petite semaine comme le font la plupart d'entre nous (beaucoup utilisent celui offert pour une période donnée par le fournisseur du PC mais oublient de le changer ou de l'actualiser dans le temps se retrouvant alors sans protection).

En attendant :
• surveillez vos barres d'outils et les liens que vous n'auriez pas ajouté personnellement ;
• contrôlez votre pointeur de souris qui à certains moments se déplacerait de façon inatendue ;
• regardez l'adresse URL du site que vous consultez car il pourrait changer lors d'une transaction financière par exemple ;
• veillez aux fenêtres intempestives qui s'affichent sur votre PC sans que vous n'interveniez et aux pages qui s'installent en arrière plan et que vous ne découvrez qu'une fois que vous fermez votre session Internet ou machine. Elles pourraient bien être la source d'un début d'installation d'une cyber-surveillance ;
• enfin si tout va plus lentement sur votre ordinateur; pensez à contrôler les fichiers qui se lancent au démarrage et surtout n'oubliez pas que le meilleur anti-virus est parfois de remettre à plat tous les six mois votre PC.

Quel est le niveau d'informatique nécessaire pour mettre en oeuvre correctement cette pratique ? Des solutions simples sont-elles mises à la disposition des amateurs ?
Michel Nesterenko : Le Hacking de haut niveau n'est pas une activité pour amateurs. Il faut des connaissances certaines pour mettre au point le virus adapté a une attaque particulière de même qu'il faut des informations précises obtenues par une opération de reconnaissance informatique et physique pour trouver l'ordinateur cible. Il s'agit d'un travail pour des spécialistes.

Jean-Paul Pinte : Dès que ces cybercriminels ont réussi à installer un virus ou un cheval de Troie (souvent aussi nommé malware ou logiciel malveillant) votre ordinateur devient une source potentielle de revenus. Ils auront accès à toutes vos données personnelles (messages, mails, documents bancaires, mots de passe, photos, vidéos, …) stockées sur votre disque dur et pourront surveiller votre activité sur Internet et sur votre machine.
Aujourd'hui, pas besoin d'être un grand expert sur le sujet en dehors de quelques types d'infiltrations spécifiques sur des sites dits plus sécurisés. En effet, malheureusement, beaucoup d'aide est apportée aux cyberdélinquants par Internet.. Des solutions contenus dans certains forums permettent à des petites mains de se lancer tout d'abord dans le cadre d'arrêt d'une machine en réseau dans une entreprise. Petit à petit, pirates, hackers ou encore crackers découvrent les modes opératoires des plus grands pour se les approprier et pour aller plus loin comme s'il y avait un concours entre eux.
Comment s'en prémunir ? Doit-on se résigner à avoir un ordinateur vierge de toute connexion à internet, avec des protocoles de sécurité stricts, comme par exemple ne pas utiliser de clé usb étrangère ou ne pas prêter les siennes ?
Michel Nesterenko : Absolument. Éviter de connecter à internet un ordinateur détenant des données critiques et stratégiques est la première étape. Interdire l'utilisation de toute clé USB non cryptées avec des codes particuliers est une deuxième étape.
Ensuite, il faudra songer à installer un blindage autour de l'écran pour éviter toute émanation électromagnétique. Surtout, il ne faut jamais oublier de tenir à jour les anti-virus et parre-feu sur chaque ordinateur et crypter toutes les données résidant sur le disque dur.
Le nombre de situations où cela sera vraiment recommandé reste fort restreint. Pour l'écrasante majorité des utilisateurs, cela ne sera jamais nécessaire heureusement.
Jean-Paul Pinte : De plus en plus, il faudra apprendre à se protéger et à avoir une culture sécuritaire en ce qui concerne les materiels que nous utilisons et que nous connectons à notre PC car ils seront autant de sources et de moyens d'attaque pour ces délinquants.
Tout ce qui est installé, introduit et (télé)chargé sur nos machines doit faire l'objet d'une sorte de scan ou contrôle si l'on veut rester dans une protection plus sereine.
Nous en sommes loin aujourd'hui quand nous validons la mise à jour d'un logiciel sans être sûr que l'envoi émane de la société en question. Certains internautes ont découvert tardivement que des exécutables s'étaient installés sur leur PC mais n'ont pu en mesurer l'impact sur leurs données, logiciels, etc.
L'objectif premier du hacker va être d'installer un virus ou un cheval de Troie sur votre ordinateur. Il se présente simplement sous la forme d'un exécutable (par exemple .exe), soit installé suite à l'attaque d'un de vos logiciels mal configurés ou obsolètes (la version installée n'est pas la dernière et contient donc des failles de sécurité). Ces failles sont en général la conséquence d'un bug de programmation dans l'application qu'un hacker saura mettre à profit pour prendre le contrôle de votre ordinateur. Ces logiciels sont très nombreux en voici quelques uns à titre d'exemple :
– Microsoft Windows ;
– Les suites bureautiques (Microsoft Office, OpenOffice) ;
– Les navigateurs (Internet Explorer, Firefox, Chrome, Opera, Safari) ;
– Les logiciels multimedia (Acrobat Reader, Flash, Shockwave, Windows Media Player, Quicktime, RealPlayer, WinAmp, iTunes, VLC) ;
– Les messageries instantanées (Windows Messenger, Pidgin) ;
– Java.

On a pu ainsi découvrir des cas de figure où les PC des internautes sont devenus des serveurs à leur insu se voyant alors stocker à des jours et des heures des données de personnes malveillantes qu'ils ne pouvaient alors contrôler sur leur propre machine.
De même d'autres ont accepté avec trop de simplicité et de naïveté une clé USB offerte avant l'entrée dans un salon ou symposium. Le but étant de garder la clé mais pas son contenu, ils ont ouvert cette dernière sans penser à l'exécutable qui allait s'installer sur la machine et qui allait devenir un moyen d'infiltration sans limite pour l'offreur.
Certaines applications sur ces clés vont même pendant qu'un tiers tente de recopier un fichier à partir de votre machine scruter votre PC pour lui sous-tirer tous vos contacts et ce que vous pouvez imaginer avec sans vous garantir qu'il n'aura pas pris la main sur votre PC pour y revenir ultérieurement.

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

Source : http://www.atlantico.fr/rdv/minute-tech/pirates-capables-voler-donnees-meme-votre-ordinateur-est-pas-connecte-internet-michel-nesterenko-1893142.html

---

Live streaming illégal : Le revers de la médaille

Live streaming illégal : Le revers de la médaille

Si depuis l'aube d'Internet, les sites pornographiques constituent le vecteur principal de propagation de virus sur la toile, les sites illégaux de live streaming représentent une concurrence de taille. Selon l'étude de l'AISP, alors que 97 % des sites de streaming illégaux sont infectés par des malwares (logiciels malveillants), faisant de cette pratique la voie d'infection la plus courante sur Internet, les plateformes illégales de live streaming représentent une grande partie des ces infections. Au point de devenir une véritable porte ouverte à la fraude et au vol de données.

Le streaming vidéo, qui constitue aujourd'hui 91 % du trafic Internet mondial, est depuis quelque temps déjà ancré dans le paysage virtuel mondial. Son pendant « en direct », le live streaming, est quant à lui entré dans les mœurs il y a peu. Développées en 2008 par des entreprises comme Youtube ou Google, les technologies permettant le visionnage et le partage de vidéos en direct sur Internet ont plus ou moins stagné depuis. Il faudra attendre la Coupe du monde de football 2014 au Brésil pour démocratiser la pratique dans le monde entier, mais surtout pour voir un véritable marché noir du live streaming se développer en parallèle. Du 12 juin au 13 juillet dernier, plus de 20 millions de personnes à travers le monde ont regardé les matches de la Coupe du monde en live streaming sur des sites illégaux.

Une question d'informations

Leur gratuité, si elle a permis à ces sites de se démocratiser, est aussi la cause principale de l'émergence des pirates dénoncée par l'AISP. Comme n'importe quelle marchandise ou service, un site peut être gratuit soit parce qu'il bénéficie de subventions ou de dons – une hypothèse peu probable pour les sites illégaux de live streaming – soit parce qu'il a minoré ses investissements dans son développement, le plus souvent au détriment de sa sécurité.

Faire sauter les pare-feu des sites illégaux de live streaming est ainsi bien souvent un jeu d'enfants pour pirates et hackers. Toujours selon ce rapport de l'AISP, certains d'entre eux vont même jusqu'à créer et développer leurs propres sites de live streaming illégal, infectés et porteurs de chevaux de Troie dès leurs créations, afin d'augmenter leurs chances d'attraper un internaute dans leur toile. Ainsi, alors que 160 000 nouveaux malwares sont créés par jour, les sites illégaux de live streaming ont envahi les moteurs de recherche et représentent une pierre de plus à l'édifice de menaces que constitue Internet aujourd'hui.

La toile est en effet souvent pointée du doigt comme la source de dangers toujours plus nombreux et variés. Des accusations parfois exagérées qui ne doivent pas faire oublier la responsabilité de l'internaute. Pour Anton Korobkov-Zemlianski, un membre de la commission de la science et des innovations de la Chambre publique de Russie, également expert en médias, Internet « présente moins de dangers que d'autres objets que nous utilisons. Les voitures causent la mort de beaucoup plus de monde qu'Internet (…) Beaucoup commencent à voir dans Internet une panacée appelée à simplifier leur vie. Le web ne simplifie pas notre vie, il crée des conditions nouvelles et exige que les gens changent et évoluent ».

Une réglementation comme le Code de la route est cependant impossible à mettre en place sur la toile, l'anonymat étant à la portée de tous sur Internet. La diffusion de l'information et la responsabilisation des usages apparaissent alors comme la plus fiable des solutions. Et tandis qu'il suffit d'ajuster son comportement aux risques et aux menaces d'Internet, « il vaut mieux prévenir que guérir » n'a jamais été aussi adapté.

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

Source : http://www.generation-nt.com/live-streaming-illegal-donnees-actualite-1909470.html
par Julien Hatier

Après le piratage, les employés de Sony reçoivent un email de menaces – L'Express avec L'Expansion

Après le piratage, les employés de Sony reçoivent un email de menaces – L'Express avec L'Expansion

Une semaine après s'être fait pirater, la société Sony Pictures a indiqué que ses employés avaient reçu un email de menaces d'un groupe de pirates informatiques. Le FBI enquête sur le dossier.

Les attaques viennent de toutes parts. Des employés de Sony Pictures, qui a fait l'objet la semaine dernière d'une attaque informatique massive, ont reçu un email de menaces qui se dit être du groupe de pirates informatique GOP (« Guardians of Peace ») a indiqué un porte-parole de la société américaine.
Il assure par ailleurs être « au courant du problème et travailler avec les forces de l'ordre ». Le FBI, la police fédérale américaine, enquête sur le dossier.

Les familles des employés aussi menacées
L'attaque informatique, qui s'est traduite par le vol de données personnelles d'employés de Sony, dont leurs adresses, dates de naissance et numéro de sécurité sociale, et la mise en ligne illégalement de cinq films du studio, a touché quelque 47 000 personnes, selon des experts informatiques.

L'email adressé aux employés est reproduit par Variety. Il ordonne à son destinataire d'envoyer son nom à une adresse email « si vous ne voulez pas faire l'objet de représailles ». « Si vous ne le faites pas, non seulement vous mais votre famille serez en danger », précise le message.

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

Source : http://lexpansion.lexpress.fr/high-tech/apres-le-piratage-les-employes-de-sony-recoivent-un-email-de-menaces_1629800.html

L’attaque informatique de Sony Pictures a touché 47.000 personnes

L’attaque informatique de Sony Pictures a touché 47.000 personnes

Les pirates informatiques responsables de la cyberattaque géante de Sony Pictures ont dévoilé des informations confidentielles de 47.000 individus dont des personnalités, ont affirmé vendredi des experts en sécurité informatique.

Les noms, adresses, numéros de sécurité sociale et dates de naissance ont ainsi été dérobés, autant d’informations permettant des usurpations d’identité, selon la société Identity Finder.
« Le plus inquiétant est le nombre très élevés de copies des numéros de sécurité sociale retrouvés dans les dossiers que nous avons analysés », a fait remarquer le président de cette société, Todd Feinman.
Il a précisé que ces numéros apparaissaient dans plus de 400 documents différents, « offrant aux pirates la possibilité de causer davantage de dégâts ». Selon lui, quelques 15.000 personnes, actuels ou anciens employés de Sony, ont eu leur numéro de sécurité sociale dérobé.
Sony Pictures a confirmé cette semaine avoir été victime d’un vol « très important de données confidentielles » fin novembre. En plus de ces informations confidentielles, cinq films, y compris des films pas encore sortis, avaient été piratés.

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

Source : http://www.jeanmarcmorandini.com/article-329895-l-attaque-informatique-de-sony-pictures-a-touche-47000-personnes.html

---

Cybercriminalité : le jeu en vaut-il la chandelle ?

Crédit Photo : Shutterstock

Cybercriminalité : le jeu en vaut-il la chandelle ?

Faire réaliser une page web factice pour faire du hammeçonnage ne coûte que 150 dollars

Attention, il n'est pas là question de dire qu'être un cybercriminel c'est bien… comme toute activité criminelle elle est punie par la loi avec des amendes et des peines de prison, nous y reviendront. Mais, tout de même, selon une étude Kaspersky, il semblerait que le ratio investissement/gains soit plus qu'intéressant… ce qui explique l'augmentation exponentielle de ce nouveau type de criminalité 2.0 qui ne nécessite plus du tout de courage. Assis tranquillement devant un ordinateur, les criminels n'ont plus rien à voir avec les gangsters des années 30.

Mais avant tout, une petite précision : tous les cybercriminels ne sont pas des hackers… et tous les hackers ne sont pas des cybercriminels. Bon nombre de cybercriminels ne font qu'acheter des logiciels préconçus par des hackers, les « Black Hats »… et il y a des hackers, les « White Hats », qui luttent justement contre ce derniers.

Le vol de données : peu d'investissement pour beaucoup de gain
Les cybercriminels qui ne veulent pas investir beaucoup dans un logiciel malveillant peuvent tout simplement faire du phising (hammeçonnage) de données. Pour 150 dollars, selon Kaspersky Lab, il est possible de se faire créer une page web similaire à celle visée (réseau social, site institutionnel, société…), de l'héberger et d'envoyer des spams (du style « Insérez vos données pour qu'on vous rembourse 450 euros de trop payé sur vos factures » et autres…)

Ce type de campagne de phising est souvent facilement décelable puisque de grossières fautes de grammaire et d'orthographe se glissent dans le texte. Mais malgré tout ça peut rapporter gros : en revendant les données ainsi captées (ne serait-ce que nom, prénom et adresse), le pirate peut toucher 100 dollars par personne touchée… avec 100 personnes touchées, les gains montent en flèche : 10 000 dollars.

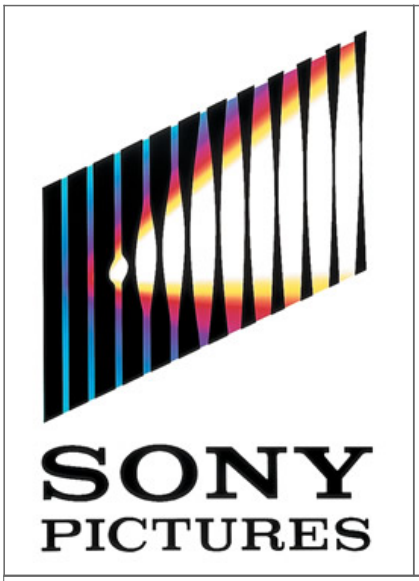
Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.economiematin.fr/news-cout-cybrecriminalite-enjeu-gain-piratage-revente-donnees

---

Piratage de Sony Pictures : le FBI met en garde contre un

malware « destructeur »



Piratage de Sony Pictures : le FBI met en garde contre un malware « destructeur »

Le piratage massif de Sony Pictures Entertainment la semaine dernière a motivé le FBI à tirer la sonnette d'alarme. Le bureau fédéral, qui enquête sur l'affaire, met en garde les entreprises concernant un logiciel malveillant « destructeur » utilisé par les pirates.

De toute évidence, le FBI ne prend pas le piratage de Sony Pictures à la légère. Le bureau fédéral d'investigation a communiqué par voie de presse pour mettre en garde les entreprises contre un nouveau malware. Ce dernier est décrit comme étant « destructeur », et serait à l'origine des déboires de Sony, dont plusieurs films encore inédits aux Etats-Unis ont été mis en ligne dans des versions piratées. Il faut cependant préciser que, dans son rapport d'alerte, le FBI ne cite jamais le nom de Sony. Néanmoins, pour des experts en sécurité interrogés par l'agence Reuters, il ne fait aucun doute que les autorités évoquent bien cette affaire.
Selon le FBI, « il s'agit de la première cyber-attaque destructrice menée contre une entreprise sur le sol américain ». Des manœuvres similaires ont été constatées en Asie et au Moyen-Orient, mais jamais aux USA jusqu'à aujourd'hui.

Concrètement, le logiciel malveillant remplace petit à petit les données présentes sur le disque dur, y compris dans les secteurs d'amorçages qui permettent à l'ordinateur de démarrer. Le système se retrouve donc bloqué, à la merci des pirates qui contrôlent le malware.
« Le FBI conseille régulièrement le secteur privé de divers indicateurs de cyber-menaces observés au cours de ses enquêtes » explique le porte-parole du bureau, Joshua Campbell. « Ces données sont fournies afin d'aider les administrateurs systèmes à se protéger des actions permanentes des cyber-criminels. » Les entreprises victimes de ce type d'attaques sont invitées à contacter les autorités au plus vite.

Du côté de Sony, si un porte-parole a récemment déclaré que l'entreprise avait d'ores et déjà restauré « un certain nombre de services importants », de nombreux documents ont été récupérés par les pirates durant l'intrusion, et pas seulement des films du studio. Des contrats de tournage et des papiers d'identité de certains comédiens font partie des fichiers volés. Quant à l'origine de l'attaque, elle reste toujours à confirmer, même si les soupçons sont tournés vers la Corée du Nord, qui n'aurait pas apprécié la sortie du film « L'Interview qui tue », comédie qui prend pour cible le régime politique du pays.

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

Source : http://www.clubic.com/antivirus-securite-informatique/virus-hacker-piratage/piratage-informatique/actualite-742501-piratage-sony-fbi-garde-malware-destructeur.html?estat_svc=s%3D223023201608%26crmID%3D639453874_766966538