Home Depot : finalement 56 millions de cartes bancaires piratées

Home Depot : finalement 56 millions de cartes bancaires piratées

Début septembre, l'enseignement américaine Home Depot révélait avoir observé une activité inhabituelle concernant les données de paiement de ses clients avant de reconnaître une intrusion informatique.

Home Depot expliquait ainsi que tout client ayant utilisé, depuis le mois d'avril, une carte bancaire pour régler un achat dans l'un de ses magasins aux Etats-Unis et au Canada est potentiellement concerné par le vol de ces données de paiement.
Le groupe ne chiffrait pas le nombre de clients affectés ni le détail exact des données personnelles compromises. Le New York Times évoquait le nombre de 60 millions de cartes de paiement compromises.

EMV
Bingo, Home Depot indique aujourd'hui que ce sont 56 millions de cartes bancaires ont été « mises en péril ». De quoi constituer un nouveau triste record en la matière, jusqu'ici détenu par Target (40 millions de cartes de paiement compromises).
D'ailleurs, comme pour Target, il semble que les pirates aient exploité une variante du programme malveillant BlackPOS installé dans le système de paiement de l'entreprise.
Seule bonne nouvelle, Home Depot estime qu'à ce stade de l'enquête aucune preuve ne permet d'établir que les codes PIN des cartes bancaires compromises figurent également parmi les données dérobées. Mais cette protection est assez peu utilisée aux Etats-Unis…
A la suite de cette intrusion informatique, dont l'ampleur doit encore être précisée, Home Depot a fait savoir qu'il déploierait sur l'ensemble de ses magasins, d'ici à octobre 2015, la technologie EMV de paiement pour cartes à puce. Ce standard international, en vigueur notamment en France, apporte en principe une sécurité accrue des transactions et contribue donc à réduire la fraude.

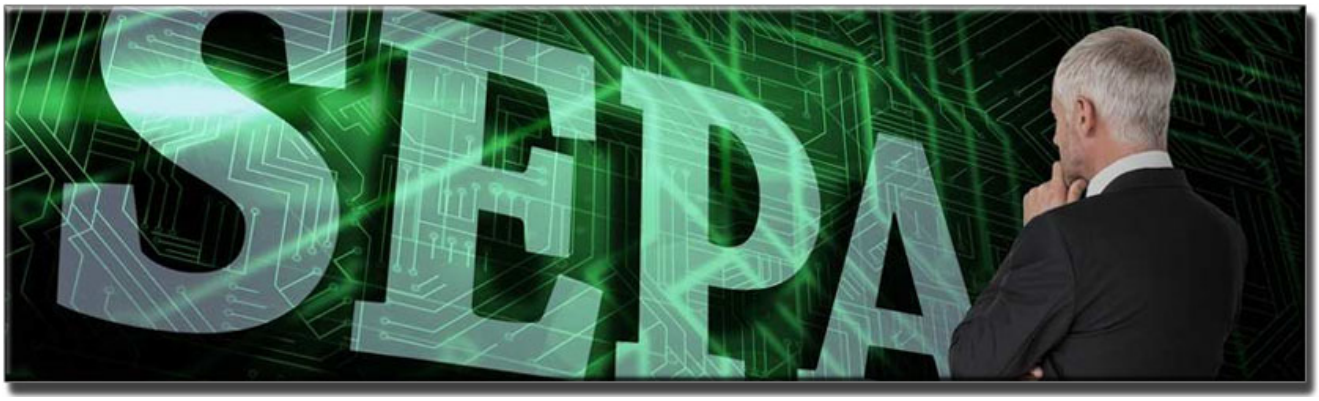
Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Source :
http://www.zdnet.fr/actualites/home-depot-finalement-56-millions-de-cartes-bancaires-piratees-39806615.htm

---

Près de 20% des entreprises

sont victimes d’escroqueries bancaires. La dernière ruse en vigueur est celle qui profite de la norme SEPA



Près de 20% des entreprises sont victimes d’escroqueries bancaires. La dernière ruse en vigueur est celle qui profite de la norme SEPA

Les entreprises font de plus en plus l'objet d'escroqueries bancaires avec un préjudice estimé à ce jour à environ 250 millions d'euros.
Les organisations professionnelles et les pouvoirs publics s'émeuvent de ce phénomène croissant qui montre l'ingéniosité de ces escrocs de plus en plus pointus en terme de détournement d'informations saisies en entrant dans les systèmes informatiques et réseaux.
Une entreprise sur six reconnait avoir été victime d'au moins une tentative de fraude en 2013. Les grandes PME sont les cibles préférées des escrocs.
Ce chiffre est le résultat d'une étude interne au secteur bancaire publié par la Fédération Bancaire Française.

Une entreprise sur deux comptant entre 500 et 1.000 salariés avec un chiffre d'affaires supérieur à 75 millions d'euros a déclaré avoir été visée par une tentative de fraude.

Ce chiffre descend entre 10 et 15% pour les plus petites entreprises.
Si ces fraudes touchent tous les secteurs d'activité sans exception, elles concernent plus fréquemment le commerce, compte tenu du grand nombre de transactions réalisées dans ce secteur.
Trois types de fraude à souligner :
Les fraudes aux virements internationaux peuvent se présenter sous plusieurs formes, selon une note d'information publiée par le Service Régional de Police Judiciaire de Clermont-Ferrand (SRPJ).

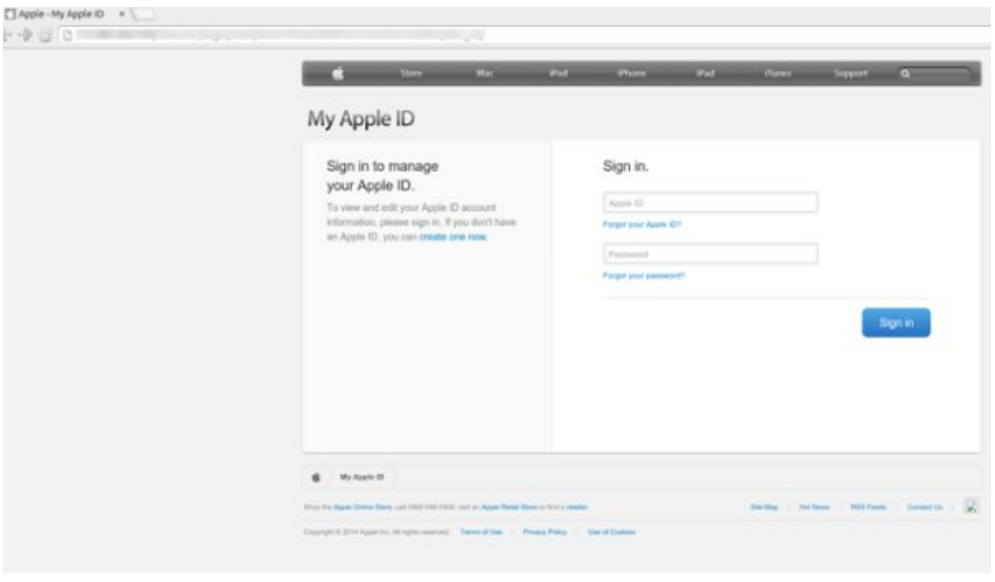
1. La première d'entre elles est baptisée «escroquerie à la nigériane», en raison de l'origine des escrocs qui opèrent depuis l'Ouest africain.
Ceux-ci détournent des transactions entre les entreprises françaises et leurs fournisseurs asiatiques.
Leur méthode consiste à envoyer des courriels aux entreprises en se faisant passer pour le fournisseur. Les fraudeurs parlent alors de «dysfonctionnements bancaires» et souhaitent que le prochain virement soit réalisé sur un compte «plus sécurisé» et …qui va donc tout droit chez eux !
2. Une autre technique de fraude est celle de l'«escroquerie au président » ou arnaque «au faux patron».
Selon le SRPJ, cette méthode est «la plus redoutable». Les escrocs exigent des virements des responsables d'une entreprise, en se faisant passer pour leur PDG.
Ce genre d'escroquerie nécessite selon les auteurs de l'étude «une autorité naturelle, un certain aplomb et, un don pour la comédie» pour duper le comptable qui exécutera servilement les instructions écrites du « faux patron ».Ceci passe par plusieurs ruses:
La première ruse consiste à insister sur le caractère urgent de la requête dans le cas d'un futur contrôle fiscal, ou autre évènement perturbateur annoncé.
La seconde catégorie, dite de «l'ingénierie sociale», est d'effectuer une collecte d'informations sur l'entreprise via les réseaux sociaux pour en adopter les codes.
Cette méthode qui touche un nombre restreint d'entreprise est de loin la plus redoutable car elle émane de bandes parfaitement organisées.
Pour les petites entreprises, les méthodes de fraude les plus répandues restent toutefois les plus banales, comme la fraude à la carte bancaire volée ou usurpée.
3. Enfin la dernière ruse en vigueur est celle qui profite de la norme SEPA, l'espace de paiement unique européen :Les escrocs se font passer pour le responsable informatique de la banque qui gère les comptes de l'entreprise ciblée. Ils arrivent alors à convaincre l'interlocuteur de la société d'effectuer une série de tests et, à distance, ils prennent le contrôle de l'ordinateur et effectuent des virements directement sur leur compte en banque.
Cette technique est rendue possible par le système SEPA grâce auquel la banque n'a plus à se soucier de l'accord du client avant d'effectuer un virement.
Le client peut toutefois contester l'opération dans le cas où il constate un virement anormal.
60% des entreprises sont satisfaites de la réaction de leur banque.
4. Enfin, il existe aussi un dernière fraude, plus automatisée, moins humaine car basée sur le principe de fonctionnement des virus : Les ransomwares.Un ransomware, ou rançongiciel, est un logiciel malveillant qui prend en otage des données personnelles. Pour ce faire, un rançongiciel chiffre des données personnelles puis demande à leur propriétaire d'envoyer de l'argent en échange de la clé qui permettra de les déchiffrer.
Un ransomware peut aussi bloquer l'accès de tout utilisateur à une machine jusqu'à ce qu'une clé ou un outil de débridage soit envoyé à la victime en échange d'une somme d'argent. Les modèles modernes de rançongiciels sont apparus en Russie initialement, mais on constate que le nombre d'attaques de ce type a grandement augmenté dans d'autres pays, entre autres l'Australie, l'Allemagne, les États-Unis.
Malheureusement, cette stratégie criminelle s'est avérée rentable et c'est pourquoi de nouvelles versions de cheval de Troie plus puissantes sont apparues en 2014. Nous souhaitions vous avertir contre le ransomware « Onion » (aussi connu sous le nom de CTB-Locker) qui utilise le réseau anonyme TOR (The Onion Router) et les Bitcoins pour mieux protéger des autorités, les criminels, leurs fonds et leurs clés d'accès aux fichiers des victimes.

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Source :
https://www.aiservice.fr/News/2014/Septembre/depannage-informatique-domicile-paris-2014-429-entreprises-sont-victimes-escroqueries-bancaires-derniere-ruse-norme-sepa-espace-de-paiement-unique-europeen
http://blog.kaspersky.fr/ransomwares-tor-cryptolocker/
http://fr.wikipedia.org/wiki/Ransomware
http://acteursdeleconomie.latribune.fr/finance-droit/2014-06-26/kpmg-les-dessous-d-une-escroquerie-record-a-7-6-millions.html

---

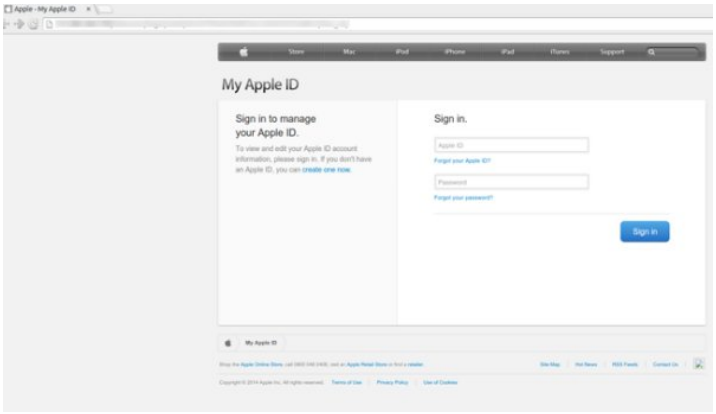
Alerte iCloud : une campagne de phishing tente de dérober des Apple ID



Alerte iCloud : une campagne de phishing tente de dérober des Apple ID

Le hack des photos de célébrités nues a-t-il donné des idées à des pirates ? Symantec signale en tout cas le lancement d'une campagne de phishing visant à dérober identifiants Apple et mots de passe.

Comme en politique, un évènement chasse l'autre. Une bonne chose pour Apple qui, grâce au lancement imminent de l'iPhone 6, a visiblement réussi à faire oublier la fuite sur Internet des photos de nombreuses vedettes américaines et les faiblesses de la sécurité de son service iCloud.
Souvent opportunistes, les cybercriminels voient au contraire dans cette récente actualité une bonne occasion de parvenir à leurs fins. Symantec signale ainsi le lancement d'une campagne de phishing visant justement à moissonner Apple ID et mots de passe auprès des utilisateurs d'Apple.



Attention, achat illicite sur votre compte ! Cliquez, vite !
La recette reste invariablement la même : des emails sont envoyés aux internautes et se présentent comme légitimes, ici envoyés par Apple. Le destinataire est ainsi informé d'un risque de compromission de son compte, un achat ayant été réalisé par son intermédiaire, depuis une IP en Russie.
Sans plus de surprise, l'internaute est prié de se rendre sur un site, reproduction d'un formulaire d'authentification d'Apple, afin de se connecter à son compte en saisissant pour cela son identifiant ainsi que son mot de passe. L'utilisateur abusé transmettra alors ses données d'accès aux pirates.

Et c'est peut-être notamment par le biais de mail de phishing que certaines des célébrités, utilisatrices d'iCloud, ont pu être abusées récemment et des photos intimes dérobées. Car selon Apple, ces informations ont été obtenues seulement par l'intermédiaire d'attaques ciblées et non grâce à une intrusion dans ses serveurs.

Néanmoins, dans une interview, Tim Cook s'est engagé à renforcer la sécurité de son service en ligne : authentification à deux facteurs, alerte mail lors de tentatives de modification du mot de passe, de la restauration des données iCloud sur de nouveaux terminaux ou de l'authentification depuis un terminal Apple encore non-enregistré.

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Source :
http://www.zdnet.fr/actualites/icloud-une-campagne-de-phishing-tente-de-derober-des-apple-id-39806035.htm

---

Comment sont volés les

smartphones

	**Comment sont volés les smartphones**

Le vol de mobiles en général et de smartphones en particulier reste une plaie, et ce malgré les dispositifs de protection et/ou de de désactivation mis en place par les fabricants et les opérateurs.

Une étude menée par IDG pour Lookout auprès de 2403 personnes tente de détailler le phénomène. Ainsi, parmi les utilisateurs détroussés, 32% des interrogés européens l'ont été par des pickpockets. Evidemment, le ton résolument alarmiste de l'étude doit être relativisé dans le sens où Lookout propose des solutions de sécurité pour les mobiles…
Le vol à l'arraché ou par ruse reste donc et de loin, le principal moyen de voir son précieux portable disparaître. L'oubli ne représente que 18% des pertes tandis que le vol à la maison ou dans sa voiture représente 11% des larcins.

Le lieu du délit varie selon les régions. Les Anglais constatent plus souvent des vols au bar, au pub ou en discothèque (23%). En France en revanche, les transports en commun semblent être le lieu de prédilection des voleurs (17%).

Prêts à payer pour récupérer leurs données
L'étude nous apprend également qu'il y a des heures « plus propices » aux vols. « Que ce soit au Royaume-Uni, en France ou Allemagne, la tranche horaire comprise entre midi et dix-sept heures semble être la plus courue des malfrats », peut-on lire.
Et le smartphone est désormais tellement une extension de sa personne que les utilisateurs sont prêts à prendre des risques pour le récupérer. Les Allemands semblent être les moins timides et les plus téméraires, 89% d'entre eux (71% au Royaume-Uni et 68% en France) étant prêts à se mettre en situation relativement dangereuse pour récupérer leur smartphone volé.
Pire, une victime sur 5 serait prête à payer 750 euros pour récupérer ses données perdues ! De quoi donner des idées, pas forcément très légales.
Les victimes françaises qui passent à l'action en cas de vol de leur téléphone procèdent de manière très organisée, la majorité d'entre eux déposant plainte auprès de la police locale (71%) et informant leur opérateur (74%). En Allemagne en revanche, seulement 58% des victimes signalent le vol à leur opérateur et 63% portent plainte auprès de la police.
Au lieu de cela, 26% des Allemands tendent à utiliser une application de localisation de mobiles (contre 17% de Français et 19% de Britanniques) lorsque leur téléphone est volé.

Avec des smartphones de plus en plus puissants et chers, il faudra encore renforcer les mesures anti-vol ce qui semble être le cas avec la généralisation de la fonction 'kill switch'.
La Californie vient ainsi de passer une loi qui contraindra les constructeurs à proposer ce 'kill switch' à l'utilisateur sur tous les portables vendus en Californie à compter du 1er juillet 2015. Ce n'est pas une première : le Minnesota avait ainsi déjà fait passer une loi comparable en mai.
De plus, les constructeurs ont déjà pris les devants. C'est notamment le cas d'Apple, qui propose à ses clients un 'kill switch' permettant de désactiver à distance les fonctionnalités de l'iPhone. Au mois de juin, le procureur général de la ville de New York avait ainsi plaidé en faveur de la mise en place de cette fonction, expliquant notamment que les vols d'iPhone avaient chuté de 38% d'une année sur l'autre, suite au déploiement de cette fonctionnalité au sein d'iOS 7.

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Source :
http://www.zdnet.fr/actualites/comment-sont-voles-les-smartphones-39805631.htm

Nouveau vol de données : Home Depot victime d'une cyberattaque et d'un vol massif de données ?

Nouveau vol de données : Home Depot victime d'une cyberattaque et d'un vol massif de données ?

Après Target, auprès de qui des pirates avaient dérobé des millions de données bancaires de clients, Home Depot pourrait bien être le dernier sur la liste. Les informations des clients de ses 2200 magasins aux US auraient été exposées pendant plusieurs mois.

Home Depot pourrait bien être la dernière enseigne américaine de la distribution à avoir fait l'objet d'une attaque informatique de grande envergure avec pour conséquence le vol de données bancaires de ses clients.
Toutefois, pour l'heure, l'entreprise ne confirme pas une telle menace. Le commerçant se borne pour le moment à faire savoir qu'il a identifié une « activité inhabituelle » en lien avec ses données de clientèle.
Néanmoins, plusieurs éléments semblent attester d'une fuite de données sensibles, dont l'ampleur reste à évaluer. D'après Brian Krebs, un spécialiste de la sécurité, Home Depot collabore avec les forces de police et « plusieurs banques » soupçonnent l'enseigne d'être la source de l'utilisation illicite de données bancaires vendues au marché noir.

Dernier naufrage d'une enseigne de distribution ?
« Protéger les données de nos clients est pour nous un sujet de très grande importante et nous faisons actuellement tout notre possible pour réunir des faits tout en nous efforçant de protéger les clients » commente auprès de la presse une porte-parole de Home Depot, qui admet la possibilité d'une faille.
« Si nous confirmons qu'une fuite s'est produite, nous nous assurerons que nos clients sont prévenus immédiatement » précise-t-elle ainsi. Et pour Brian Krebs, il y a bien eu fuite. Celle-ci aurait débuté en avril dernier et concernerait les 2.200 magasins de Home Depot aux US.
La faille pourrait ainsi s'avérer de plus grande ampleur que celle qui a touché Target en 2013, et pourtant déjà affecté plus de **110 millions de données clients (numéros de cartes, codes PIN et informations personnelles)**.

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Source :
http://www.zdnet.fr/actualites/home-depot-victime-d-une-cyberattaque-et-d-un-vol-massif-de-donnees-39805665.htm

Les fraudes bancaires touchent plus d’une entreprise sur six

Un peu moins de 20% des entreprises, victimes d’une fraude bancaire.

Les entreprises sont de plus en plus les cibles d'escrocs bancaires. Avec un préjudice estimé à ce jour à 250 millions d'euros, les pouvoirs publics et les organisations professionnelles tirent le signal d'alarme.

1 entreprise sur 6 affirme avoir été victime d'au moins une tentative de fraude en 2013. Ce chiffre est le résultat d'une étude interne au secteur bancaire publiée aujourd'hui par . Les grandes PME sont les cibles préférées des escrocs. En effet, une entreprise sur deux qui compte entre 500 et 1.000 salariés et qui a un chiffre d'affaires supérieur à 75 millions d'euros a déclaré avoir été la cible d'une tentative de fraude. Un chiffre qui retombe entre 10 et 15% pour les plus petites entreprises. Autre phénomène: si ces fraudes touchent tous les secteurs d'activité sans exception, elles visent très fréquemment le commerce, en raison du grand nombre de transactions réalisées dans ce secteur.

Trois types de fraude font fureur

Les fraudes aux virements internationaux peuvent se présenter sous plusieurs formes, comme l'indique une note d'information publiée par le Service Régional de Police Judiciaire de Clermont-Ferrand (SRPJ). La première d'entre elles est appelée «escroquerie à la nigériane», en raison du lieu d'agissement des escrocs, qui opèrent depuis la côte ouest africaine. Ceux-ci détournent des transactions entre les entreprises françaises et leurs fournisseurs asiatiques. Leur méthode: envoyer des courriels aux entreprises en se faisant passer pour le fournisseur. Les fraudeurs parlent alors de «dysfonctionnements bancaires» et souhaitent que le prochain virement soit réalisé sur un compte «plus sécurisé», qui va donc tout droit dans leur poche.

Une autre technique de fraude est celle de l'«escroquerie au président» ou arnaque «au faux patron». Selon le SRPJ de Clermont, cette méthode est «la plus redoutable». Les escrocs exigent des virements des responsables d'une entreprise, en se faisant passer pour leur PDG. Comme le décrit le SRPJ, ce genre d'escroquerie nécessite «une autorité naturelle, un certain aplomb et, il faut bien le reconnaître, un don pour la comédie». Un don qui passe par plusieurs ruses. Selon Les Echos, la première est d'insister sur le caractère urgent de la requête dans le cas d'un futur contrôle fiscal, d'une OPA ou autres. Les escrocs ne manquent pas d'imagination. La seconde, dite de «l'ingénierie sociale», est d'effectuer une collecte d'informations sur l'entreprise via les réseaux sociaux pour en adopter les codes. Et s'ajoute à cette pointe de réalisme une touche de flatterie. Comme l'indique le SRPJ, la supercherie aura plus de chance de fonctionner si le comptable de l'entreprise se sent «flatté d'être dans la confidence du patron». Cette méthode qui ne fait toutefois que peu de victimes est de loin la plus redoutable car elle émane de bandes parfaitement organisées. Pour les petites entreprises, les méthodes de fraude les plus répandues restent toutefois celles liées aux actions du quotidien, comme la fraude à la carte bancaire volée ou usurpée.

Enfin la dernière ruse à la mode est celle qui profite de la norme Sepa, l'espace de paiement unique européen. Les escrocs se font alors passer pour le responsable informatique de la banque qui gère les comptes de l'entreprise ciblée. Ils arrivent alors à convaincre l'interlocuteur de la société d'effectuer une série de tests et, à distance, ils prennent le contrôle de l'ordinateur et effectuent des virements directement sur leur compte en banque. Cette technique est rendue possible par le système Sepa grâce auquel la banque n'a plus à se soucier de l'accord du client avant d'effectuer un virement. Celui-ci peut toutefois contester l'opération dans le cas où il constate un virement anormal.

60% des entreprises sont satisfaites de la réaction de leur banque

Même si ces trois techniques sont les plus répandues, les fraudeurs ne manquent pas d'imagination pour escroquer les entreprises qui, dans bien des cas, ne pourront pas se faire rembourser les montants dérobés. Une fois le virement réalisé, elles peuvent en effet contacter leur banque, mais les établissements ne peuvent pas s'immiscer dans les ordres de paiement. Toutefois, les entreprises sont majoritairement satisfaites de la réaction de leur banque, à hauteur de 60%. Un pourcentage qui diminue pour les petites entreprises de moins de 20 salariés mais qui passe à 80% pour les grandes entreprises. Un chiffre qui dépend également du type de banque choisi par l'entreprise, les taux de satisfaction étant en effet plus élevés pour ceux qui optent pour une banque commerciale par rapport à une banque mutualiste.

Pour lutter contre ces fraudes, la Fédération bancaire Française (FBF) a annoncé qu'elle rencontrerait prochainement, avec des représentants de la police et de la justice, ses homologues chinois, pays d'où proviennent un grand nombre de fraudes. Pour le moment, elle a fait savoir dans une vidéo que «plusieurs centaines de procédures sont en cours au sein de la police judiciaire» pour un montant des préjudices qui se chiffre à «plus de 250 millions d'euros».

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Références :

http://www.lefigaro.fr/conjoncture/2014/08/22/20002-20140822ARTFIG00233-les-fraudes-bancaires-touchent-plus-d-une-entreprise-sur-six.php

---

4,5 millions de données médicales dérobées aux Etats-Unis – Un vol de données de

plus…

Community Health Systems, un spécialiste américain de la gestion des hôpitaux, a reconnu avoir été victime d'une attaque informatique entre avril et juin 2014. Résultats : 4,5 millions de données personnelles ont été dérobées. Un vol de données de plus…

Confidentialité des données : attention danger pour les DSI européens

	**Confidentialité des données : Attention danger pour les DSI européens**

Les DSI ne peuvent se préoccuper des seuls aspects technologiques des projets conduits au sein de l'entreprise. Si les décideurs IT veulent et doivent peser plus dans les décisions business, ils doivent alors composer avec les risques liés à l'activité de l'entreprise et non seulement ceux ayant trait au système d'information.
C'est notamment le cas de la confidentialité des données client. Or, juge Forrester, il s'agit même désormais d'une priorité, en particulier pour les DSI européens en raison de la régulation dans ce domaine et de la préoccupation croissante des européens à l'égard de leurs données.
Vie privée : une préoccupation pour le client et l'entreprise
Et selon le cabinet, l'arrêt de la CUJE sur le droit à l'oubli rappelle aux DSI que la gestion des données personnelles s'impose comme une des grandes priorités business. « La régulation de la confidentialité est désormais un sujet que les DSI ne devraient pas sous-estimer en tant que risque majeur pour les entreprises ».
Car, prévient Forrester, **un incident impliquant des données client peut déboucher sur des conséquences plus que significatives, comme une sanction financière, un préjudice d'image pour l'entreprise et une perte de confiance de la part des consommateurs**.
Et pour le DSI lui-même, c'est son emploi même qui pourrait être en jeu. Victime d'un piratage informatique (vol des données bancaires de 40 millions de clients), l'enseigne américaine Target a poussé son DSI à la démission – suivie ensuite de celle du PDG.
Mais la confidentialité des données n'est-elle pas avant tout du ressort des métiers et notamment des services marketing et juridique ? Non, selon Forrester pour qui la DSI est directement impliquée dans la gestion de ces données.
Quid de la collecte et du stockage des données client
Les responsables des systèmes d'information interviennent ainsi dans le choix et le déploiement des solutions destinées à garantir la sécurité et l'intégrité de ces informations. Les DSI doivent également s'informer des mécanismes de collecte des données, de leur localisation et des usages associés (transfert, partage, etc.). En clair, connaître le cycle de vie de la donnée.
Et cela peut s'avérer complexe estime Forrester, par exemple lorsqu'un client de l'entreprise demande à exercer son droit à la suppression. « De nombreuses entreprises stockent les données client de façon redondante, par exemple pour chaque division ou chaque pays. De telles données peuvent aussi avoir été sauvegardées sur plusieurs serveurs, souvent à des localisations distinctes ».
« Ces structures complexes de stockage des données client transforment une suppression complète des données en un exercice difficile – certains disent impossible » commente l'analyste Dan Bieler. La problématique de la confidentialité des données comprend donc bien une dimension technologique et impose dès lors aux DSI de ne pas la négliger.
« Les entreprises qui conçoivent leur infrastructure IT en gardant à l'esprit la régulation de la confidentialité [Ndlr : privacy by design] disposent d'un avantage compétitif pour cet ère du client », en particulier dans un contexte d'accroissement du nombre de données collectées, de leur numérisation et de leur exploitation, par exemple dans le cadre d'un projet Big Data.

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Références :
http://www.zdnet.fr/actualites/confidentialite-des-donnees-attention-danger-pour-les-dsi-europeens-39804963.htm

---

1,2 milliard d'identifiants volés par des pirates russes – Vol d'identifiants au

dessus d’un nid de coucou

1,2 milliard d’identifiants volés par des pirates russes _ Vol d’identifiants au dessus d’un nid de coucou

Le vol d’identifiants est passé à l’échelle supérieure avec la découverte que des cybercriminels russes avaient détourné 1,2 milliard de noms et mots de passe. A ce niveau, cela touche tout le monde, estime la firme de sécurité Hold Security qui a découvert ce groupe de pirates qu’il désigne sous le nom de CyberVor.
En Russie, des criminels ont constitué une énorme base constituée de 1,2 milliard de noms d’utilisateurs et de mots de passe volés, auxquels s’ajoutent 500 millions d’adresses e-mail, selon Hold Security, une société américaine spécialisée sur la sécurité Internet. Il s’agit probablement de la plus grosse base d’identifiants dérobés, récupérés d’attaques conduites dans tous les coins du web et qui ont touché environ 420 000 sites. « Jusqu’à présent, nous étions stupéfaits lorsque 10 000 mots de passe avaient été compromis, maintenant nous en sommes au stade du vol massif », a confié Alex Holden, fondateur de Hold Security, à nos confrères d’IDG News Service. Sa société n’a pas communiqué le nom des sites qui avaient été attaqués, invoquant des accords de confidentialité avec ses clients, mais elle a indiqué que cela incluait des familles et de petits sites web.

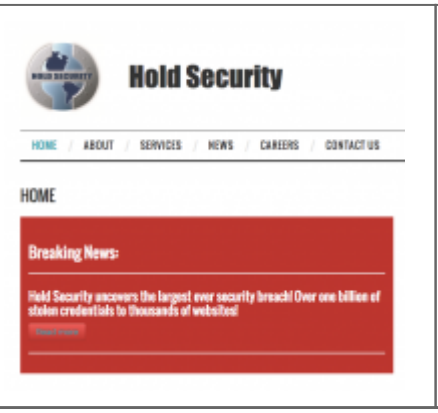
Le New York Times, qui fut le premier à rapporter ce vol, s’est adressé à un expert en sécurité indépendant pour vérifier que les données volées étaient authentiques. L’ampleur de la base constituée semble éclipser les précédentes découvertes de données compromises. Par comparaison, le vol subi par Target (révélé en janvier dernier) a affecté 40 millions de cartes de débit et 70 millions d’informations personnelles. C’est, en matière de détournement d’identifiants, l’un des faits de cybercriminalité les plus importants constatés jusqu’à présent et qui porte ce type de délit à un niveau supérieur. « Ces gens n’ont rien fait de nouveau ni d’innovant », constate Alex Holden. « Ils l’ont juste fait mieux et à un niveau de masse ce qui touche absolument tout le monde ».

Le gang CyberVor est constitué d’une douzaine de jeunes gens
Le groupe derrière l’attaque semble être basé dans le centre-sud de la Russie, a indiqué Alex Holden au New York Times. Selon les informations qu’il a communiquées au quotidien américain, il s’agit d’une douzaine de personnes d’une vingtaine d’années qui ne semblent pas avoir de liens avec le gouvernement. Avec des serveurs basés en Russie, le groupe a étendu ses activités cette année, probablement après avoir été en contact avec une organisation plus importante. Hold Security a dénommé le gang CyberVor d’après le mot russe « vor » (voleur). La société a indiqué qu’elle fournirait un service pour permettre aux utilisateurs de vérifier si leurs identifiants figurent parmi ceux qui ont été volés. L’information sera disponible dans deux mois environ. Le pré-enregistrement pour y accéder est possible dès maintenant.
Ce détournement massif de noms d’utilisateurs et de mots de passe met une fois de plus en lumière le peu de sécurité apportée par ces méthodes d’authentification, en particulier si les personnes se servent des mêmes noms et passwords pour plusieurs sites. Le recours à une méthode d’authentification à deux niveaux (avec envoi d’un code par SMS) renforce la sécurité mais ne constitue pas une garantie comme un utilisateur de PayPal vient tout juste de le démontrer. Après avoir, sans succès, alerté PayPal sur cette faille, il a expliqué comment cette fonction pouvait, en l’occurrence, être détournée via une connexion eBay.
Article de Martyn Williams / IDG News Service (adapté par Maryse Gros)

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Références :
http://www.lemondeinformatique.fr/actualites/lire-des-pirates-russes-ont-amasse-1-2-milliard-d-identifiants-58272.html?utm_source=mail&utm_medium=email&utm_campaign=Newsletter

Un milliards de mots de passe volés par un gang de pirates…



Un milliards de mots de passe volés par un gang de pirates…

Un petit groupe de cybercriminels a employé un botnet pour infiltrer des dizaines des milliers de sites web et récupérer une quantité gigantesque de données sensibles. Mais la firme qui a fait cette découverte en profite pour faire un formidable coup de com' et vendre un service derrière. Bizarre.La page d'accueil alarmiste de Hold Security, entreprise qui a révélé le piratage… Et qui propose une solution payante pour tenter d'y remédier.
Que vous soyez un expert en informatique ou un technophobe, à partir du moment où vous avez des données quelque part sur le web, vous pouvez être affecté par cette brèche. On ne vous a pas nécessairement volé directement. Vos données ont peut être été subtilisées à des services ou des fournisseurs auxquels vous avez confié des informations personnelles, à votre employeur, même à vos amis ou votre famille ». Voilà le discours flippant de Hold Security pour décrire la gigantesque collection de données personnelles volées que cette entreprise de sécurité a mis au jour.
Les chiffres présentés donnent en effet le tournis : d'après Hold Security, un gang d'une douzaine de hackers russes baptisé CyberVor aurait donc récupéré pas moins de 4,5 milliards de combinaisons de mots de passe et de noms d'utilisateurs. En omettant les doublons, CyberVor aurait accès à plus d'un milliard de comptes sur des milliers de sites différents, qui seraient rattachés à 500 millions d'adresses e-mail. Le hack du siècle, en somme.
Pour voler autant d'informations sensibles, CyberVor aurait usé de multiples sources et techniques, mais aurait surtout profité des services d'un botnet (un réseau de PC infectés par un logiciel malveillant) « qui a profité des ordinateurs des victimes pour identifier des vulnérabilités SQL sur les sites qu'ils visitaient. » Les membres de CyberVor auraient de cette manière identifié plus de 400 000 sites web vulnérables, qu'ils ont ensuite attaqué pour voler leur bases de données d'utilisateurs.

Des détails qui clochent
Sauf qu'il y a quelques petits détails qui clochent dans cette histoire. A commencer par le fait que Hold Security profite de cette annonce hallucinante pour tenter de s'enrichir immédiatement, en misant sur la peur du hacker qu'il a généré. En gros, la firme propose aux entreprises et aux particuliers de se préinscrire à un service –payant même s'il y a un essai gratuit- qui leur permettra notamment de savoir si oui ou non ils sont concernés par cette fuite de données. Et ce n'est pas donné : comptez 120 dollars par mois si vous êtes une entreprise.
D'autre part, Hold Security se refuse à donner le moindre nom de site dont la base a été piratée. Ce peut être compréhensible : son patron Alex Holden l'explique dans le New York Times, il ne souhaite pas révéler le nom des victimes pour des raisons de confidentialité. Il y aurait pourtant des entreprises du Fortune 500 selon lui dans le lot.
Mais comme le fait remarquer Forbes, il semble pour le moins étonnant (mais pas totalement impossible) que de si grandes entreprises se soient fait berner par une injection SQL, une technique très connue des hackers… et des experts en sécurité qui protègent les sites importants de telles attaques.

Des infos de piètre qualité ?
Il y a aussi de nombreuses informations qui manquent, dans la description de Hold Security. Quels botnets ont été utilisés ? Comment le malware a-t-il été inoculé dans la machine des victimes ? Et surtout pourquoi, comme l'indique le New York Times, le gang se contente-t-il d'utiliser pour l'instant leur fabuleuse base de données pour… envoyer du spam sur les réseaux sociaux, alors qu'ils pourraient à priori faire bien plus de mal ?
En réalité, il se peut que les milliards de mots de passe collectés par CyberVor étaient déjà disponibles sur le web underground depuis bien longtemps. Hold Security l'avoue sur son site : « Au départ, le gang a acquis des bases de données d'identifiants sur le marché noir ». Une pratique fort courante chez les cybercriminels, mais qui ne repose pas sur le moindre hack : il suffit de payer. Il est fort possible que ces « collectionneurs » aient au fil du temps accumulé un nombre de données incroyable, mais pas forcément « fraîches » et donc de piètre qualité. Il se peut aussi que la technique de l'audit d'un site par un botnet ait été fructueuse… Sur des sites de moindre envergure, voire des sites perso, mal sécurisés, qui n'ont pas fourni à Cybervor de quoi faire autre chose que du spam sur Twitter.
Quoiqu'il en soit, l'annonce de Hold Security vous donne une excellente excuse pour changer dès aujourd'hui vos mots de passe, ça ne fait jamais de mal !

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Références :
http://www.01net.com/editorial/624854/comment-un-gang-de-pirates-a-t-il-pu-voler-plus-d-un-milliard-de-mots-de-passe/#?xtor=EPR-1-NL-01net-Actus-20140806