La CNIL veut encadrer le traçage des clients dans les magasins

La CNIL veut encadrer le traçage des clients dans les magasins

La Commission indique qu'elle souhaite garder le contrôle et encadrer les dispositifs de traçage et de profilage des clients dans les magasins, les supermarchés et les centres commerciaux.
A mesure que les smartphones équipent de plus en plus de personnes, les commerçants comptent bien tirer parti de ces appareils nichés dans nos poches. Que ce soit pour de la mesure de fréquentation ou simplement de l'analyse comportementale, les téléphones portables permettent d'identifier facilement les cibles. La CNIL tente de protéger les consommateurs que nous sommes en mettant plusieurs garde-fous.

Ainsi, dans certains centres commerciaux, la fréquentation des magasins est mesurée : des boîtiers captent les données émises par le téléphone portable (adresses MAC de la carte réseau par exemple) et calculent la position géographique des personnes. Ainsi, il est possible de connaître la fréquentation, mais aussi le parcours des personnes à l'intérieur du centre (la géolocalisation indoor).

La CNIL note que les personnes doivent d'abord en être informées. « Une information claire doit être affichée dans les lieux où sont mis en place ces dispositifs », demande-t-elle avant d'émettre des propositions de mesures. Par exemple, la suppression des données lorsque le client sort du magasin. Ou encore : l'algorithme d'anonymisation utilisé doit assurer un fort taux de collision, c'est-à-dire qu'un identifiant en base doit correspondre à de nombreuses personnes.

Mesure d'audience
Autre point sensible : la mesure d'audience avec par exemple les panneaux publicitaires. « Ils permettent de compter le nombre de personnes qui regardent la publicité et le temps passé devant celle-ci, d'estimer leur âge et leur sexe, voire d'analyser certains comportements », rappelle la CNIL.
Là encore elle émet des mesures simples à appliquer, comme l'interdiction de l'enregistrement des images, de leur transmission à des tiers ou de leur visualisation auprès des prestataires. Une nouvelle fois, les clients doivent être informés de ce qu'il se passe. Car « ces dispositifs reposent sur des caméras placées sur des panneaux publicitaires » et ne sont pas forcément visibles.

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

Références :
http://www.linformaticien.com/actualites/id/33899/la-cnil-veut-encadrer-le-tracage-des-clients-dans-les-magasins.aspx

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

Et si le Cloud ne respectait pas vos données personnelles ?

	**Et si le Cloud ne respectait pas vos données personnelles ?**

Seulement 1% des fournisseurs de Cloud est prêt pour la prochaine loi UE La grande majorité des fournisseurs de cloud ne sont pas encore préparés à répondre aux exigences de la nouvelle directive sur la protection des données, dite « EU General Data Protection Regulation », qui devrait entrer en application l'année prochaine. Une loi qui remplacera l'ancienne directive de 1995 sur la protection des données (EU Data Protection Directive).
Selon les conclusions d'une étude réalisée par le spécialiste de la sécurité de Skyhigh Networks, seulement 1 fournisseur de services cloud sur 100 est prêt pour respecter la nouvelle directive portant sur la protection des données. Une loi qui entend moderniser l'ancienne régulation pour s'aligner sur les contraintes imposées par Internet et le Cloud.
La nouvelle directive, qui devrait être votée en 2014 pour une implémentation en 2015, impose aux contrôleurs des données (les entreprises propriétaires des données), à ceux qui traitent les données (tels que les fournisseurs de cloud et les hébergeurs) de **partager leur responsabilité en matière de fuite de données et de violations de la loi**.
Cette nouvelle loi s'appliquera aux entreprises européennes qui traitent des données personnelles et aux entreprises hors de l'Europe, qui contrôlent les citoyens européens ou traitent des données personnelles obtenues à partir de biens ou de services offerts aux citoyens européens.
Un examen de plus de 7 000 services cloud, effectué par Skyhigh Networks , a ainsi révélé que les fournisseurs ont des problèmes évidents avec les contraintes imposées par la nouvelle loi, notamment au sujet de la résidence des données, de la détection et de la notification des fuites de données, du chiffrement et des politiques de suppression des données (le droit à l'oubli).
« Il est sidérant de constater que peu de fournisseurs cloud sont préparés aux nouvelles régulations européennes, mais heureusement, il reste encore du temps pour se mettre en conformité. Cela implique de résoudre dès maintenant un certain nombre de problèmes, comme le droit à l'oubli, et d'implémenter des politiques de protection des données qui soient conformes à ces nouveaux standards », affirme Charles Howe, directeur de Skyhigh Networks pour l'Europe.
Cette nouvelle loi vise également à renforcer la confiance des consommateurs et des entreprises dans l'économie numérique en Europe.
« Pour les fournisseurs de cloud, cela implique inévitablement des ressources ainsi que des dépenses supplémentaires, mais ce n'est rien comparé aux pénalités pour violation de la loi, qui peuvent atteindre jusqu'à 5% des revenus annuels d'une entreprises ou jusqu'à 100 millions d'euros. »
Ce qui tranche avec la directive de 1995 qui ne comportait aucune démarche en matière de pénalités. Ces lourdes amendes vont transformer la protection données en un enjeu crucial et obligeront les entreprises à passer en revue ce qu'elles doivent faire pour se mettre en conformité, soutiennent quelques experts.

Le droit à l'oubli – un parcours difficile
L'un des amendements les plus controversés est le droit à l'oubli – les individus ont le droit civique de demander que leurs informations personnelles soient supprimées d'Internet. « Il s'agit d'un problème complexe, mais étant donné l'intérêt des medias, il est peu probable que les fournisseurs de cloud soient pris par surprise », explique Howe.

« Un gros problème est que 63% des fournisseurs cloud conservent leurs données indéfiniment et n'ont aucune disposition en matière de rétention des données dans leurs conditions de vente », ajoute-t-il.

Une autre donnée vient s'ajouter : **23% des fournisseurs cloud gardent la notion de droit de partager les données avec d'autres entreprises tierces dans leur condition de vente**. Ce qui complique un peu plus le fait de garantir la suppression de toutes les données, a également révélé l'étude. « Il est juste de dire que le droit à l'oubli peut s'avérer être un vrai parcours du combattant pour de nombreuses entreprises – les fournisseurs de cloud eux-mêmes et leurs clients. Il ne s'agit pas que d'un problème pour Google », soutient Howe.

L'étude rapporte également que seulement 11 pays sont conformes aux contraintes de l'UE en matière de résidence des données. La loi impose que les entreprises ne stockent ni ne transfèrent des données dans des pays hors de la zone européenne qui n'ont pas de standards équivalents en matière de protection des données.

La question de la résidence des données se pose également pour fournisseurs de cloud avec des datacenters dans le monde, qui dans leurs opérations courantes peuvent transférer ou stocker des données dans des pays qui ne sont pas conformes aux règles européennes. Les Etats-Unis, où 67% des datacenters pour le cloud sont localisés, font partie de ces 11 pays.

La résidence des données sera une difficulté clé pour les services cloud lorsque la nouvelle loi entrera en vigueur – puisque seulement 8,9% des fournisseurs américains disposent de la Safe Harbour Certification, qui les exempte de cette contrainte, soutient Skyhigh Networks.

« Un brouillon de **la nouvelle loi obligeait les entreprises à notifier aux autorités européennes dans les 24 heures, une fuite de données**, même si celle-ci est intervenue dans un service cloud tiers. Le problème tient au fait que de nombreux fournisseurs de cloud tiennent expressément responsable le client de la détection de faille et cela peut être une opération impossible », ajoute encore Howe.

« Certaines régulations en place, comme au Royaume-Uni ou en France, permettent aux entreprises de contourner les contraintes liées à la notification de failles, si les données sont rendues inaccessibles via le chiffrement. Malheureusement, seulement 1,2% des fournisseurs de cloud propose la gestion des clés de chiffrement nécessaires pour cela », commente-t-il.

« La difficulté est que seuls quelques fournisseurs de cloud proposent des outils pour protéger nativement les données. En fait, seulement 2,9% des services cloud ont en place un système de mots de passe sécurisés. « La General Data Protection Regulation n'entre pas en application avant 2015, mais il reste encore beaucoup de travail à accomplir jusque-là », conclut Howe.

Lien pour télécharger l'étude :
http://info.skyhighnetworks.com/Cloud-Adopt–Risk-Report-July-2014_Registration.html

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

Références :
http://www.lemagit.fr/actualites/2240226789/Protection-des-donnees-1-fournisseur-de-cloud-sur-100-pas-pret-pour-la-prochaine-loi-UE

La CNIL lancera des contrôles à partir du mois d’octobre sur la gestion des cookies

	La CNIL lancera des contrôles à partir du mois d’octobre sur la gestion des cookies

La Commission Nationale de l'Informatique et des Libertés (CNIL) vient d'annoncer qu'elle allait mettre prochainement en oeuvre des contrôles sur internet pour vérifier l'application de la nouvelle législation relative aux cookies. Il est grand temps de mettre votre site internet en conformité !

La législation française relative aux cookies informatiques a été modifiée par l'ordonnance du 24 août 2011, qui a révisé l'article 32 II de la loi Informatique & Libertés du 6 janvier 1978.
Depuis lors, l'utilisation de ces cookies est soumise à l'information préalable des internautes, voire également à leur consentement préalable si le cookie n'a pas une finalité purement technique (comme ceux utilisés pour mémoriser un panier d'achat sur un site commerçant, par exemple).
D'une part, la loi énonce le principe selon lequel l'utilisateur doit être informé « de manière claire et complète » de tout traitement de ses données à caractère personnel.
Ceci suppose que l'utilisateur ait pu prendre connaissance, avant la pose du cookie, de l'objet de ce cookie (ce dont il s'agit) et de sa finalité (ce à quoi il vise), ainsi que de la possibilité de s'opposer à cette pose.

Avant la modification de la loi en France, cette information préalable prenait parfois la forme d'une simple clause dans les Conditions générales de vente ou les Conditions générales d'utilisation des sites internet utilisateurs de cookies.
Désormais, la CNIL considère qu'une telle clause n'est pas suffisante. Si elle reste possible, elle doit être assortie d'une mention plus explicite, par exemple sous la forme d'un bandeau diffusé sur la page d'accueil du site.
D'autre part, en ce qui concerne l'obtention du consentement des internautes, la loi dispose que « l'abonné ou la personne utilisatrice [doit avoir] exprimé, après avoir reçu cette information, son accord ».
Après consultation des acteurs et notamment des annonceurs professionnels, la CNIL considère désormais que, si le consentement doit toujours se manifester par le biais d'une « action positive » de la personne préalablement informée des conséquences de son choix et disposant des moyens de l'exercer, ce consentement peut être simplement présumé si l'internaute a été explicitement informé que la poursuite de la navigation vaut accord du dépôt du cookie.
Le consentement de l'internaute peut donc être présumé, sous réserve que l'information préalable ait été suffisamment claire et explicite. Mais en tout état de cause, l'internaute doit toujours pouvoir revenir sur son consentement et s'opposer ultérieurement à l'utilisation des cookies par un site internet. En d'autres termes, il est fondamental que tout site internet prévoie une page dédiée spécifiquement aux cookies, indiquant leur finalité et mettant en place un système d'opposition.
A ce jour, si l'on constate que de nombreux sites internet se sont conformés à la nouvelle législation, tous n'ont pas encore été modifiés : parfois, non seulement les internautes ne sont pas informés de l'utilisation de cookies par le biais d'un bandeau sur la page d'accueil du site, mais leur consentement n'est pas recueilli. De même, certaines conditions générales d'utilisation se contentent de préciser que le site utilise des cookies, sans faire la moindre référence à la notion de consentement.
Or la CNIL vient d'annoncer qu'elle allait contrôler le respect de la nouvelle règlementation à partir du mois d'octobre 2014. Si elle a laissé le temps aux opérateurs de se conformer aux nouvelles dispositions légales, le temps de la transition est terminé. La CNIL va utiliser ses pouvoirs de vérification sur place ainsi que ses nouveaux pouvoirs de contrôle en ligne.
La CNIL annonce qu'elle contrôlera le type de cookies utilisé, leur finalité, ainsi que les modalités de recueil du consentement, la visibilité, la qualité et la simplicité de l'information relative aux cookies.
L'autorité indique que, selon le bilan des contrôles qu'elle sera conduite à effectuer, elle pourra adopter des mises en demeure voire des sanctions à l'égard des entités qui n'auront pas respecté la loi.
Il est donc urgent, pour chacun des exploitants de site internet, de se mettre en conformité avec cette nouvelle législation.

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

Références :
http://www.journaldunet.com/ebusiness/expert/58185/cookies–la-cnil-lancera-ses-controles-a-partir-du-mois-d-octobre.shtml

---

Google monte une équipe de supers hackers pour traquer

les failles informatiques

Une équipe de supers hackers pour traquer les failles informatiques

Google veut éradiquer les bugs qui peuvent être exploités par les pirates, mais aussi le gouvernement.

On croirait lire le scénario d'un film d'espionnage. Google a annoncé la création d'une équipe spéciale chargée de traquer les failles informatiques. Dénommée Project Zero, cette nouvelle équipe de sécurité sera composée des meilleurs hackers. Parmi eux, George Hortz, un Américain de 24 ans, surtout connu pour avoir piraté l'écran verrouillé de l'iPhone à l'âge de 17 ans et la Playstation 3, raconte le magazine spécialisé Wired. Quand il a découvert, au début de l'année, des failles dans le système d'exploitation de Google, Chrome OS, l'entreprise l'a payé 150.000 dollars pour les corriger. Outre Hortz, Project Zero accueille d'autres hackers célèbres, et Chris Evans , le recruteur du projet, continue de chercher des talents.

Project Zero sera chargée de trouver les failles dîtes «zero-day», c'est à dire des vulnérabilités qui n'ont pour l'instant jamais été découvertes et peuvent être dangereuses si elles sont exploitées par des pirates. L'équipe travaillera sur n'importe quel produit, et donc pas uniquement sur ceux de Google. «Nous ne posons pas de limite particulière à ce projet et travaillerons à l'amélioration de la sécurité de n'importe quel programme informatique utilisé par de nombreuses personnes. Nous porteront une grande attention aux techniques, aux cibles et aux motivations des attaquants», explique Chris Evans dans son communiqué.

Une réponse de Google à Heartbleed
Ce projet de Google arrive après Heartbleed, la faille de sécurité qui a secoué Internet il y a quelques mois. Fin avril déjà, l'entreprise s'associait à Facebook, Microsoft et d'autres pour lancer la Core Infrastructure Initiative. Un regroupement qui finance les projets Open Source en difficulté financière, et donc ceux qui seraient le plus exposés à une faille de sécurité passée inaperçue. Project Zero c'est aussi la réponse de Google à la NSA. La firme a mal encaissé les failles utilisées par l'agence américaine pour espionner ses utilisateurs. Google a déjà mis en place de nouveaux mécanismes de sécurité pour mieux protéger ses données.
Le mythe des hackers embauchés par les entreprises dont ils révèlent les failles n'est pas nouveau. En 2011, Apple embauchait Nicholas Allegra. À 19 ans, il était un membre éminent de la communauté du jailbreaking, c'est à dire du débridage d'iOS (le système d'exploitation des iPads et iPhones). Un an plus tard, la firme embauchait Kristin Paget dans son équipe de sécurité. Cette informaticienne avait longtemps fait partie d'un groupe de hackers éminents qui avait révélé des failles chez Microsoft.

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

Références :
http://www.lefigaro.fr/secteur/high-tech/2014/07/16/01007-20140716ARTFIG00221-google-monte-une-equipe-de-supers-hackers-pour-traquer-les-failles-informatiques.php

---

Les objets connectés ont de véritables problèmes en matière de sécurité

Les objets connectés ont de véritables problèmes en matière de sécurité

Connexions Bluetooth bavardes, chiffrement de piètre qualité, politiques de protection des données personnelles inexistantes… Les accessoires connectés ont tendance à vous mettre à nu.

Votre dernière course en forêt, vos déplacements à l'étranger, vos phases de sommeil, votre consommation en nicotine ou alcool, vos cycles de menstruations (si vous êtes une femme), votre pression artérielle, votre activité sexuelle… Pour toute activité personnelle, il y a désormais une application mobile et un accessoire connecté pour capter ces informations, comme par exemple le Nike Fuel Band. Et les utilisateurs en raffolent, si l'on croit les analystes. Selon Pew Research Center, plus de 60 % des Américains utilisent ces outils pour améliorer leur performances sportives ou préserver leur bonne santé. D'ici à 2018, le nombre de ces accessoires connectés devrait dépasser les 485 millions d'unités. Un marché en plein boom que tous les grands acteurs cherchent à accaparer, à commencer par Google et Apple.

Mais ce marché est encore très balbutiant, et notamment en matière de protection de données personnelles. Symantec vient de publier, il y a quelques jours, un rapport d'analyse qui évalue le niveau de sécurité de tous ces engins. Résultat: la plupart des applications révèlent des failles flagrantes permettant à des tiers de récupérer des données à l'insu des utilisateurs. Une majorité des bracelets peuvent être localisés grâces à leurs puces Bluetooth. Activés en permanence, ils sont plutôt bavards et émettent une adresse physique de type MAC, ainsi que des identifiants divers et variés, qu'il est aisé de capter dans un rayon de 100 mètres.
C'est d'ailleurs ce que les analystes de Symantec ont fait: ils ont créé des sniffeurs Bluetooth basés sur une carte Raspberry Pi, qu'ils ont disséminés aux abords d'une compétition sportive, ou trimballés dans un sac à dos en plein milieu d'un centre commercial. Certes, ces données ne permettent pas d'identifier une personne, mais c'est un premier pas…

Des mots de passe transmis en clair
Autre problème: parmi les applications qui utilisent des services cloud pour stocker ou traiter les données captées, 20 % transmettent les identifiants en clair, sans aucun chiffrement. Parmi les 80 % restantes, certaines appliquent aux identifiants des fonctions de hachage de faible protection comme MD5, qui peut facilement être craqué par les cybercriminels.
Dans un certain nombre de cas, la gestion de sessions laisse également à désirer, permettant par exemple de deviner ou de calculer des identifiants et ainsi d'accéder à des comptes utilisateurs.
Enfin, plus de la moitié des applications (52 %) n'apportent aucune information sur la manière dont toutes ces données sont traitées et stockées, alors que c'est obligatoire dans bon nombre de pays. Et quand il existe un document d'information, celui-ci est souvent très vague. On peut donc douter du sérieux de ces fournisseurs en matière de protection des données personnelles.
En somme: si toutes ces nouveaux appareils et applications semblent bien pratiques, il est conseillé de regarder en détail leur fonctionnement, histoire de pas se faire avoir !

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

Références :
http://www.01net.com/editorial/624818/les-objets-connectes-sont-des-passoires-en-matiere-de-securite/#?xtor=EPR-1-NL-01net-Actus-20140806

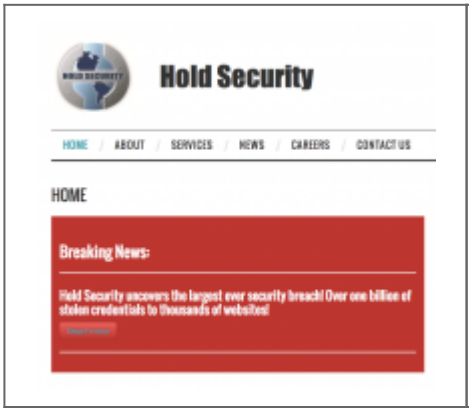
Google espionne et dénonce des pédophiles aux Etats Unis. Qu'en est t-il en

France ?

Google espionne et dénonce des pédophiles aux Etats Unis. Qu'en est t-il en France ?
Google a fait arrêter un Américain qui échangeait des photos pédopornographiques. Une pratique dont la légalité reste à prouver.

Il a alerté les autorités après avoir découvert des photos pédopornographiques dans les e-mails d'un habitant de Houston (Texas, Etats-Unis), rapporte la chaîne locale KHOU. Ce Texan, déjà coupable d'agression sexuelle sur un garçon de 8 ans en 1994, a été inculpé pour possession de pornographie infantile et promotion de pédopornographie.

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

Un logiciel d'extorsion (ransomware) utilise un simple fichier batch

Un logiciel d'extorsion (ransomware) utilise un simple fichier batch
Informatique

Des chercheurs de Symantec ont récemment identifié une menace d'extorsion qui fonctionne avec un script et une ligne de commande en utilisant le programme de chiffrement Open Source

GnuPG.

Pour extorquer de l'argent aux utilisateurs, des pirates ont mis au point un nouveau programme capable de chiffrer les fichiers sur l'ordinateur cible. Ce nouveau type de malware indique que les attaquants n'ont plus besoin de compétences pointues en programmation pour créer de dangereux programmes d'extorsion (ransomware) très efficaces, surtout quand les technologies de chiffrement avancé sont accessibles gratuitement. Des chercheurs du fournisseur d'antivirus Symantec sont récemment tombés sur un logiciel malveillant de ce type, d'origine russe, dont le composant principal se limite à un simple fichier batch, c'est à dire un script avec une ligne de commande. Cette stratégie de développement permet à l'attaquant de contrôler et de mettre facilement à jour le malware, explique dans un billet le chercheur Kazumasa Itabashi.

Le fichier batch télécharge une clef publique RSA en 1024 bits depuis un serveur et l'importe dans GnuPG, un programme de chiffrement gratuit qui fonctionne également par ligne de commande. GnuPG est une implémentation Open Source de la norme de chiffrement OpenPGP. Il est utilisé pour chiffrer les fichiers de la victime avec la clé téléchargée. « Si l'utilisateur veut déchiffrer les fichiers concernés, ils a besoin de récupérer la clé privée de l'auteur du malware », indique le chercheur.

Une rançon de 150 € pour déchiffrer ses propres données

Dans le chiffrement à clé publique sur lequel est basé OpenPGP, les utilisateurs génèrent une paire de clés associées, l'une rendue publique et l'autre qui reste privée. Le contenu chiffré avec une clé publique ne peut être déchiffré qu'avec la clé privée correspondante. La nouvelle menace représentée par le ransomware que Symantec appelle Trojan.Ransomcrypt.L chiffre les fichiers avec les extensions

suivantes: .xls, .xlsx, .doc, .docx, .pdf, .jpg, .cd, .jpeg, .1cd, .rar, .mdb et .zip. Les victimes sont invitées à payer une rançon de 150 € pour récupérer la clef privée.

Ce qui distingue le Trojan.Ransomcrypt.L des autres malwares ne tient pas à l'usage du chiffrement à clé publique – d'autres menaces adoptent la même technique – mais à sa simplicité et au fait que l'auteur a choisi d'utiliser un programme de chiffrement légal et Open Source, au lieu de créer sa propre mise en oeuvre, ce que font souvent les auteurs de malwares.

Les chercheurs prévoient une augmentation des menaces

Il existe certains programmes d'extorsion complexes avec des fonctionnalités avancées, développés essentiellement pour être vendus à d'autres cybercriminels qui n'ont pas les compétences nécessaires. Mais Trojan.Ransomcrypt.L montre qu'il est devenu possible de développer ce type de logiciels malveillants à peu de frais et sans connaissance de programmation avancée. Si bien que les chercheurs de Symantec s'attendent à une augmentation du nombre de menaces de ce type dans l'avenir.

Article de Jean Elyan avec IDG News Service

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

Références :

http://www.lemondeinformatique.fr/actualites/lire-un-logiciel-d-extorsion-utilise-un-simple-fichier-batch-58248.html?utm_source=mail&utm_medium=email&utm_campaign=Newsletter

Vol de données et racket auprès de la BCE (Banque centrale européenne)

Vol de données et racket auprès de la BCE (Banque centrale européenne)

Par le biais d'un email anonyme, un pirate a tenté d'extorquer de l'argent à la BCE en échange de données dérobées dans une base de données liée au site Web de la Banque centrale. Les données de marché sensibles n'ont pas été compromises.

Dans un communiqué, la BCE, la Banque centrale européenne, responsable de la monnaie unique au sein de l'UE, alerte sur le vol d'une base de données de contacts. Selon La Tribune, ce sont potentiellement 20.000 personnes dont les données pourraient être ainsi exposées.

La BCE précise que seules des informations de contacts, dont des adresses email, des noms et coordonnées, ont été dérobées dans cette base de données isolée de son système interne. « Aucune donnée sensible de marché n'a été compromise » assure ainsi la Banque centrale.

Des données partiellement chiffrées

Cette base de données est attachée au site Web de la BCE et

contient l’identité des personnes inscrites à des évènements organisés par la Banque, dont ses conférences. Celle-ci précise que seule une partie des données volées sont chiffrées – la nature de ce chiffrement n’est pas mentionnée.

La BCE contacte actuellement l’ensemble des personnes dont les données pourraient ainsi avoir été compromises et a, par précaution, réinitialisé l’ensemble des mots de passe. Une vulnérabilité, non spécifiée mais corrigée selon la BCE, serait à l’origine du vol.

Et comment la Banque centrale a-t-il pris connaissance de cette intrusion informatique ? Grâce à un email anonyme, n’émanant toutefois pas d’un bienfaiteur. Au contraire, l’auteur du message a exigé de l’argent en échange des données subtilisées. La justice allemande – le siège de la BCE est à Francfort – a été saisie et une enquête de police a été ouverte.

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

Références :

http://www.zdnet.fr/actualites/vol-de-donnees-et-racket-aupres-de-la-banque-centrale-europeenne-39804225.htm