Enfin une protection contre les attaques informatiques de type DDoS ?

Enfin une protection contre les attaques informatiques de type DDoS ?

Comment lutter efficacement contre les attaque de type DDoS ? Telle est la problématique que Google souhaite résoudre en lançant son Project Shield tout en faisant appel aux sociétés souhaitant participer à ce programme.
Le DDoS (**D**istributed **D**enial **O**f **S**ervice) est l'une des attaques les plus fréquentes sur Internet. Celle-ci consiste à paramétrer plusieurs ordinateurs ou serveurs lançant des requêtes automatiques et répétées vers un serveur afin de le rendre inaccessible. Google explique que ce type d'opérations est relativement facile à mettre en place et peu coûteux.

DDoS

Pour prévenir les organisations n'ayant pas les moyens de parer ce type d'attaques, la firme de Mountain View lance alors le Project Shield (« bouclier » en français). Ce dernier repose sur le service Page Speed, initialement présenté sous la forme d'un module pour le serveur Apache en novembre 2010 puis proposé en tant que DNS pour rediriger le trafic vers les serveurs de Google. Il en résulterait un gain de performances aux alentours de 50%.

Avec Project Shield, le trafic des sites Internet passera donc via l'infrastructure de Google, et ceux-ci bénéficieront alors d'un même niveau de protection. Pour tester ce dispositif, le géant de la recherche propose aux sociétés intéressées de remplir un formulaire afin de recevoir une invitation. Google cherche tout d'abord des testeurs « de confiance », c'est-à-dire des agences de presse ou des organisations politiques ou impliquées dans le droit des hommes.

Ces participants seront invités à configurer Page Speed ainsi que leur domaine. **Pour l'heure le dispositif est gratuit mais Google n'exclut pas de le monétiser à l'avenir**.

Retrouvez davantage d'informations sur cette page

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

Références :

http://www.clubic.com/internet/google/actualite-594612-project-shield-google-souhaite-lutter-attaques-ddos.html

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

Augmenter la sécurité des transactions sur Internet, le défi de la nouvelle technologie IST Model

	**Augmenter la sécurité des transactions sur Internet, le défi de la nouvelle technologie IST Model**

IST Model (Intrinsic Security Technology Model) est une technologie qui permet d'augmenter considérablement la sécurité des transactions électroniques sur internet. Née comme une puissante méthode d'identification des utilisateurs sur des réseaux non protégés, elle a été spécialement conçue pour être robuste à de nombreuses attaques informatiques telles que le phishing, pharming, arp poisoning, etc.
Cette technologie, déjà brevetée en Italie, vient d'achever avec succès le processus d'enregistrement du brevet de l'US Patent Office, le Bureau de Brevets des Etats-Unis.

En utilisant une approche différente et complémentaire par rapport au chiffrement, IST Model garantit une sécurité intrinsèque au cours d'une transaction électronique entre deux ou plusieurs partenaires, quelle que soit la tâche, et pour toute sa durée. Conçu comme un protocole ouvert, IST Model peut être implémenté sur tous les standards et protocoles de communication existants. Le moteur interne de cette technologie assure des algorithmes rapides, pouvant être mis en oeuvre même sur de petits dispositifs.
Un premier champ d'application possible pour cette technologie est le domaine du commerce électronique sur internet, mais de manière plus générale, il est possible d'utiliser IST Model dans tous les domaines d'activité où il est nécessaire d'identifier les partenaires d'une transaction électronique, par exemple pour un nouveau passeport électronique, un système électronique d'ouverture/fermeture de portes/voitures/coffre-fort, un vaisseau spatial qui reçoit des commandes du centre de contrôle sur Terre etc.
L'utilisation idéale de cette technologie est le smartphone en réseau, mais tout appareil électronique peut en être équipé.

Source :
http://newsspazio.blogspot.it/2014/03/un-nuovo-brevetto-usa-per-uninvenzione.html

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

Références :
http://www.bulletins-electroniques.com/actualites/76521.htm

Attaque informatique contre les fournisseurs d'énergie –

Dragonfly lance la cyberguerre froide…

Attaque informatique contre les fournisseurs d'énergie – Dragonfly lance la cyberguerre froide…
Le scénario du pire. Ou presque. Un groupe de hackers, baptisé Dragonfly, est parvenu à corrompre certains systèmes de contrôle des opérateurs d'énergie. Notamment en France. Les pirates avaient alors la possibilité de saboter la distribution d'énergie de certains pays.

Une victime des pirates informatique guidée en ligne pour payer la rançon

Une victime des pirates informatique guidée en ligne pour payer la rançon

Témoignage d'un client :
L'informaticien Robert Hyppolite a dû payer une rançon aux pirates de SynoLocker… qui lui ont offert une assistance en ligne.

«Imaginez une entreprise de conseil juridique qui perd tous ses documents: mémoires, pièces, scans.
C'est un énorme coup dur. Sans les pièces, il y a de quoi perdre un procès!» Robert Hyppolite travaille depuis trente ans dans l'informatique à Genève. Il a notamment fondé l'entreprise Infologo, rachetée par VTX. Depuis 2007, il propose à ses clients le produit Synology, un système d'exploitation pour les serveurs de stockage en réseau. Des pirates ont élaboré un virus baptisé «SynoLocker TM» (sic) qui exploite la faille de sécurité de certaines anciennes versions du système. La police genevoise prend connaissance de cinq à dix nouveaux cas chaque semaine. Sur les trente clients de Robert Hyppolite équipés de Synology, deux ont été infectés et leurs sauvegardes ont également été atteintes. L'informaticien a dû payer une rançon en urgence dans la nuit de mardi à mercredi: l'un des deux clients touchés demandait une solution immédiate.

«La première difficulté était qu'il fallait payer en bitcoins, explique-il. On ne peut pas en acheter du jour au lendemain: il faut ouvrir un compte, donner son identité, faire un virement… Pour gagner du temps, je suis allé au distributeur de bitcoins des Pâquis (lire: Le bitcoin gagne l'économie réelle à Genève). La somme exigée par les pirates est de 0,6 bitcoin, ce qui correspondait à 650 francs, mais le cours est très fluctuant et dépend des pays et des plates-formes. »

Contre paiement de la rançon, un code permet normalement de décrypter les données et de retrouver ses fichiers. Sauf que l'aventure ne s'est pas arrêtée là. «Le virus chiffre les fichiers avec une clé réputée inviolable (2048 bits), ce qui les rend inutilisable. Ils restent normalement visibles avec leur nom correct. Mais le système de cette entreprise n'a pas réagi comme les autres et a été entièrement corrompu.» Conséquence: il a fallu réinstaller le système d'exploitation Synology, puis… réinstaller le virus, pour pouvoir permettre le décryptage des fichiers au moyen du code.

Les pirates répondent en ligne
Comment installer soi-même un virus? L'informaticien fait une curieuse découverte: «Sur le site Internet des ravisseurs, on trouve un onglet «support»… avec un chat en direct. Ils m'ont répondu très poliment: «Cher Monsieur, nous avons pris note de votre problème…» J'avais l'impression de parler à l'assistance en ligne d'une compagnie officielle! Une heure après, ils m'envoyaient une marche à suivre: il fallait entrer manuellement des instructions en ligne de commande. Tout a fonctionné sauf la dernière opération. A nouveau, le support informatique des pirates m'a répondu: leur dernière instruction contenait une erreur. J'ai ensuite pu entrer le code et tout est revenu à la normale.»
Une sauvegarde sur un serveur ou un disque dur séparé aurait permis de récupérer les données sans être rançonné. «Je préconise toujours cette mesure, mais dès qu'il faut s'équiper, il n'y a plus personne, regrette l'informaticien. Les clients pensent qu'on veut leur vendre des produits ou services inutiles, sauf ceux qui ont déjà vécu un sinistre…»
L'entreprise Synology souffrira-t-elle du virus SynoLocker? «Oui, mais ce sera vite oublié, estime Robert Hyppolite. J'ai vécu la mise à jour de l'antivirus Avast qui rendait les machines inutilisables… Pendant une année, leurs ventes ont baissé. Depuis, ils se sont rattrapés.» L'informaticien devra encore résoudre le problème du second client pris en otage. L'occasion, peut-être, d'une nouvelle discussion avec des ravisseurs informatiques très organisés et qui semblent prendre soin de leurs «clients».
Note: en cas d'infection avec SynoLocker, la police recommande de ne pas s'acquitter de la rançon et de réinitialiser les disques durs. Dans une note publiée ce jeudi, la Confédération émet des recommandations contre SynoLocker et conseille un outil de décryptage gratuit contre un virus au fonctionnement semblable, Cryptolocker.
Lire la suite…
Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Références :
http://www.tdg.ch/high-tech/hard-software/Des-pirates-informatiques-guident-leurs-victimes-en-ligne/story/19256356

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

---

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

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.

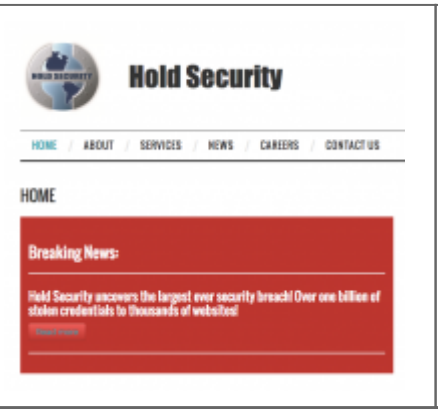
Mais ce marché est encore très balbutiant, et notamment en matière de protection de données personnelles. Symantec vient de publier, il y a quelques jours, un rapport d'analyse qui évalue le niveau de sécurité de tous ces engins. Résultat: la plupart des applications révèlent des failles flagrantes permettant 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

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

Objets connectés : HP s'inquiète des failles de sécurité

Le danger pourrait aussi bien venir des Objets connectés

Au total, 10 objets ont été passés au crible par les services de Fortify, la division d'HP dédiée à la cybersecurité.

Lesquels ? On ne sait pas exactement, l'entreprise se contente de préciser qu'ils sont de tous types (webcam, domotique, hub etc…) et font partie des objets les plus vendus. Mais dans un souci diplomatique, le rapport semble préférer la discrétion, afin peut être de laisser le temps aux constructeurs de corriger ces vulnérabilités.

Le problème n'est pas anodin puisque comme le relève l'étude, 9 de ces 10 objets stockent ou utilisent des données personnelles de l'utilisateur. Parmi ceux la, 7 d'entre eux ne chiffrent pas les données qu'ils transfèrent vers le réseau, et 6 objets proposent des interfaces web vulnérables à des attaques de cross-site scripting ainsi qu'à d'autres types d'attaques plus simples basées sur le social engineering. Un exemple criant : 8 objets sur 10 ne posent aucune restriction sur le choix du mot de passe, permettant ainsi à l'utilisateur de choisir un mot de passe du type « 123456 »

L'internet des objets : un gruyère ?

En moyenne, les objets étudiés par Fortify présentaient chacun 25 failles de sécurité, allant des plus obscures à d'autres beaucoup plus connues telles que des vulnérabilités ayant

trait à Heartbleed. La générosité gratuite n'étant pas vraiment de ce monde, cette initiative n'est pas innocente de la part d'HP qui en profite pour faire la promotion de son activité de sécurité Fortify et redirige tout au long du rapport le lecteur vers son site Owasp, un site open source dédié à la sécurité des objets connectés.

Peu de chiffres, pas de noms, HP ne se mouille donc pas trop mais on peut rappeler que l'objet du rapport n'en reste pas moins pertinent : la sécurité des objets connectés est un enjeu de taille que les constructeurs ne peuvent se permettre de traiter à la légère.

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

Références :

http://www.zdnet.fr/actualites/objets-connectes-hp-s-inquiete-des-failles-de-securite-39804463.htm