Qui protège le mieux ses données personnelles ? | Le Net Expert Informatique

Qui protège le mieux ses données personnelles ?

La récente affaire Ashley Madison a démontré une nouvelle fois les nombreuses failles de nos systèmes informatiques et la négligence des utilisateurs à confier leurs données personnelles à tous types de sites. Newmanity au travers de son étude a voulu étudier le comportement des français face à cette polémique et les résultats s'avèrent des plus surprenants ! Homme, femme, qui a le plus peur pour ses données personnelles ?

L'échantillon
Enquête réalisée auprès d'un échantillon de Français recrutés par téléphone puis interrogés par Internet les 31 août et 1er septembre 2015. Echantillon de 1183 personnes, représentatif de la population française âgée de 18 ans et plus. La représentativité de l'échantillon est assurée par la méthode des quotas appliqués aux variables suivantes : sexe, âge, profession du chef de famille et profession de l'interviewé après stratification par région et catégorie d'agglomération.

Ce qu'il faut retenir de l'étude
La majorité des actifs Français déclarent faire plus attention à leurs données numériques dans le cadre personnel, plutôt que dans le cadre professionnel > Les hommes déclarent protéger davantage leurs données que les femmes.
Les Français expriment plus de méfiance à l'égard des appareils mobiles (Smartphones, Tablettes) que des ordinateurs > La déconnexion des comptes est une habitude peu fréquente pour les Français

Les hommes plus méfiants que les femmes
Selon les actifs français, les données numériques les plus préoccupantes sont celles issues d'une utilisation personnelle : 69% d'entre eux déclarent y être plus vigilants contre 28% dans le cadre professionnel. Et ce sont les femmes qui sont les moins regardantes (34%) sur la protection de leurs données dans le cadre personnelles contre 73% des hommes qui scrutent méticuleusement la moindre trace sur la toile !
Paradoxalement, les manipulations de base permettant de limiter les problèmes de sécurité en matière de données numériques sont encore assez peu utilisées :
Se déconnecter d'une boîte mail : Moins de 6 actifs sur 10 se déconnectent systématiquement de leur boite mail personnelle lorsqu'ils la consultent depuis le bureau, et cette proportion tombe à 48% lorsque l'utilisation se fait sur ordinateur personnel.
Suppression de l'historique de navigation : Que ce soit sur leur ordinateur personnel ou professionnel, moins de 4 Français sur 10 suppriment leurs données de navigation tous les jours ou au moins une fois par semaine. D'ailleurs, près de 3 actifs sur 10 ne suppriment jamais leur historique de navigation sur leur ordinateur professionnel. Des gestes pourtant simples qui permettraient une meilleures protection de la vie privée de tout un chacun.

Les appareils mobiles suscitent plus de méfiance
Près de la moitié des Français détenteurs d'équipements numériques n'en n'ont pas confiance, signe d'une certaine méfiance alors que les affaires de piratage de données personnelles (Orange, Ashley Madison…) font régulièrement la Une de l'actualité. Dans le détail, que ce soit à l'égard des ordinateurs personnels ou professionnels, les cadres et les femmes qui semblent être les plus confiants. A l'inverse, les hommes et les CSP 'employés' et 'ouvriers' sont nettement plus réservés.
Il est à noter que cette méfiance devient défiance lorsqu'il s'agit de tablettes ou de smartphones. Ces équipements mobiles sont marqués par le peu de confiance qui leur est accordé en matière de sécurité de données transmises : Seulement 37% des Français détenteurs d'une tablette numérique lui font confiance et à peine plus d'un tiers (34%), en ce qui concerne les possesseurs de smartphones.

Source : http://www.economiematin.fr/news-internet-securite-utilisateurs-protection-donnees
Par Stéphane Petibon

Les centrales nucléaires vulnérables aux cyberattaques | Le Net Expert Informatique

	Les centrales nucléaires vulnérables aux cyberattaques

Financement insuffisant, manque de formation ou encore mauvaise culture sur le sujet… Les centrales nucléaires sont particulièrement vulnérables aux cyberattaques selon un rapport du groupe de réflexion britannique Chatham House publié ce lundi.

L'industrie nucléaire, en retard dans la prévention du risque technologique, constitue une cible particulièrement vulnérable aux cyberattaques, elles-mêmes de plus en plus répandues et sophistiquées, selon un rapport du Think Tank Chatham House publié ce lundi.

Les acteurs de l'industrie nucléaire «commencent, mais ont du mal, à lutter contre cette nouvelle menace insidieuse», analyse le groupe de réflexion britannique dans une étude reposant sur 18 mois d'enquête. L'institut estime que les centrales nucléaires «manquent de préparation pour affronter une urgence en matière de cybersécurité, dans un incident de grande ampleur, et auraient du mal coordonner une réponse adéquate». En cause : un financement insuffisant de cette prévention, un manque de formation, de normes réglementaires et de culture de la cybersécurité, l'utilisation croissante du numérique dans les systèmes d'exploitation des centrales et le recours à des logiciels de série peu onéreux mais plus vulnérables au piratage, observe le rapport.

Les centrales de plus en plus connectés

Chatham House dénonce le «mythe répandu» selon lequel les centrales nucléaires seraient protégées parce qu'elles ne seraient pas connectées à internet. Dans les faits, de nombreuses installations ont progressivement mis en place une forme de connectivité et leurs systèmes informatiques peuvent être piratés par des moyens parfois très simples.

Ainsi, le virus Stuxnet, qui avait perturbé le fonctionnement de sites nucléaires iraniens en 2010, avait été implanté au moyen d'un périphérique USB. Selon Chatham House, cette attaque est devenue une référence dans le monde des cybercriminels et leur a permis d'améliorer leur technique. «Une fois que l'existence de Stuxnet a été connue, explique le rapport, les pirates à travers le monde se sont inspirés de son fonctionnement et ont incorporé certaines de ses fonctionnalités à leurs propres logiciels à visée malveillante».

Source :
http://www.leparisien.fr/high-tech/les-centrales-nucleaires-vulnerables-aux-cyberattaques-05-10-2015-5157897.php
Illustration. De nombreuses centrales ont progressivement mis en place une forme de connectivité et leurs systèmes informatiques peuvent être piratés par des moyens parfois très simples. (AFP/SEBASTIEN BOZON)

Les Cnil européennes peuvent-elles condamner un éditeur de site étranger ? | Le Net Expert Informatique

	Les Cnil européennes peuvent-elles condamner un éditeur de site étranger ?

Le responsable du traitement de données personnelles d'un pays de l'UE peut se voir appliquer le droit d'un autre Etat membre. La Cour de Justice de l'Union européenne vient de statuer dans une affaire opposant un site slovaque à la Cnil hongroise, considérant que les régulateurs sont compétents pour condamner un éditeur de site étranger si celui-ci exerce sur le sol national.

Un site Web, même immatriculé à l'étranger (en l'occurrence dans un autre État membre de l'UE), peut se voir appliquer le droit d'un État membre relatif à la protection des données personnelles, pour peu que l'éditeur de ce site exerce « au moyen d'une installation stable sur le territoire de cet État membre, une activité effective et réelle, même minime, dans le cadre de laquelle ce traitement est effectué ». C'est en substance l'arrêt qu'a publié hier la CJUE.

L'affaire opposait un site d'annonces immobilières slovaque et la Cnil hongroise. La société slovaque, refusant de supprimer gratuitement les données personnelles de clients hongrois, avait été condamnée à une amende par la Nemzeti Adatvédelmi és Információszabadság Hatóság (l'équivalent hongrois de notre Cnil). L'éditeur du site a par la suite contesté la compétence territoriale de la NAIH : l'affaire termina devant la Cour suprême de Hongrie, qui a soumis la question à la CJUE.

Compétence territoriale précisée

Laquelle vient de rendre un arrêt on ne peut plus clair sur la compétence territoriale des Cnils européennes. Elle considère que le droit européen « permet l'application de la législation relative à la protection des données à caractère personnel d'un État membre autre que celui dans lequel le responsable du traitement de ces données est immatriculé ». Indépendamment de la nationalité des victimes, à la seule condition que « le responsable du traitement des données » exerce une activité dans l'État membre concerné.

En outre, précisent les juges, si l'autorité de contrôle d'un État membre estime que ce n'est pas le droit national qui doit s'appliquer, mais celui d'un autre État membre, « elle ne saurait infliger de sanctions sur la base du droit de cet État membre au responsable du traitement de ces données qui n'est pas établi sur ce territoire ». Toutefois, elle peut saisir la Cnil du second État membre. Il revient dès lors à la juridiction nationale de déterminer si la société « étrangère » exerce sur son sol, « au moyen d'une installation stable sur le territoire de cet État membre, une activité effective et réelle, même minime ».

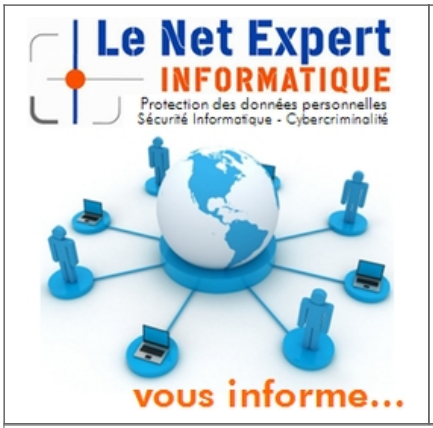
Evidemment, cet arrêt ne concerne que les éditeurs responsables du traitement de données à caractère personnel établis sur le territoire de l'UE. Mais, considérant qu'un certain nombre de géants du Web disposent de sièges en Europe, la jurisprudence pourrait bien être utilisée contre eux, ce qui suscitera sans aucun doute de nouveaux débats juridiques et, qui sait, une nouvelle jurisprudence.

Denis JACOPINI est Expert Judiciaire en Informatique, consultant, formateur et chargé de cours.
Nos domaines de compétence :
• **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
• **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
• **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.
Contactez-nous

Source :
http://www.linformaticien.com/actualites/id/38047/les-cnil-europeennes-peuvent-elles-condamner-un-editeur-de-site-etranger.aspx
par Guillaume Périssat

Le site Web des universités de Montpellier piraté par un

groupe pro-palestinien | Le Net Expert Informatique



Le site Web des universités de Montpellier piraté par un groupe pro-palestinien

L'attaque s'est déroulée pendant quelques heures ce samedi. Des hackers se revendiquant de l'opération « Save Gaza » ont pris en main le site des Universités de Montpellier comme l'a repéré le site H24.Dans un message écrit à la fois en anglais et en français, ils dénoncent l'aide américaine au gouvernement d'Israël, accusé de « contrôler le monde, l'armée, l'économie et les cerveaux ».

« Save Gaza »

Dans un long paragraphe, les auteurs du piratage accusent les deux « gouvernements monsters » d'être « à l'origine de l'hypnose dont souffre la race humaine ». Le texte se conclut sur une adresse aux français: « Si être un vrai « Français », comme vous le dites, c'est d'être soumis, alors personne n'a à le cacher, nous ne sommes pas français, et bien heureux et vous nous considériez différents de vous ».

Le groupe affiche en conclusion son objectif: « The Intruders Will Transform The World », traduit en français par « Les Intruders changeront le monde ».

Source :
http://www.bfmtv.com/societe/le-site-web-des-universites-de-montpellier-pirate-par-un-groupe-pro-palestinien-919637.html

Données personnelles : mais à quoi sert la CNIL ? – Cash Investigation ce mardi 6 octobre 2015 | Le Net Expert Informatique

Données personnelles : mais à quoi sert la CNIL ? – mardi 6 octobre 2015

Certaines associations caritatives vendent en toute illégalité leurs fichiers de donateurs à La Poste. Face à Elise Lucet, la présidente de la CNIL ne semble pas au courant et se déclare « surprise ». Un extrait de « Cash Investigation » diffusé sur France 2 le mardi 6 octobre à 20h55. Lire la suite….
Ci-dessous, le rapport d'activité 2014 de la CNIL dont il est fait mention dans le reportage (Merci à Eric EGÉA) :
http://www.cnil.fr/fileadmin/documents/La_CNIL/publications/CNIL-35e_rapport_annuel_2014.pdf.pdf

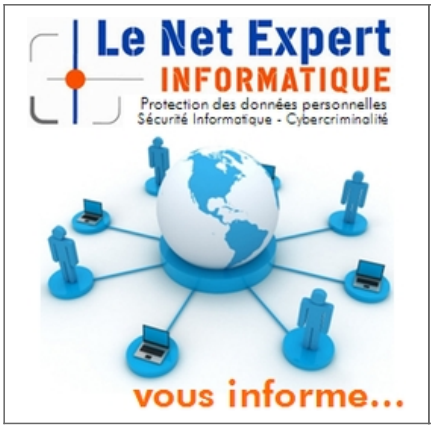
---

Même si remplir un formulaire de déclaration à la CNIL est gratuit et enfantin, il vous engage cependant, par la signature que vous apposez, à respecter scrupuleusement la loi Informatique et Libertés. Cette démarche doit d'abord commencer par un Audit de l'ensemble de vos systèmes de traitements de données. Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.
Besoin d'informations complémentaires ?
Contactez-nous
Denis JACOPINI
Tel : 06 19 71 79 12
formateur n°93 84 03041 84

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : http://www.francetvinfo.fr/internet/cash-investigation-donnees-personnelles-mais-a-quoi-sert-la-cnil_1109973.html

Il est nécessaire d’éduquer et de former les élèves à la cybersécurité ! | Le Net Expert Informatique



Il est nécessaire d’éduquer et de former les élèves à la cybersécurité !

Il est désormais du devoir des institutions et de l'Éducation nationale d'encadrer les plus jeunes afin de les aider à devenir des citoyens numériquement responsables.

À l'occasion du mois européen de la cybersécurité, qui se tiendra en octobre, il est primordial de penser à faire évoluer les pratiques d'Internet des jeunes Français et de leur en inculquer les bases d'un usage sécurisé. C'est un fait, aujourd'hui les enfants de 9 à 16 ans utilisent quasiment tous Internet (93 %), et ce malgré les risques qu'il comporte (1).

Avec l'arrivée des objets connectés (smartphones, tablettes, accessoires, etc.) pouvant s'avérer être, pour certains individus parmi les plus jeunes, une réelle addiction, les cyber-risques ne cessent de croître. La formation de nos chères têtes blondes à devenir des utilisateurs responsables d'Internet et à être au fait de ses enjeux de sécurité ne doit pas seulement se limiter à celles des parents, les institutions et l'Éducation nationale doivent également y participer.

L'importance de différents niveaux d'apprentissage de la cybersécurité

Les écoles sont comme une seconde maison pour les enfants, où les enseignants viennent complémenter les parents en termes de connaissances, d'enseignement et de discipline. Voilà pourquoi l'École apparaît tout naturellement comme une bonne option pour dispenser une véritable éducation en matière de cybersécurité.

Aujourd'hui, une telle contribution est vitale dans la préparation des enfants au monde virtuel. Des sujets tels que la cyber-civilité, la cyber-image, la cyber-hygiène et la cybersécurité pourraient, par exemple, être mieux appréhendés et expliqués dans une salle de classe. Or, à ce jour, la plupart des écoles n'offrent seulement qu'un bref aperçu de ce qu'est la cybersécurité.

Bien entendu, l'enseignement de la sécurité du « cyber-life » se doit de différer en fonction de l'âge de l'élève, mais quelques règles de base sont communes à tous afin de mieux les prémunir dans le cadre de leurs interactions tant dans leur vie sociale que digitale !

Pour les plus jeunes, c'est au moment où l'intérêt des enfants pour l'univers digital est minime qu'il faut les sensibiliser à la cybersécurité. Des règles et enseignements simples pourraient être inculqués comme leur apprendre à demander l'autorisation à leurs parents avant d'utiliser un appareil, être sensibilisé à la dangerosité de communiquer avec des personnes inconnues sur le Net ou encore la nécessité de prévenir ses parents en cas d'échange bizarre sur le Net, etc.

Quant aux préadolescents, la cyberéducation doit intervenir au moment où ils commencent à jouer en ligne, à regarder des vidéos sur le Net, à créer leur propre compte sur les réseaux sociaux, etc. Afin qu'ils puissent surfer en toute sécurité, il est primordial de leur enseigner quelques bases de sécurité par exemple l'importance de créer un mot de passe efficace et sécurisé, la manière de reconnaître un site/une application sûr(e), les risques de vol existant en ligne, les dangers du téléchargement et du partage de contenu personnel sur le Web, etc.

Vient ensuite la période de l'adolescence, où les jeunes aiment se retrouver et échanger sur des sites Internet communautaires au sein desquels le risque de partage d'informations personnelles et d'interaction avec des inconnus est omniprésent. L'adolescence se présente également comme une période au cours de laquelle il faudrait renforcer l'apprentissage des adolescents en termes de pratiques éthiques, de reflet d'image, de sûreté et de sécurité des outils, etc., l'idée étant de faire des adolescents des citoyens numériques responsables et conscients de dangers que représente la Toile (addiction, hacking, phishing, cyberharcèlement, etc.).

Espérons que les actions menées par les associations et les professionnels concernés à l'occasion du mois européen de la cybersécurité s'imposent comme un détonateur dans la prise de conscience des politiques et de l'Éducation nationale quant à la nécessité de l'apprentissage numérique des plus jeunes afin de mieux protéger et sécuriser les individus et le monde de demain.

Denis JACOPINI est Expert Judiciaire en Informatique, consultant, formateur et chargé de cours.

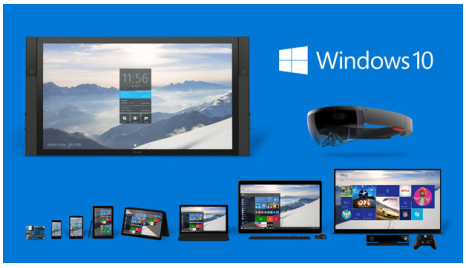
Nos domaines de compétence :

- **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
- **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
- **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.

Contactez-nous

Source :
http://www.lesechos.fr/idees-debats/cercle/cercle-140152-il-est-necessaire-deduquer-et-de-former-les-eleves-a-la-cybersecurite-1160311.php?XMmKySpwheCXjjJG.99

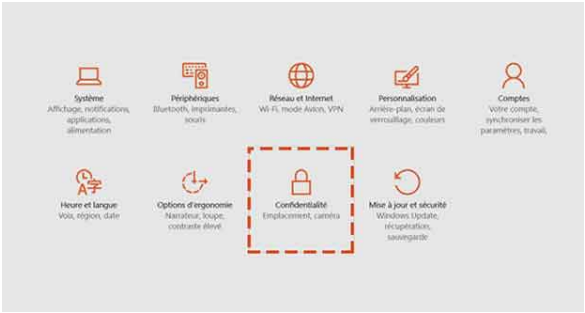
Windows 10 et sa vie privée, la CNIL met en garde et propose une fiche pratique | Le Net Expert Informatique



Windows 10 et sa vie privée, la CNIL met en garde et propose une fiche pratique

Windows 10 est disponible gratuitement pour les PC sous Windows 7 ou Windows 8.1. Il propose des changements face à ses prédécesseurs dont certains touchent à la surveillance, l'analyse et la collecte de données personnelles concernant ses utilisateurs. La CNIL met en garde et propose un tutoriel pour se protéger des yeux indiscrets de la firme.

En France, la CNIL a rapidement réagi devant les nombreux systèmes de surveillance et de collecte de données accompagnant Windows 10. Dans un dossier mis en ligne quelques jours seulement après le lancement de l'OS, elle propose « quelques réglages de confidentialité qui permettent de limiter la communication de vos informations à l'éditeur et à ses partenaires ».



Windows 10, des fuites dans Cortana, Microsoft Edge ou encore la synchronisation

Ils se concentrent sur trois thèmes, Cortana avec un paramétrage de la » vie privée « , la synchronisation des comptes sur les autres appareils utilisés et le navigateur Microsoft Edge.

Elle recommande ainsi de désactiver la géo-localisation, d'empêcher la collectes de données liées à l'Appareil photo, le Microphone, les Informations de Compte, des Contacts, du Calendrier, de la Messagerie, des communications Radio ou encore d'agir sur la fonctionnalité » apprendre à me connaître » pour la dictée vocale. Au sujet du nouveau navigateur, Microsoft Edge, il est recommandé de désactiver l'option » Utiliser la prédiction de page pour accélérer la navigation, et améliorer le mode lecture ainsi que mon expérience globale » puisque celle-ci requiert d'envoyer votre historique de navigation tandis l'obtention de suggestions de recherche demande qu'une grande partie des informations que vous saisissez dans la barre de navigation soit envoyée au moteur de recherche Bing. Il est donc recommandé de désactiver « Afficher les suggestions de recherche à mesure que je tape « .

Vous trouverez ici, un pas à pas complet pour reprendre la main sur vos données personnelles : Régler les paramètres vie privée de Windows 10

Denis JACOPINI est Expert Judiciaire en Informatique, consultant, formateur et chargé de cours.
Nos domaines de compétence :
• **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
• **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
• **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.
Contactez-nous

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source :
http://www.ginjfo.com/actualites/logiciels/windows-10/windows-10-et-sa-vie-privee-la-cnil-met-en-garde-et-une-fiche-pratique-20150928

Panne de Facebook ? La carte des dysfonctionnements | Le Net Expert Informatique

Panne de Facebook ? La carte des dysfonctionnements

Facebook est un réseau social en ligne sur internet. Il permet de publier des informations (photos, liens, textes) en contrôlant la visibilité.
Il est aujourd'hui le réseau social le plus populaire. Fondé en 2004 par Mark Zuckerberg, le site est devenu incontournable au fil des années.

Les statistiques d'usages sont ahurissantes :
Utilisateurs actifs mensuels (MAU, juillet 2015) : 1,49 milliard
En Europe : 3011 millions
En Amérique du Nord : 213 millions
En Asie : 496 millions
Dans le reste du monde : 471 millions
En France : 30 millions d'utilisateurs

Utilisateurs actifs mensuels sur mobile : 1,314 milliard.
En France : 24 millions d'utilisateurs
Utilisateurs actifs mensuels uniquement sur mobile : 655 millions.
Utilisateurs actifs quotidiens (DAU) : 968 millions

Ainsi, une panne de Facebook de quelques minutes, ou plus comme celles passées en Octobre 2015, impactera des utilisateurs de toute la planète.
Lien vers la carte des pannes de Facebook

Denis JACOPINI est Expert Judiciaire en Informatique, consultant, formateur et chargé de cours.
Nos domaines de compétence :
• **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
• **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
• **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.
Contactez-nous

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : https://touteslespannes.fr/statut/facebook/carte/

Découverte d’un malware sous Linux derrière un important botnet | Le Net Expert Informatique

Découverte d’un malware sous Linux derrière un important botnet

Réputé plus sûr que Windows, Linux connaît aussi son lot d’attaques, et en connaîtra de plus en plus avec l’augmentation des objets connectés reposant sur une distribution Linux. En témoigne un nouveau malware découvert principalement en Asie, qui forme un botnet capable d’orchestrer des attaques DDOS très puissantes, jusqu’à plus de 150 Gbps.

La firme Akamai a révélé lundi la découverte d’un botnet qui serait capable d’organiser une attaque DDoS de plus de 150 Gbps, formé grâce à un malware qui cible les ordinateurs et serveurs sous Linux. Baptisé XOR DDoS, l’armée de zombies rassemblés par des chevaux de Troie se compose également de nombreux appareils connectés dont la couche logicielle repose souvent sur des systèmes Linux non mis à jour, soit que le service après-vente n’est pas assuré, soit que les utilisateurs n’aient pas le réflexe de mettre à jour le firmware d’un appareil qui semble fonctionner correctement.

Selon Akamai, le malware d’origine asiatique se répandrait grâce aux services SSH d’appareils mal sécurisés tels que de routeurs, qui peuvent être attaqués par force brute (tenter des milliers de mots de passe jusqu’à tomber sur le bon). Chaque accès gagné sur une machine permet de gagner un nouveau relais vers de nouveaux serveurs, et ainsi de suite.

Le botnet XOR DDoS aurait déjà été utilisé de très nombreuses fois (une vingtaine d’attaques par jour dont 90 % vers l’Asie), avec des degrés divers de puissance, allant de flots de données de 2 Gbps à plus de 150 Gbps. Les cibles prioritaires seraient le secteur du jeu d’argent, suivi par les institutions éducatives. Une orientation qui peut être le fait des créateurs du botnet, ou des clients qui louent ses services pour attaquer une URL ou une adresse IP en payant à l’heure et à la puissance d’attaque voulue.

Denis JACOPINI est Expert Judiciaire en Informatique, consultant, formateur et chargé de cours.
Nos domaines de compétence :
• **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
• **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
• **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.
Contactez-nous

Source :
http://www.numerama.com/magazine/34342-decouverte-d-un-malware-sous-linux-derriere-un-important-botnet.html
par Guillaume Champeau

Quinze millions de clients T-Mobile victimes d’un piratage | Le Net Expert Informatique

Quinze millions de clients T-Mobile victimes d’un piratage

Des cyberpirates ont dérobés les données personnelles de 15 millions d’abonnés de l’opérateur de téléphonie T-Mobile. Le piratage a ciblé son prestataire Experian, spécialisé dans la relation client et l’analyse du risque de crédit. Le butin comprend notamment des noms, adresses, dates de naissance ainsi que des numéros de sécurité sociale.

L’opérateur T-Mobile et Experian, son prestataire chargé de vérifier la solvabilité ont annoncé qu’un piratage massif avait permis à des cybercriminels de dérober les données personnelles de quelques 15 millions de clients. Évoquant une “acquisition d’information non autorisée” depuis l’un de ses serveurs, Experian a révélé qu’il s’agit de données sensibles telles que des noms, adresses, dates de naissance, numéros de sécurité sociale, numéros de passeport ou de permis de conduire ainsi que des informations relatives aux évaluations des emprunteurs. L’intrusion s’est produite entre le 1er et le 16 septembre.

Dans un message adressé à ses clients, John Legere, le P-dg de T-Mobile, assure que les données bancaires n’ont pas été exposées. Il a également annoncé que tous les clients concernés avaient droit à un abonnement de deux ans à un service de surveillance et protection en cas d’usurpation d’identité et de fraude.

Denis JACOPINI est Expert Judiciaire en Informatique, consultant, formateur et chargé de cours.
Nos domaines de compétence :
• **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
• **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
• **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.
Contactez-nous

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source :
http://www.zdnet.fr/actualites/quinze-millions-de-clients-t-mobile-victimes-d-un-piratage-39825840.htm