Compter une population seulement avec le Wi-Fi | Le Net Expert Informatique

Compter une population seulement avec le Wi-Fi

Plus besoin de se baser sur le nombre de smartphones connectés dans une certaine zone pour compter des groupes de personnes. La découverte de chercheurs de Santa Barbara se base uniquement sur le signal Wi-Fi.

L'idée est assez simple sur le papier : analyser les variations des ondes Wi-Fi d'une certaine zone pour compter les personnes présentes. Partant du principe que chacun altère légèrement les ondes par sa présence, les chercheurs de l'université de Californie Santa Barbara ont mis au point un modèle mathématique pour estimer le nombre d'individus dans une zone donnée. Le professeur d'ingénierie informatique Yasamin Mostofi et son équipe ont disposé deux spots Wi-Fi à deux extrémités d'une aire de 70 mètres carrés. Grâce à l'analyse de leurs ondes, les ingénieurs sont ensuite parvenus à estimer le nombre de personnes présentes dans la zone en temps réel. Et ce même si les individus étaient en mouvement.

Un outil pour la sécurité ?
En fait, la découverte répond à un besoin : celui de connaître l'étendu d'un groupe de personnes dans une manifestation ou dans un lieu public. La sécurité de certains événements pourrait en être accrue, selon les chercheurs, grâce à la notion de temps réel qu'apporte l'invention, même si les méthodes de comptage par les données télécoms se rapprochent déjà de ces objectifs. D'autant que le Wi-Fi ne peut s'étendre sur une surface aussi large que celles qui voient défiler des manifestants. L'aspect sécuritaire ne concernerait donc que les petits événements. Son seul avantage étant la prise en compte des individus sans smartphone.

Le Wi-FI rendra-t-il les bâtiments plus verts et plus intelligents ?
Vers des bâtiments plus intelligents
C'est en réalité dans un autre domaine que la découverte pourrait changer la donne. Les bâtiments intelligents seraient, en effet, à même de bénéficier d'une telle invention. Comme l'explique le professeur Mostofi dans le communiqué de l'université : « les stores intelligents pourraient se servir du dénombrement des utilisateurs du lieu pour mieux s'adapter par exemple ». Savoir précisément le nombre d'occupants d'un lieu ou le nombre de consommateurs dans un magasin permettrait à la fois une consommation d'énergie plus efficace mais également une nouvelle opportunité marketing. Les écrans publicitaires pourraient, en effet, se moduler selon la population présente pour ne citer que cet exemple.

Source : http://www.atelier.net/trends/articles/compter-une-population-seul-wi-fi_436129?utm_source=emv&utm_medium=mail&utm_campaign=lettre_toute_zone

---

Grosse menace sur les mots de passe contenus dans le

trousseau d’Apple | Le Net Expert Informatique

Grosse menace sur les mots de passe contenus dans le trousseau d’Apple

Peu importe que vous utilisiez iOS ou OS X, vos mots de passe sont en danger s’ils sont stockés dans le trousseau d’Apple.

Des chercheurs universitaires ont découvert une énorme faille de sécurité chez Apple, une faille suffisamment importante pour que la marque à la pomme n’ait pas encore réussi à la corrigé alors qu’elle a été signalée au mois d’octobre dernier. Pour causse, elle touche le mécanisme censé protéger les mots de passe : le trousseau.
L’idée du trousseau est simple : centraliser les identifiants et mots de passe pour que l’utilisateur n’ait pas à les ressaisir. Le problème, c’est que des chercheurs universitaires ont découvert toute une série de failles de sécurité.
Alors que le bac à sable est censé isoler les données pour qu’elles soient protégées, les chercheurs sont parvenus à percer le mécanisme.
Ils ont aussi créé un malware capable d’afficher tous les mots de passe de l’Apple’s Keychain, c’est-à-dire ceux stocker dans le trousseau, ce qui expose tous les identifiants utilisés par les applications tierces : Facebook, Twitter, iCloud, Gmail, etc.
« Nous sommes parvenus à pirater tout le service Keychain, où Apple stocke les mots de passe et les autres paramètres de ses applis ainsi que les sandbox containers’ dans OS X », explique Luyi Xing, responsable de cette recherche. « Nous avons découvert de nouvelles faiblesses dans les mécanismes de communication entre applis au sein d’OS X et d’iOS, qui pourraient être exploitées pour dérober des données confidentielles d’Evernote, Facebook et d’autres applis largement utilisées. »
Pour l’heure, le problème est énoncé, mais aucune solution n’est pour le moment encore disponible, le problème subsiste dans les versions actuelles d’iOS et d’OS X.

Source : http://www.linformatique.org/grosse-menace-sur-les-mots-de-passe-contenus-dans-le-trousseau-dapple/

Surveillance informatique par la NSA, C’est bien réel | Le Net Expert Informatique

Surveillance informatique par la NSA, C’est bien réel

Sur son blog, le cybercriminologue Jean-Paul Pinte a relayé un article du « Monde » racontant comment la NSA avait pu surveiller les organes de pouvoir de la France. « C'est bien réel, ce n'est pas de la science-fiction » assure-t-il.

Maître de conférences à l'université de Lille, spécialiste de la veille et de l'intelligence compétitive, il estime que la France devait savoir qu'elle était surveillée. Notamment « après l'expérience vécue par Angela Merkel en 2012 et 2013. Il ne peut donc y avoir de surprise, surtout vis-à-vis des États-Unis. Ceci dit, pour les pays qui subissent ce genre de surveillance, la principale chose qui les dérange c'est qu'ils ne peuvent pas faire la même chose. »
> Les moyens des États-Unis. Pour Jean-Paul Pinte la puissance acquise par les États-Unis dans le domaine du renseignement n'a pas d'égal. « Ils ont des logiciels comme Upstream qui vont capter les informations et analyser les contenus. Même involontairement, on peut être à la base d'une surveillance. Imaginez deux personnes qui communiquent par mail. L'une fait partie d'Alcatel ou EDF et si elle raconte qu'il y a du mouvement dans son entreprise, ce sera capté. » On a beaucoup parlé du programme Prisme, « cela prouve que les États-Unis pratiquent ce genre de surveillance depuis très longtemps ». Et les écoutes téléphoniques à la sauce américaine ont « plus de 50 ans ».
> L'espionnage dépasse les États. C'est pour cela que Jean-Paul Pinte ne croit absolument pas à la possibilité d'instaurer un code de bonne conduite. « Il faut être naïf pour penser s'en sortir comme ça. C'est une méconnaissance des entrailles du Web qui vont au-delà des États. Les États-Unis ont par ailleurs une certaine emprise sur Internet, ils peuvent fermer ou ouvrir des robinets et bloquer des pays, ils ont accès aux infrastructures, aux câbles et Prisme, Upstream… sont tellement puissants qu'ils sont presque devenus indolores. »
> Avoir toujours un coup d'avance. L'espionnage a toujours existé. « Aujourd'hui encore, des passagers montent dans l'Eurostar en première classe uniquement pour écouter les conversations de cadres ou de patrons du Cac40 et en faire des rapports. » Et le citoyen lambda n'est pas en reste. « Nous laissons énormément d'informations en chemin. C'est ce qu'on appelle aussi des métadonnées qui permettent de suivre nos pérégrinations, nos interactions sur les réseaux sociaux… » Pour l'espion, le tout est de ne pas se faire prendre. « Ce qui importe c'est que celui qu'on surveille ne soit pas conscient des écoutes. En cybercriminalité, c'est la même chose. C'est ce qui permet de se garantir d'avoir toujours un coup d'avance. »
Lire la suite….

Source : http://www.centre-presse.fr/article-397900-jean-paul-pinte-il-ne-peut-y-avoir-de-surprise-surtout-venant-des-etats-unis.html

---

Alerte partage ! Les

antivirus ESET victimes d’une faille de sécurité. Mettez vite à jour le moteur d’analyse | Le Net Expert Informatique

Alerte partage ! Les antivirus ESET victimes d’une faille de sécurité. Mettez vite à jour le moteur d’analyse

Un chercheur du Project Zero de Google a dévoilé une vulnérabilité critique affectant plusieurs produits et logiciels proposés par l'éditeur de sécurité ESET. La vulnerabilité est exploitable à distance et permet l'exécution de code malveillant sur la machine visée.

Les solutions de sécurité, comme n'importe quel autre logiciel, sont également exposées à des failles de sécurité qui peuvent permettre à un attaquant d'exécuter du code sur la machine. C'est d'ailleurs probablement l'une des raisons ayant poussé la NSA et le GCHQ à orienter leurs efforts de reverse engineering sur les produits de Kaspersky et d'autres éditeurs antivirus, afin de transformer ces obstacles en porte d'entrée au système de la cible.
La faille décrite par le chercheur Tavis Ormandy, qui avait déjà décelé une vulnérabilité affectant les logiciels de Sophos en 2012, porte plus précisément sur le moteur d'émulation utilisé par les produits de la société ESET. Cet outil est utilisé par l'antivirus pour faire tourner les instructions exécutées par la machine dans un environnement isolé, afin de détecter du code potentiellement malveillant pour l'utilisateur.

Même la version Linux est touchée
Malheureusement, celui-ci présente une vulnérabilité permettant à l'attaquant d'exécuter du code en disposant d'un haut niveau de privilège. Outre cet aspect, l'attaque est envisageable via un certain nombre de vecteurs : web, messagerie, ou périphérique de stockage, tous étant susceptibles d'être scannés par les programmes d'ESET à la recherche de code malveillant. La faille affecte les logiciels même dans leur configuration par défaut.
La vulnérabilité affecte de nombreux logiciels proposés par ESET : NOD32 Antivirus pour Windows, Cyber Security Pro pour OS X, NOD32 pour Linux Desktop, Endpoint Security et NOD32 Business Edition.
Un correctif est également proposé par ESET depuis le 22 juin, afin de corriger la faille de sécurité repérée par le chercheur. Le blog post détaille notamment divers moyen d'exploiter la faille, ainsi que des mesures d'atténuations : ainsi, couper l'analyse temps réel des outils d'ESET pourrait réduire le risque, en désactivant l'analyse automatique dans les outils proposés par la société slovaque. Mais la meilleure solution reste évidemment de patcher. Et vite.

Source : http://www.zdnet.fr/actualites/les-antivirus-eset-victimes-d-une-faille-de-securite-39821472.htm
Par Louis Adam

Les nouvelles cibles de la Cybercriminalité | Le Net Expert Informatique

	Les nouvelles cibles de la Cybercriminalité

Le piratage de TV5 Monde il y a quelques semaines est symptomatique du futur qui se prépare en matière de cybercriminalité. A mesure que les attaques deviennent plus sophistiquées, les pirates se rapprochent des infrastructures critiques. Ainsi, l'an passé, 43 % des entreprises œuvrant dans l'énergie (mines, compagnies du gaz, pétrolière) ont été la cible des cybercriminels au moins une fois dans l'année, rapporte une étude Symantec. Même constat chez Trend Micro, qui pointe que 47 % de l'industrie a fait l'objet d'une attaque, soit plus que les sites gouvernementaux. « Les attaques contre les infrastructures critiques deviennent une préoccupation grandissante de tous les gouvernements. En raison des conséquences potentielles des attaques, ces sites sont devenus très attractifs pour les pirates », dit l'étude de Trend Micro.

13,2 millions d'euros par an

Les dommages commis par les cybercriminels coûtent 13,2 millions d'euros par an à chaque entreprise de l'énergie, soit plus que dans n'importe quelle industrie, selon une étude réalisée par Poneman pour HP, relayée par Bloomberg. Pour se protéger, le secteur énergétique devrait porter son investissement en cybersécurité à 1,9 milliard de dollars d'ici à 2018, note ABI Research. Depuis quelques années, les exemples d'attaques contre des sites sensibles se multiplient. En France, le spécialiste du nucléaire Areva a avoué en 2011 que des pirates s'étaient introduits dans son réseau informatique pendant deux ans. En 2012, la compagnie pétrolière Aramco a vu 30.000 de ses ordinateurs infectés par un virus. Après avoir subi l'assaut des Anonymous, sorte de Robin des bois autoproclamés du Net, la compagnie nationale du pétrole koweïtien a déconnecté ses trois raffineries d'Internet. Sans être certaines d'être immunisées contre le fléau. Stuxnet, le virus conçu pour attaquer les sites nucléaires iraniens, s'est propagé sur des sites qui n'étaient pas connectés à Internet.

Afin de garder un temps d'avance sur des grands groupes qui se protègent mieux qu'hier, les cybercriminels font évoluer leurs méthodes. Pour atteindre leur cible, ils passent de plus en plus par des sous-traitants ou des fournisseurs. Pour preuve, les entreprises de B to B (commerce interentreprise) ont été ciblées par 15 % des 6 milliards d'attaques répertoriées en 2014 par NTT Com Security.

En attendant, si la crainte d'un virus qui ferait dérailler un train ou plongerait une ville dans le noir est dans tous les esprits, l'essentiel de la cybercriminalité a encore des motifs financiers. L'an passé, 18 % des attaques ont visé des institutions financières, devançant tous les secteurs d'activité.

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

Source : http://www.lesechos.fr/tech-medias/hightech/021137768977-cybercriminalite-les-nouvelles-cibles-1128488.php
Par Sandrine Cassini

Défendre la loi renseignement et s’indigner de la surveillance de la NSA, c’est possible | Le Net Expert Informatique

Défendre la loi renseignement et s’indigner de la surveillance de la NSA, c’est possible

Des hommes et femmes politiques qui avaient voté la loi renseignement se sont émus après les révélations de Wikileaks de la surveillance opérée par l'agence américaine NSA. Sans peur de la contradiction.

Trois présidents sur écoute. Libération et Médiapart ont publié ce 23 juin des documents de Wikileaks qui indiquent que la NSA a réussi à écouter au moins trois présidents, Jacques Chirac, Nicolas Sarkozy et François Hollande, au moins entre 2002 et 2012.
Ces révélations sont arrivés la veille de l'adoption définitive par le Parlement du projet de loi sur le renseignement, qui, comme le rappelle Le Lab, «légalise des pratiques contestables des services [de renseignement], selon ses détracteurs».

Certains n'ont donc pas manqué de souligner l'ironie de la situation:
Les mesures de surveillances internationales #PJLRenseignement permettront de faire ce que le PS dénonce http://t.co/x8ITr9YBxq #FranceLeaks
Pour @fhollande @manuelvalls @BCazeneuve, être écoutés, ce n'est pas grave, ils n'ont rien à cacher… #Franceleaks #PJLRenseignement
Et le ministère de l'Intérieur lui-même a bien vu le problème, regrettant la date de parution des révélations de Wikileaks, susceptibles selon lui de «créer un amalgame» avec le projet de loi renseignement.

Source : https://fr.news.yahoo.com/d%C3%A9fendre-loi-renseignement-sindigner-surveillance-nsa-cest-possible-170902346.html

---

Un réseau de fraude de clés

de connexion Internet démantelé | Le Net Expert Informatique

Un réseau de fraude de clés de connexion Internet démantelé

La brigade ville de la gendarmerie de Bogodogo vient de mettre hors d'état de nuire un réseau qui disposerait de clés de connexion internet de l'ONATEL SA à navigation illimitée.

La cybercriminalité est en pleine expansion au Burkina Faso. Face à ce fléau, le commandement de la Gendarmerie a décidé de lancer une opération d'envergure.
C'est ainsi que la Brigade ville de Bogodogo découvre par une source digne de foi, un réseau de vendeurs de clés de connexion de l'ONATEL SA sur le marché noir, selon le Colonel Sam Djiguiba Ouédraogo, Commandant du groupement départemental de la Gendarmerie de Ouagadougou.
Une enquête ouverte à cet effet a permis de mettre la main sur un auteur principal et trois complices.

La gendarmerie invite la population à la vigilance
Technicien d'exploitation et de maintenance à l'ONATEL SA, l'auteur de la fraude profite de son accès à la base technique pour activer des clés de connexions internet déjà résiliées ou suspendues pour en faire des clés de connexion à navigation illimitée.
Il les met ensuite sur le marché noir par l'intermédiaire de ses complices à des prix variant de 50 000 F CFA à 250 000 F CFA, soutient le commandant de la gendarmerie.
Une fois de plus, la gendarmerie invite la population à la vigilance et à signaler aux forces de sécurité toutes activités suspectes.

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

Source : http://burkina24.com/2015/06/24/cybercriminalite-un-reseau-de-fraude-de-cles-de-connexion-internet-demantele/
Par Serge Balma (stagiaire)

Un hacker cloue plusieurs avions au sol | Le Net Expert Informatique

	Un hacker cloue plusieurs avions au sol

Une attaque informatique subie par la compagnie polonaise LOT a causé l'annulation de 20 vols dimanche.

Des hackers qui clouent des avions au sol. Ce n'est pas le scénario d'un film catastrophe, mais la mésaventure subie dimanche par la compagnie polonaise LOT et racontée par CNN.
Les ordinateurs au sol piratés. Tout a commencé à l'aéroport Chopin de Varsovie, où la compagnie dit avoir été victime d'une attaque. Ses ordinateurs au sol, utilisés pour créer les plans de vols, ont subi une attaque. Résultat : impossible de créer des plans de vols pour les avions au départ de la capitale polonaise.
Au total, la compagnie polonaise a dû annuler pas moins de 20 vols et plusieurs autres ont subi des retards. Quelque 1.400 passagers ont ont été affectés. Une enquête a été ouverte, mais les autorités ignorent l'identité des hackers.
Un hacker arrêté en mai. Ce n'est pas la première fois que des hackers illustrent la vulnérabilité des compagnies aériennes : fin mai, un pirate américain a été arrêté par le FBI après s'être vanté sur Twitter d'avoir réussi à hacker un avion en plein vol. Il assure s'être connecté au système informatique de l'avion et avoir légèrement modifié la trajectoire de l'avion, afin de démontrer les faiblesses du système de sécurité aérien.

Source : http://www.europe1.fr/international/un-hacker-cloue-plusieurs-avions-au-sol-1359726

Une convention internationale pour lutter contre le cybercrime | Le Net Expert Informatique

	Une convention internationale pour lutter contre le cybercrime

En avril 2015, la société Symantec spécialisée dans la sécurité informatique présentait son rapport annuel. Selon ses dires, en 2014, 317 millions de nouveaux programmes malveillants auraient été crées au niveau mondial. Enfin, faut-il rappeler ce qui est arrivé à nos amis de TV5 Monde, il y a de cela quelques semaines ? Ecran noir pour la chaîne les 8 et 9 avril 2015. Sans que pour le moment on sache d'où vient l'attaque.

C'est une évidence, la cybercriminalité est en pleine croissance. Multiforme, mondialisée, l'œuvre d'un petit génie malfaisant, ou d'organisations criminelles quand il ne s'agit pas d'une nouvelle arme d'Etat. Une pieuvre, Octopus…

La Convention de Budapest

Pour le moment, le seul grand texte international existant dans le cadre de la lutte contre ce type de criminalité est l'œuvre du Conseil de l'Europe. Signée à Budapest en novembre 2001, la convention traite des infractions possibles à l'égard des droits d'auteur, de la sécurité des réseaux informatique, des fraudes en général et aussi à la lutte contre la pornographie enfantine. Un texte unique en son genre, qui dépasse le seul cadre du Conseil de l'Europe. Puisque déjà 66 pays du monde entier ont adhéré. Dernier en date, il y a de cela quelques jours le Sri Lanka.

Que ce soit le Conseil de l'Europe qui est en pointe dans ce combat ne paraît pas illogique. Comme le rappelle le spécialiste de cette lutte au sein du Conseil de l'Europe, Alexander Seger, ce sont les droits de l'Homme et la démocratie qui sont en danger.

Ce texte permet avant tout de mener la bataille du droit. Il n'a pas de rapport avec les lois en cours sur le renseignement et qui font beaucoup la Une dans de nombreux pays dont la France. En revanche, devant la croissance de ce type de criminalité et le développement toujours plus rapide de la technique, ce texte doit constamment évoluer de même que les pratiques des autorités. Ainsi le Conseil de l'Europe vient-il de créer à Bucarest un bureau destiné à encadrer et à proposer une aide technique aux juristes ou aux politiques lancés dans ce combat.

De même, tous les 18 mois, une grande réunion internationale se tient avec tous les acteurs concernés. C'est cette réunion qui répond au doux nom d'Octopus. La dernière se tient à Strasbourg ces jours-ci. Ces conférences permettent de faire le point sur de nouvelles pratiques problématiques qui apparaissent. Ainsi sur le droit des victimes passablement oubliées pour le moment ou bien encore, et ce sera le thème principal des travaux, sur la difficulté pour la justice de trouver des preuves informatiques. Dans quel disque dur les trouver, quel nuage explorer ? En rappelant à nouveau qu'il ne s'agit là que d'un texte portant sur le judiciaire.

Il y a quelques semaines, à La Haye, s'est tenu également une Conférence mondiale sur le Cyber espace 2015. Cette rencontre qui prend en compte les extraordinaires possibilités qu'offre internet avait pris en compte également la question de la sécurité qui doit régner dans le cyberespace. La prise de conscience est donc bien là, il faut espérer que les techniques des criminels quels qu'ils soient n'aillent pas en se développant plus vite que les solutions. Or, et l'on revient à l'étude annuelle de Symantec, il faut désormais aux éditeurs de logiciels beaucoup plus de temps pour créer et déployer des correctifs en cas de faille sécuritaire.

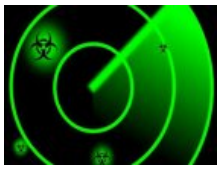
Et s'il fallait vous convaincre du problème, un dernier exemple, celui des « rançongiciels ». Ils prennent le contrôle de vos PC et vous piquent littéralement vos données rendues plus tard contre rançon. Une entreprise française s'est vu réclamer ainsi 90.000 euros.

Et vous, si vous êtes amateurs de pizzas, vous risquez gros…

Lire la suite….

Source : http://geopolis.francetvinfo.fr/une-convention-internationale-pour-lutter-contre-le-cybercrime-65027

Une faille de Flash exploitée pour des attaques de phishing contre des entreprises | Le Net Expert Informatique



Une faille de Flash exploitée pour des attaques de phishing contre des entreprises

Alerté début juin par FireEye de l'exploitation d'une faille inconnue de Flash pour des attaques ciblées de phishing, Adobe met à jour son plugin Flash sur Windows et Mac OS X.

Une nouvelle faille critique de Flash a été identifiée. C'est banal, presque. Adobe, l'éditeur de Flash, est régulièrement confronté à des problèmes de sécurité. Toutefois, si la vulnérabilité a été découverte c'est car celle-ci faisait d'ores et déjà l'objet d'exploitations malveillantes.
C'est la société de sécurité FireEye qui a détecté ces attaques. Plus tôt ce mois-ci, ses chercheurs ont repéré des campagnes de phishing dirigées contre des entreprises et exploitant une faille inconnue de Flash.

Des attaques « limitées »
Selon FireEye, ces attaques de phsihing ont ainsi ciblé des entreprises des secteurs de l'aéronautique, de la défense, de la construction, des transports mais aussi de l'informatique et des télécoms. L'acteur de la sécurité a alerté Adobe début juin.
L'éditeur a donc été contraint de diffuser un correctif de sécurité, en dehors de son cycle habituel de mise à jour. Adobe assure que le nombre d'attaques ciblées exploitant la faille est resté limité.
La firme ajoute qu'Internet Explorer sur Windows 7 (et les versions suivantes) est affecté par ce problème de sécurité, tout comme Firefox sur Windows XP. La version 18.0.0.194 du plugin Flash remédie à la vulnérabilité sur Windows et Mac OS. Les utilisateurs de Chrome recevront automatiquement la mise à jour.

Source : http://www.zdnet.fr/actualites/une-faille-de-flash-exploitee-pour-des-attaques-de-phishing-contre-des-entreprises-39821388.htm