Denis JACOPINI participera au 8e IT-Forum à Abidjan les 2 et 3 juin 2016

Denis JACOPINI participera au 8e IT-Forum à Abidjan les 2 et 3 juin 2016

La 8e édition du IT-Forum (Forum des décideurs et acteurs des Technologies de l'Information) se déroulera les 2 et 3 juin prochain à Abidjan.

IT FORUM 8ème EDITION

Des conférences seront animées en plénières par des spécialistes, des Experts-Consultants et des Universitaires. Ce sera le lieu de faire des exposés, de partager des expériences, de former et d'informer les participants.
Les enjeux de la transformation numérique et plus globalement de l'appropriation des nouvelles technologies modifient considérablement notre mode de vie. La sécurisation des données et des dispositifs de paiement comporte des failles qu'il comporte d'améliorer pour apporter la confiance nécessaire au climat des affaires.
De nombreuses études viennent conforter ce constat et tendent à démontrer le potentiel de croissance du secteur.
En Côte d'Ivoire, les transactions mobiles s'élèvent à 15 milliards de FCFA par jour soit 22,5 millions d'Euros.
Des montants qui donnent le vertige et qui poussent les sites marchands notamment les opérateurs de télécommunications à prendre des mesures de sécurité de plus en plus importantes… mais qui montrent aussi rapidement leurs limites !
Au fil des années, la Côte d'Ivoire s'est imposée comme l'un des leaders naturels dans le domaine des transactions mobiles en Afrique.
En insistant sur la priorité à donner à la protection des données et des transactions (mobile banking, eCommerce),
Devenu un rendez-vous incontournable depuis une décennie, l'IT Forum s'impose aujourd'hui comme l'une des
rencontres les plus importantes.
QUAND
Jeudi 2 juin 2016 à 08:00 – Vendredi 3 juin 2016 à 18:00 (Heure : Côte d'Ivoire) – Ajouter au calendrier
LIEU
Maison de l'entreprise – CGECI (Confédération Générale des Entreprises de Côte d'Ivoire – Patronat ivoirien), Avenue Lamblin, Abidjan, Lagunes, Côte d'Ivoire, Abidjan, Plateau, Cote d'Ivoire –
PROGRAMME
http://www.ciomag-event.com/8eme-edition-it-forum-cote-d-ivoire

---

Réagissez à cet article

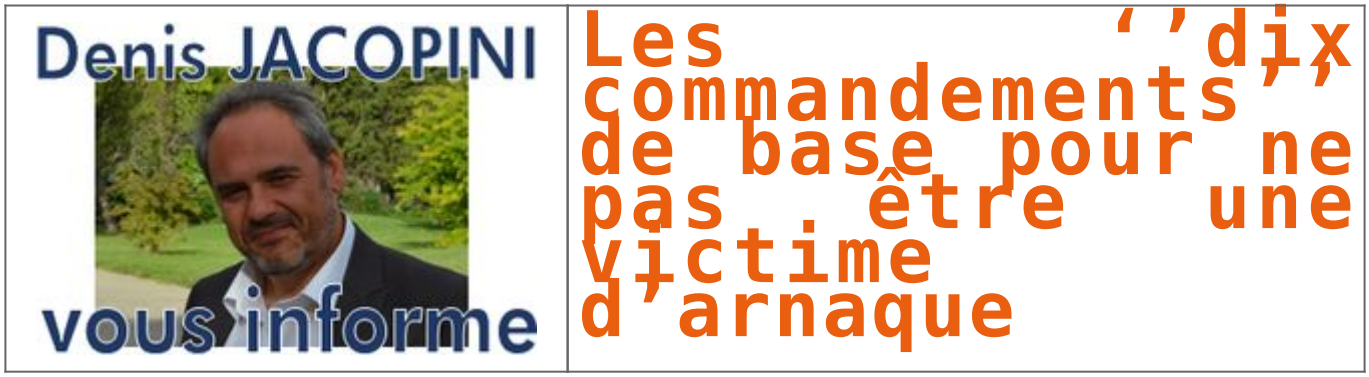
Sources :

IT-Forum 2016 – 8e édition du Forum des décideurs et acteurs des Technologies de l'Information

http://it-forum.ci

https://www.eventbrite.fr/e/inscription-it-forum-2016-8eme-edition-24951266911

Les ‘’dix commandements’’ de base pour ne pas être une victime d'arnaque



Les cybercriminels continuent de faire de nombreuses victimes à travers le monde. Si des moyens de répression de cette activité criminelle sont entrepris dans nos différents pays, l'un des moyens les plus efficaces de l'éradiquer reste la prévention.

Dans cet article, la Plateforme de lutte contre la cybercriminalité (PLCC) fait un rappel en 10 points des mesures à prendre pour naviguer sur la toile en toute sécurité.

1- Changer régulièrement vos mots de passe. (Un site = Un mot de passe unique)

2- Aucune autorité judiciaire, de police ne possède d'adresse mail gratuite de type Hotmail, Yahoo, Gmail…

3- Ne divulguez pas d'informations personnelles sur Internet. Prenez le temps de sécuriser vos comptes ainsi que ceux de vos enfants. Ne rendez pas visibles vos contacts sur Facebook ou autre réseau sociale.

4- Allez toujours sur une adresse commençant par https://, officielle et habituelle pour vous connecter à votre compte bancaire, à votre messagerie ou autres réseaux sociaux.

5- Evitez d'envoyer des photos ou vidéos, de vous, à caractère sexuelle ou tout autre position indélicate.

6- Ne versez jamais d'argent par Mandat Cash ou Western Union à une personne que vous ne connaissez pas, que vous n'avez jamais rencontrée physiquement.

7- Méfiez-vous des trop bonnes affaires. Ne cédez jamais à la précipitation. Les bases d'une transaction sont les mêmes dans la réalité et sur Internet. Une annonce trop alléchante cache souvent une arnaque. Renseignez-vous, comparez les prix et les produits avant d'acheter.

8- Cessez tout contact si votre interlocuteur (que vous ne connaissez pas) vous demande de l'argent sous prétexte de frais, de maladie, de transport…

9- Remettez vous souvent en question. Il n'y a pas de profil type de victime, personne n'est à l'abri sur Internet. Les cyberdélinquants jouent parfois sur notre confiance excessive en nos capacités.

10- Ayez un anti-virus efficace et à jour sur votre ordinateur.

Une fois de plus, la PLCC vous exhorte à la prudence !… [Lire la suite]

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet…) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Source : *Lutte contre la cybercriminalité: Voici les ‘’dix commandements’’ de base pour ne pas être une victime d’arnaque*

Combien vous coûterait le piratage de vos données ?

Combien vous coûterait le piratage de vos données ?

Un consommateur français sur trois reconnaît que sa loyauté envers une marque diminue après qu'une attaque informatique a porté atteinte aux données qu'il lui avait confié.

Souvent préparées de longues dates, les attaques informatiques qui frappent les entreprises laissent des traces longtemps après.
Publiée aujourd'hui, une étude internationale menée par Vanson Bourne, pour l'éditeur de logiciels de cybersécurité FireEye, souligne que les conséquences de tels épisodes entament la performance commerciale de la société victime, au-delà des dégâts informatiques des premiers jours. « *La sécurité des systèmes d'information a un réel impact sur la confiance des consommateurs* », affirme Yogi Chandiramani, directeur des ventes en Europe pour FireEye.
« *En France, l'attaque qui a touché TV5 Monde en avril 2015 et les vols de données chez Orange en 2014 ont particulièrement marqué les esprits* », poursuit-il. 34 % des consommateurs français reconnaissent que leur loyauté en tant que client actuel ou potentiel d'une marque diminue après qu'une entreprise a laissé fuiter des données, pointe le questionnaire en ligne envoyé à 1.000 d'entre eux. Un argument de plus pour ceux qui voient les efforts de cyber-sécurité comme un argument de compétitivité .
L'atteinte à leurs données personnelles refroidit particulièrement les ardeurs à l'achat des consommateurs. Quand le vol de données est connu, plus de trois Français sur quatre déclarent qu'ils stopperaient leurs emplettes de produits ou services fournis par la victime, surtout si la faute vient de l'équipe dirigeante – ils sont plus conciliants s'il s'agit de l'erreur humaine d'un subordonné. La tendance se confirme au fil des années. D'après l'étude, 61 % des Français déclarent avoir pris en considération la sécurité de leurs données lors de leurs achats en 2015. Ils n'étaient que 53% dans cet état d'esprit en 2014…

Après une cyber-attaque, la transparence prime

A cette perte de chiffre d'affaires potentiel s'ajoute le risque de poursuite en justice. La moitié des Français déclarent qu'ils engageraient des poursuites contre l'entreprise cyber-attaquée qui n'a pas su protéger leurs données personnelles, volées ou utilisées à des fins criminelles. Aux Etats-Unis, Target et Sony Picture s ont été attaqués en Justice par des procédures de class action, le premier par ses clients, le second par ses salariés.
Dès lors, la tentation peut être grande pour une entreprise de garder secret le fait que son système d'information ait été vulnérable à des cyber-criminels. Ce serait pourtant aggraver le mal qui surviendra au moment où, inévitablement à l'heure d'Internet, l'information ressortira.
« *Les consommateurs pointent les négligences des entreprises mais attendent surtout d'elles de la transparence, 93 % d'entre eux souhaitent être prévenus dans les 24h quand leurs données sont exposées* », prévient Yogi Chandiramani.

Des changements dans quelques mois ?

Le règlement européen sur la protection des données, qui devrait s'appliquer en France d'ici 2018, prévoit d'imposer aux sociétés de notifier les autorités, voir leurs clients, de toutes atteintes sur les données personnelles des citoyens européens dans les 72h après la découverte du problème.
A noter :
L'attaque particulièrement destructrice qui a touché TV5Monde en 2015 devrait coûter près de 10 millions d'euros sur trois ans, uniquement en réparation informatique… [Lire la suite]

Réagissez à cet article

Source : *Cyber-attaque : les coûts d'après, Cybersécurité – Les Echos Business*

La police peut-elle obliger un suspect à débloquer son iPhone avec son doigt ?

La police peut-elle obliger un suspect à débloquer son iPhone avec son doigt ?

Aux États-Unis, une affaire judiciaire pose la question du droit que peuvent avoir les autorités judiciaires à contraindre un suspect à débloquer son iPhone avec le capteur Touch ID qui permet d'accéder au contenu du téléphone avec les empreintes digitales.

La question s'est certainement déjà posée dans les commissariats et dans les bureaux des juges d'instruction, et elle devrait devenir plus pressant encore dans les années à venir : alors qu'un suspect peut toujours prétendre avoir oublié son mot de passe, ou refuser de répondre, les enquêteurs peuvent-ils contraindre un individu à débloquer son téléphone lorsque celui-ci est déblocable avec une simple empreinte digitale ?
Le débat sera tranché aux États-Unis par un tribunal de Los Angeles. Le Los Angeles Times rapporte en effet qu'un juge a délivré un mandat de perquisition à des policiers, qui leur donne le pouvoir de contraindre physiquement la petite amie d'un membre d'un gang arménien à mettre son doigt sur le capteur Touch ID de son iPhone, pour en débloquer le contenu.

Le mandat signé 45 minutes après son placement en détention provisoire a été mis en œuvre dans les heures qui ont suivi. Le temps était très court, peut-être en raison de l'urgence du dossier lui-même, mais aussi car l'iPhone dispose d'une sécurité qui fait qu'au bout de 48 heures sans être débloqué, il n'est plus possible d'utiliser l'empreinte digitale pour accéder aux données. Mais l'admissibilité des preuves ainsi collectées reste sujette à caution et fait l'objet d'un débat entre juristes.

EN MONTRANT QUE VOUS AVEZ OUVERT LE TÉLÉPHONE, VOUS DÉMONTREZ QUE VOUS AVEZ CONTRÔLE SUR LUI
Certains considèrent qu'obliger un individu à placer son doigt sur le capteur d'empreintes digitales de son iPhone pour y gagner l'accès revient à forcer cette personne à fournir elle-même les éléments de sa propre incrimination, ce qui est contraire à la Constitution américaine et aux traités internationaux de protection des droits de l'homme. « En montrant que vous avez ouvert le téléphone, vous montrez que vous avez contrôle sur lui », estime ainsi Susan Brenner, une professeur de droit de l'Université de Dayton. Le capteur Touch ID ne sert pas uniquement à débloquer le téléphone, mais aussi à le déchiffrer, en fournissant une clé qui joue le rôle d'authentifiant du contenu.
D'autres estiment qu'il s'agit ni plus ou moins que la même chose qu'une perquisition à domicile réalisée en utilisant la clé portée sur lui par le suspect, ce qui est chose courante et ne fait pas l'objet de protestations. Ils n'y voient pas non plus de violation du droit de garder le silence, puisque le suspect ne parle pas en ne faisant que poser son doigt sur un capteur.

ET EN FRANCE ?
Pour le moment, le sujet n'est pas venu sur la scène législative en France. Mais il pourrait y venir par analogie avec d'autres techniques d'identification biométrique.
En matière de recherche d'empreintes digitales ou de prélèvement de cheveux pour comparaison, l'article 55-1 du code de procédure pénale punit d'un an de prison et 15 000 euros d'amende « le refus, par une personne à l'encontre de laquelle il existe une ou plusieurs raisons plausibles de soupçonner qu'elle a commis ou tenté de commettre une infraction, de se soumettre aux opérations de prélèvement ». De même en matière de prélèvements ADN, le code de procédure pénale autorise les policiers à exiger qu'un prélèvement biologique soit effectué sur un suspect, et « le fait de refuser de se soumettre au prélèvement biologique est puni d'un an d'emprisonnement et 30 000 euros d'amende ».
Sans loi spécifique, les policiers peuvent aussi tenter de se reposer sur les dispositions anti-chiffrement du code pénal, puisque l'empreinte digitale sert de clé. L'article 434-15-2 du code pénal punit de 3 ans de prison et 45 000 euros d'amende le fait, « pour quiconque ayant connaissance de la convention secrète de déchiffrement d'un moyen de cryptologie susceptible d'avoir été utilisé pour préparer, faciliter ou commettre un crime ou un délit, de refuser de remettre ladite convention aux autorités judiciaires ou de la mettre en oeuvre, sur les réquisitions de ces autorités ». Mais à notre connaissance, elle n'a jamais été appliquée pour forcer un suspect à fournir lui-même ses clés de chiffrement, ce qui serait potentiellement contraire aux conventions de protection des droits de l'homme… [Lire la suite]

Réagissez à cet article

Source : *La police peut-elle obliger un suspect à débloquer son iPhone avec son doigt ? – Politique – Numerama*

Airbus déjoue douze attaques informatiques majeures par an

Airbus déjoue douze attaques informatiques majeures par an

Source : *Piratage informatique : Airbus déjoue douze attaques majeures par an – 06/05/2016 – ladepeche.fr*

article de Gil Bousquet

Comment s’introduire dans le web invisible ?

Comment s’introduire dans le web invisible ?

La façon la plus répandue et la plus simple de s'introduire dans cette partie immergée du web est le serveur Tor, acronyme pour The Onion Router. Pourquoi oignon ? Parce que le logiciel assure plusieurs couches de protection, qui permettent entre autres de conserver l'anonymat de l'internaute.

Tous les sites qui ont cours sur ce moteur de recherche se terminent par .onion. L'étudiant en informatique qui a accepté de faire une démonstration à L'Express affirme qu'à toutes les fois qu'une personne brassant des affaires sur le «*deep web*» fait une requête, elle ne passe jamais par le même chemin afin de brouiller les pistes.
«Tout le monde se connecte sur un même serveur et une fois que tu es connecté sur ce serveur, tu passes par un réseau de connections international, explique-t-il. Tu as un serveur d'entrée et un serveur de sortie. Ce qui se passe entre, on ne le sait pas. Ton adresse IP se perd. »

Un enseignant en informatique au Cégep de Drummondville, Louis Marchand, abonde également en ce sens : «Si la personne est excessivement prudente dans ses démarches, la seule chose qui pourrait être retracée serait sa connexion au réseau Tor. Toutes les actions, légales ou pas, que cette personne a pu effectuer à l'intérieur du serveur sont pratiquement introuvables.» Pratique lorsqu'on veut publier des anecdotes sur un blogue en évitant la censure… ou pour publier une offre d'achat de cocaïne.
Ce moteur de recherche, développé par la marine américaine, se télécharge aussi facilement que Google Chrome et est associé avec le moteur Firefox. Comme quoi Tor n'est pas illégal du tout : «c'est l'utilisation qu'on en fait qui peut être négative», complète l'étudiant.

Les bitcoins, la monnaie virtuelle anonyme
La monnaie ayant cours sur le web invisible est le *bitcoin*, une forme d'argent virtuelle cryptée. Elle n'est soumise à aucun taux de change ni à aucune banque, donc aucun intermédiaire n'existe entre l'acheteur et la marchandise. Cependant, son atout majeur pour les consommateurs de produits illicites est qu'elle peut être utilisée de façon anonyme.
Louis Marchand décrit le bitcoin comme n'étant rien d'autre qu'un fichier. «Il faut faire attention à ça : toutes les transactions sont enregistrées, même si le bitcoin en tant que tel n'est pas identifié. C'est beaucoup plus difficile de retracer de l'argent liquide, puisque absolument rien ne lie un 20 $ à son propriétaire», spécifie-t-il.

Selon l'enseignant, le bitcoin fonctionne exactement comme l'or ou le diamant. «Ce qui diffère, c'est que quelque chose de virtuel change beaucoup plus rapidement que n'importe quelle ressource physique. Demain, un bitcoin peut valoir 2 $ et le lendemain, plus de 2000 $. C'est un coup de dé.»
Cette monnaie est cependant extrêmement difficile à générer et est très coûteuse en électricité, d'après Louis Marchand : elle nécessite beaucoup de ressources et de temps, puisqu'elle doit correspondre à des critères mathématiques très précis. C'est notamment ce qui expliquerait la valeur toujours montante des bitcoins. Au moment de la vérification de L'Express, un de ces fichiers valait 550 $.
Selon les dires de l'étudiant en informatique qui a préféré conserver l'anonymat, lorsqu'il s'est lui-même procuré huit bitcoins il y a quelques années, ça ne lui avait pas coûté plus d'une centaine de dollars. «Si je me souviens bien, ça a déjà monté à 1400 $. C'est hallucinant», s'étonne-t-il.
Il faut dire que le marché du web invisible, dans lequel évoluent les bitcoins, est aussi extrêmement lucratif. La Sureté du Québec, les deux compères ayant testé les drogues du «*deep web*» et l'informaticien s'accordent tous sur un point : la rémunération est la motivation principale de n'importe quel trafiquant de marchandises illégales sur Internet, selon eux.
«Moins c'est légal, plus c'est payant. Personne n'ira vendre un foie sur Internet, à part pour l'argent que ça rapporte. Il faut oublier le côté humain et ne penser qu'au montant final», croit Louis Marchand… [Lire la suite]

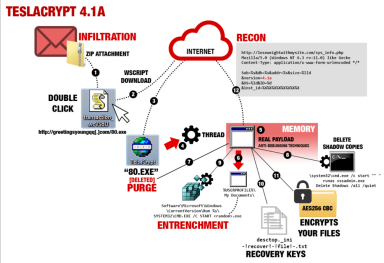
Source : *Le logiciel Tor, la porte d'entrée du web invisible – Actualités – L'Express – Drummondville*

Le CryptoVirus TeslaCrypt s’attaque à de nouveaux fichiers et améliore sa protection

	Le CryptoVirus TeslaCrypt s’attaque à de nouveaux fichiers et améliore sa protection

Ces nouveaux exemplaires de TeslaCrypt sont diffusés massivement en tant que pièce jointe dans des spams qui imitent les avis de réception de colis des courriers express. D'après Endgame, la version 4.1A est apparue il y a environ une semaine ; outre les extensions déjà ciblées, elle attaque également les fichiers suivants .7z, .apk, .asset, .avi, .bak, .bik, .bsa, .csv, .d3dbsp, .das, .forge, .iwi, .lbf, .litemod, .litesql, .ltx, .m4a, .mp4, .rar, .re4, .sav, .slm, .sql,

La diffusion de TeslaCryp via le spam constitue également un changement : lors des campagnes récentes de TeslaCrypt, le ransomware avait été propagé via des kits d'exploitation et des redirections depuis des sites WordPress et Joomla. Dans ce cas, la victime doit ouvrir le fichier ZIP en pièce jointe afin d'activer un downloader JavaScript qui utilise Wscript (un composant de Windows) pour télécharger le fichier binaire de TeslaCrypt depuis le domaine greetingsyoungqq[.]com.
D'après notre interlocutrice, l'analyse de la version actualisée du ransomware fut complexe car elle lance de nombreux flux d'application et d'opérations de débogage afin de compliquer la tâche des outils de protection. Comme l'explique Amanda Rousseau, « il semblerait qu'il essaie de dissimuler les lignes dans la mémoire. Il est plus difficile pour l'Antivirus de les détecter s'il n'analyse pas la mémoire. »



Le recours à Wscript rend également la détection plus compliquée car le trafic ressemble à des communications légitimes de Windows. Selon Amanda Rousseau, il aura fallu quatre jours aux outils de détection pour identifier la technique et l'ajouter aux signatures. La durée de service des serveurs de commande sur lesquels se trouve TeslaCrypt a été limitée. A l'issue de celle-ci, les individus malintentionnés changent d'hébergement.
La version actualisée du ransomware utilise également un objet COM pour dissimuler les lignes de code extraites et élimine les identifiants de zone afin qu'ils ne soient pas découverts. De plus, pour éviter la surveillance, le malware arrête plusieurs processus Windows : Task Manager, Registry Editor, SysInternals Process Explorer, System Configuration et Command Shell. Pour garantir sa présence permanente, il se copie sur le disque et crée le paramètre correspondant dans la base de registres.
Vous trouverez une description technique détaillée de TeslaCrypt, y compris de ses méthodes de chiffrement et de ses techniques de lutte contre le débogage sur le blog d'Endgame.
Amanda Rousseau a indiqué dans ses commentaires que lors des essais, les nouveaux échantillons ont atteint les disques réseau connectés et ont tenté de chiffrer les fichiers qui s'y trouvaient. Ils tentent également de supprimer le cliché instantané du volume afin de priver la victime de toute chance de récupération.
Mais il y a malgré tout une bonne nouvelle : la version actualisée de TeslaCrypt chiffre les fichiers à l'aide d'une clé AES 256 et non pas à l'aide d'une clé RSA de 4 096 bits comme indiqué dans la demande de rançon et qui plus est, les informations indispensables au déchiffrement restent sur la machine infectée. « Nous avons trouvé l'algorithme de chiffrement : il fonctionne correctement, mais laisse le fichier de restauration dans le système » a confirmé Amanda Rousseau. « Si l'on part du programme de déchiffrement antérieur de TeslaCrypt et que son code est actualisé conformément aux [découvertes], il sera possible de réaliser le déchiffrement. » Il y a un an environ, Cisco a diffusé un utilitaire de ligne de commande capable de déchiffrer les fichiers touchés par TeslaCrypt.
Amanda Rousseau a également signalé que les auteurs de la version actualisée du ransomware avait emprunté beaucoup de code aux versions antérieures, notamment l'utilisation des objets COM et certaines techniques de débogage. « On dirait que les individus malintentionnés suivent les chercheurs à la trace en surveillant le code [de déchiffrement] publié sur Github en open source » explique le président d'Endgame en montrant les modifications introduites au cours du dernier mois depuis la version 4.0 jusqu'à la version 4 1A. – De petites modifications sont introduites dans chaque version et à la sortie de chaque nouveau décrypteur. Il prenne le meilleur de ce qui était utilisé il y a deux mois et l'appliquent aujourd'hui. »… [Lire la suite]

Source : *TeslaCrypt s'attaque à de nouveaux fichiers et améliore sa protection – Securelist*

Une Afrique de plus en plus connectée mais qui doit faire face aux cybermenaces mondiales

Une Afrique de plus en plus connectée mais qui doit faire face aux cybermenaces mondiales

Avec un taux de croissance au niveau des TIC de l'ordre de 30% sur un marché de plus d'un milliard de personnes, l'Afrique représente le nouvel Eldorado du monde numérique.

Or, la surface d'attaque augmentant, les cybercriminels élargissent leur champ d'action. La cybercriminalité en Afrique est organisée et bien enracinée, en particulier au Nigéria, au Ghana et en Côte d'Ivoire. Désormais, l'Afrique n'est plus le théâtre des seuls cybercriminels mais aussi de cyberhacktivistes voire de hackers. Le Sénégal a été la victime de cyberattaques en janvier dernier revendiquées par le collectif anonymous du Sénégal. Par rebond des attaques massives menées en janvier en France suite aux attentats de Charlie Hebdo, les serveurs de l'agence de l'informatique de l'Etat du Sénégal sont tombés.
Devant ce désert cybernétique, les Etats d'Afrique tentent de réagir en relevant le défi de sécuriser leurs infrastructures réseau, leurs données et en formant leurs personnels. La France participe activement à la formation cyber des officiers et des techniciens par le biais de la coopération opérationnelle (ministère de la défense). Depuis 2013, une centaine d'officiers et sous-officiers ont été formés au Sénégal, au Niger et au Burkina Faso par les Eléments français au Sénégal.

SecurityDay 2016

Avec la présence des plus grands décideurs du monde de la confiance numérique, l'évènement SecurityDay 2016 vous ont proposé pendant deux jours des conférences sur le thème « cybersécurité et confiance numérique ».
Les SecurityDays ont pour objectif de réunir l'ensemble de l'écosystème numérique africain et d'accélérer le développement d'un espace de confiance afin d'accompagner l'essor du numérique en Afrique, vecteur durable de croissance économique et de développement.
Avec le soutien de l'ANSSI française et de l'ADIE sénégalaise, cet évènement unique en Afrique de l'Ouest est un cadre d'échanges entre experts militaires, civils, décideurs IT, chefs d'entreprise, industriels et utilisateurs finaux pour réfléchir conjointement aux problématiques liées à la cybersécurité en Afrique. … [Lire la suite]

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, arnaques Internet...) et judiciaires (contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Denis JACOPINI est expert informatique assermenté spécialisé en cybercriminalité en Afrique de l'Ouest

Suivez-nous sur

Réagissez à cet article

Source : *SecDay 2016*

Darknet: qu’est ce qu’on y trouve et comment y accéder ?

Darknet:, qu’est ce qu’on y trouve et comment y accéder ?

Au fil de nos CyberBalades, notre souris s’est arrêtée sur un article très intéressant sur le DarkNet. Pour votre plus grand plaisir, veuillez trouver ci-dessous un extrait et le lien permettant de le consulter en entier.

Qu’est-ce qu’on trouve dans le Darknet ?

Ce qui frappe en premier c’est la **quantité de contenus illégaux**. On compte environ un tiers de porno (dont une bonne partie de pédopornographie et d’autres trucs louches), un autre tiers de contenu illégal (culture de drogue, négationnisme, numéro de carte bancaire, comment faire un petit engin explosif, etc.) et un dernier tiers de sites inclassables… [Lire la suite]

Liste des URL intéressantes pour explorer le darknet

- **Moteur de recherche** : http://hss3uro2hsxfogfq.onion
- **Hidden wiki**: http://zqktlwi4fecvo6ri.onion/wiki/index.php/Main_Page
- **Annuaire des liens** : http://torlinkbgs6aabns.onion
- **Facebook pour Tor**: https://facebookcorewwwi.onion
- **Moteur de recherche Darknet**: http://grams7enufi7jmdl.onion
- **Vente des mobiles débloqués:** http://mobil7rab6nuf7vx.onion
- **Location des services d’un hacker**: http://2ogmrlfzdthnwkez.onion
- **Moteur de recherche DuckDuckGo**: http://3g2upl4pq6kufc4m.onion

[Lire la suite]

[block id="24761" title="Pied de page HAUT"]

Quelques articles sélectionnés par notre Expert qui pourraient aussi vous intéresser :

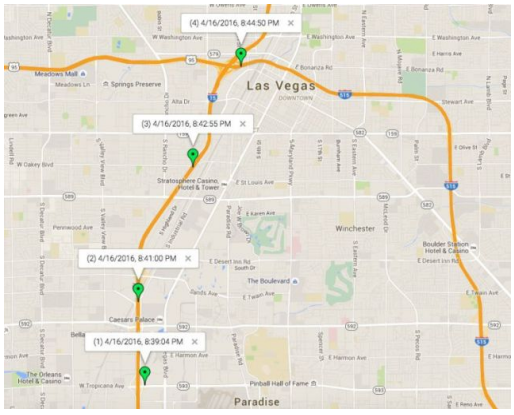
Les 10 conseils pour ne pas se faire «hacker» pendant l'été
Les meilleurs conseils pour choisir vos mots de passe
Victime d'un piratage informatique, quelles sont les bonnes pratiques ?
Victime d'usurpation d'identité sur facebook, tweeter ? Portez plainte mais d'après quel article de loi ?
Attaques informatiques : comment les repérer ?

[block id="24760" title="Pied de page BAS"]

Source : *Darknet: qu'est ce qu'on y trouve et comment y accéder ?*

Auteur : Ahmed EL JAOUARI

Waze : les hackeurs peuvent vous suivre à la trace

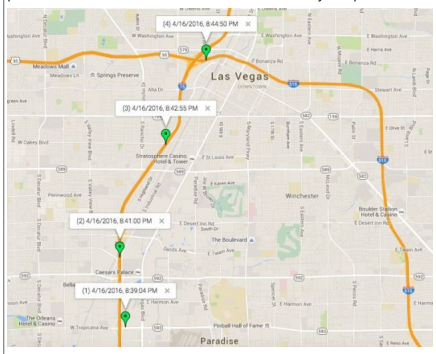


Waze : les hackeurs peuvent vous suivre à la trace

Des experts en sécurité informatique ont découvert une faille permettant d'espionner en temps réel les trajets des utilisateurs de l'application de navigation communautaire Waze. Selon eux, presque toutes les applications d'aide à la conduite seraient concernées. Explications.

C'est l'une des applications d'aide à la conduite les plus populaires en France. Aujourd'hui, près de 5 millions d'automobilistes utilisent presque quotidiennement le service de navigation communautaire Waze. Il a y a quelque mois, des chercheurs de l'Université de Californie à Santa-Barbara (Etats-Unis) ont découvert une faille, partiellement corrigée seulement, qui permet à des hackeurs d'espionner en temps réel les déplacements de n'importe quel utilisateur.
L'équipe d'experts en sécurité informatique a suivi durant trois jours les trajets d'une journaliste du site américain Fusion. Afin de vous livrer les informations de trafic, Waze utilise une connexion sécurisée pour communiquer avec votre smartphone. Or c'est justement là que se trouve la faille. Les chercheurs sont parvenus, en effet, à se placer entre les serveurs de l'application et l'utilisateur. De ce fait, ils ont pu intercepter toutes ses données de navigation, ainsi que ses trajets en bus ou en taxi.

Voiture fantôme, véhicule espion, embouteillage virtuel
Une fois infiltrés dans les serveurs de l'application, ils ont pu étudier en détail le fonctionnement des algorithmes de Waze. Au-delà des problèmes de confidentialité, les chercheurs se sont aperçus qu'ils pouvaient également créer des véhicules « fantômes ». Dans le but, par exemple, de créer de faux embouteillages ou d'épier tous les utilisateurs se trouvant à proximité de ce conducteur virtuel. En envoyant plusieurs véhicules fantômes, ils affirment avoir été en mesure de quadriller un quartier entier.



D'après ces experts en sécurité en informatique, il serait même possible de surveiller l'intégralité de la population américaine, simplement "en utilisant quelques serveurs de plus". Imaginez : tous vos trajets pourraient être enregistrés et mis à disposition du plus offrant. L'équipe de recherche a informé Waze de sa découverte, il y a plusieurs mois, et l'application, rachetée par Google en 2013, avait procédé à une mise à jour. Mais elle ne corrige que partiellement la faille.
« Toutes ont quasiment toutes ce type de failles »
Depuis janvier dernier, les données de géolocalisation ne sont plus partagées avec les conducteurs situés à proximité lorsque l'application est ouverte en tâche de fond. En revanche, il est toujours possible de vous espionner lorsqu'elle est en marche. Mais la faille est toujours présente quand on l'utilise en premier plan.

Comment faire ? ⇒ Seule solution pour le moment : utiliser le mode invisible… qui se désactive automatiquement à chaque redémarrage de l'application.

Waze semble être en effet conscient de ses lacunes. Dernièrement, l'application a mis en place une fonction censée permettre à son utilisateur de masquer son emplacement réel. Cependant, comme on le démontre l'enquête de Fusion, ce nouveau système n'est pas vraiment efficace. Et surtout, elle n'est pas à la seule application concernée, si l'on en croit Ben Zhao : « Nous avons étudié de nombreuses applications. Presque toutes ont ce type de failles. Nous ne savons pas comment stopper cela », s'inquiète Zhao. Pas de quoi rassurer les automobilistes… [Lire la suite]

Réagissez à cet article

Source : *Waze : les hackeurs peuvent vous suivre à la trace – metronews*