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

Les voitures semi-autonomes, cause de distraction des conducteurs ?

Les voitures semi-autonomes, cause de distraction des conducteurs ?

Des experts canadiens dénoncent les voitures semi-autonomes qui favoriseraient la déconcentration des conducteurs. Tesla est dans le viseur.

Ne jamais quitter la route des yeux. C'est peut-être la règle la plus inlassablement martelée par les moniteurs d'auto-école pour des raisons évidentes de sécurité. Pour ces mêmes raisons, des experts dénoncent le risque de déconcentration que pourraient provoquer les voitures semi-autonomes.
En effet, un groupe d'experts chargés d'établir un cadre réglementaire pour les voitures sans conducteur a fait part de ses inquiétudes au ministre des transports canadien l'automne dernier, en mettant en garde sur l'affaiblissement de la vigilance que pourrait induire la conduite gérée par un système de bord.

Trafic routier

Dans des notes récemment révélées par The Canadian Press, et relayées par le site CBC, ils y évoquent la « question de la vigilance des conducteurs qui peut poser problème » lorsque ce mode de conduite dirige le véhicule. Ils écrivent que « les conducteurs tendent à surestimer les capacités des systèmes automatisés et sont naturellement déconcentrés quand l'auto-pilote est activé ».
Dans ce cas de figure, les automobilistes pourraient s'adonner à d'autres activités – comme lire le journal, regarder leur téléphone ou discuter avec les autres passagers – pendant que la voiture est en auto-pilote, estimant qu'elle est tout à fait capable de se passer de la supervision humaine.
Or, ces autres activités réduisent de fait la capacité des conducteurs à réagir rapidement quand il faut prendre le relais. Barrie Kirk, du Canadian Automated Vehicles Centre of Excellence, est même allé jusqu'à affirmer que « lorsque l'ordinateur conduira, les automobilistes feront beaucoup plus l'amour » derrière le volant.

Volant Toyota

Des conducteurs incapables de réagir avec promptitude ?
Sans surprise, le constructeur automobile américain Tesla est cité par les experts au regard de sa relative avancée dans le domaine de la voiture autonome. L'entreprise n'a pas officiellement réagi, mais il est important de rappeler qu'elle ne présente à aucun moment ses voitures comme des moyens de transport totalement autonomes.
Plusieurs vidéos prises à bord de voiture Tesla montrent d'ailleurs que le système d'auto-pilotage est encore à améliorer. Les experts suggèrent notamment l'installation de sortes de boites noires dans les véhicules qui récolteraient les informations de route et permettraient d'améliorer les capacités de l'auto-pilote… [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

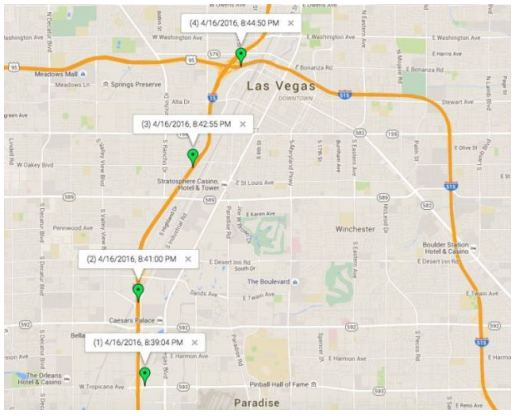
Contactez-nous

Suivez-nous sur

Réagissez à cet article

Source : *Les voitures semi-autonomes, cause de distraction des conducteurs ? – Tech – Numerama*

Waze : les hackeurs peuvent vous suivre à la trace

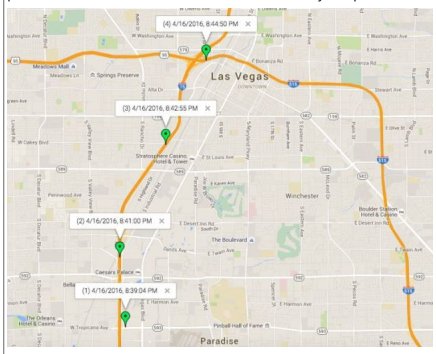


Waze : les hackeurs peuvent vous suivre à la trace

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]

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

Suivez-nous sur

Réagissez à cet article

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

Publier un selfie devant la pyramide du Louvre, est-ce du

vol ?

Publier un selfie devant la pyramide du Louvre, est-ce du vol ?

Oui, selon les sénateurs, qui ont réservé cette publication aux particuliers sur des sites strictement non commerciaux pour protéger les droits des créateurs.

Avez-vous le droit de photographier la pyramide du Louvre, et d'en publier l'image sur les réseaux sociaux ? Avez-vous le droit de vous prendre en photo devant la tour Eiffel illuminée en arrière-plan, et de diffuser le cliché ? C'était tout l'enjeu de la « liberté de panorama » qui était soumise à la discussion parlementaire dans le cadre du vote de la loi numérique. Et comme les députés avant eux, les sénateurs ont répondu non. Sauf à demander son avis à l'ayant-droit de l'oeuvre, il sera possible de diffuser des photos de bâtiments ou de sculptures protégées par le droit d'auteur, mais en les réservant aux seuls particuliers et à l'exclusion de tout usage à caractère directement ou indirectement commercial. Excluant de ce champ les associations, les sénateurs ont plongé Wikimedia (l'association qui a pour objet la diffusion de connaissance, via Wikipedia entre autres) dans un cauchemar sans fin : le site internet ne pourra désormais plus illustrer ses articles avec des photos des œuvres dont il parle.

Protéger la démarche artistique

L'objectif de cet amendement est d'empêcher un quidam de tirer un bénéfice financier de l'utilisation d'une photo d'une œuvre (même si c'est lui qui l'a prise) sans en avoir demandé l'autorisation aux ayants-droit de leur créateur, de manière à protéger la création. L'amendement concerne « les reproductions et représentations d'oeuvres architecturales et de sculptures, placées en permanence sur la voie publique », comme par exemple les illuminations de la tour Eiffel ou encore la pyramide du Louvre.

Mais les partisans d'une liberté totale de panorama pointent les restrictions considérables qu'apporte cet amendement. En effet, de tels clichés devenant interdits pour « tout usage à caractère directement ou indirectement commercial », ils seront désormais interdits de séjour sur les réseaux sociaux comme Facebook, Twitter ou Instagram. Il ne restera plus qu'à patienter jusqu'à ce que les œuvres tombent dans le domaine public (70 ans après la mort de l'artiste) pour partager entre amis un selfie touristique, ou bien créer un site internet personnel ne laissant aucune place à la publicité. Le nain de jardin d'Amélie Poulain, photographié devant les monuments du monde entier pour les besoins d'un film – commercial –, ne connaîtrait plus aujourd'hui le même fabuleux destin…. [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

Suivez-nous sur

Réagissez à cet article

Source : *Liberté de panorama : publier un selfie devant la pyramide du Louvre, est-ce du vol ?*

Une alerte à la bombe dans un

avion causée par un réseau Wi-Fi

Une alerte à la bombe dans un avion causée par un réseau Wi-Fi

Les passagers d'un vol interne australien ont eu une petite frayeur à cause d'un réseau WiFi.

Le réseau WiFi en question a été repéré par un des passagers qui, inquiet de ce nom étrange, en a tout de suite informé le personnel de bord. Ce dernier a alors remonté l'information jusqu'au commandant de bord, qui a décidé de garder l'avion au sol tant que l'appareil émetteur de ce réseau n'a pas été repéré. Une annonce retentit dans les hauts parleurs de l'avion afin de prévenir les passagers, mais après une demi-heure de recherche, la source n'est toujours pas localisée.
« Un réseau WiFi peut avoir une bonne portée, donc cela aurait pu venir d'une personne dans le terminal », explique un des passagers. Des recherches sont menées dans et autour de l'avion, sans résultat. Finalement, après trois heures d'attente sur le tarmac, l'avion se met finalement en route pour sa destination, Perth, en Australie, où il atterrit sans encombre 80 minutes plus tard... [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

Suivez-nous sur

Réagissez à cet article

Source : *Une alerte à la bombe dans un avion causée par un réseau Wi-Fi*

Les hackers privilégient le «drive-by download»

Les hackers privilégient le «drive-by download»

Les cybercriminels sont constamment à la recherche de possibilités d'infecter les appareils, selon un rapport paru jeudi.

MELANI a observé une augmentation des attaques contre des sites Web au deuxième semestre 2015. Les criminels sont constamment à la recherche de possibilités d'infecter commodément un maximum d'appareils de victimes potentielles.
Dans son rapport semestriel, publié jeudi, la Centrale d«enregistrement et d'analyse pour la sûreté de l«information (MELANI) constate que si les hackers privilégiaient par le passé l'envoi de courriels, qui demande peu de connaissances techniques, c'est désormais le «drive-by download» qui a la cote: il consiste à propager des logiciels malveillants (maliciels) à grande échelle, à travers des sites web très fréquentés.
Les portails des journaux et les réseaux publicitaires sont les cibles préférées des escrocs, explique MELANI. Une infection chez un fournisseur de contenu publicitaire peut se révéler lourde de conséquences, en infectant plus loin de nombreux sites clients.

Familles de maliciels

Au deuxième semestre de l'année dernière, l'extorsion est restée une des méthodes favorites des cybercriminels afin d'obtenir des gains rapides. Les familles de maliciels de cryptages sont toujours plus nombreuses, avertit MELANI. Les attaques DDoS (déni de service distribué), qui visent à rendre des sites inaccessibles pour ensuite exiger une rançon, se sont multipliées en 2015.
Les criminels choisissent avant tout des entreprises qui dépendent de l'accès à leur site Internet, car elles sont plus faciles à faire chanter. Sous la menace d'une éventuelle perturbation de l'accès à leur site, certaines sont prêtes à mettre la main au porte-monnaie. «Mais en payant, elles donnent aux hackers les moyens financiers pour renforcer leur infrastructure d'attaque et intensifier leurs actions», souligne la centrale.

En 2015, MELANI a ouvert le site «antiphishing.ch», qui permet à chacun de signaler des sites de hameçonnage. Quelque 2500 sites ont été dénoncés la première année. A côté du phishing par usage abusif du logo de l'administration fédérale, constaté plusieurs fois, le recours au phishing à l'aide de fichiers PDF est en recrudescence: au lieu d'un lien HTML, le courriel contient un fichier .pdf en annexe, qui lui-même incite à cliquer sur un lien malveillant.

Zurich et Valais

Comme au premier semestre 2015, Zurich et le Valais affichent au deuxième semestre un taux d«infection par habitant supérieur aux autres cantons. «Alors qu'à Zurich ce résultat tient à la forte densité d«ordinateurs, les raisons du taux d'infection élevé en Valais ne sont pas connues à l'heure actuelle», écrit MELANI dans son rapport.
Consultable en ligne, ce document permet de découvrir les innombrables techniques développées par les cybercriminels pour gagner de l'argent illégalement, et suggère des moyens pour se prémunir d'une attaque.
(ats)… [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

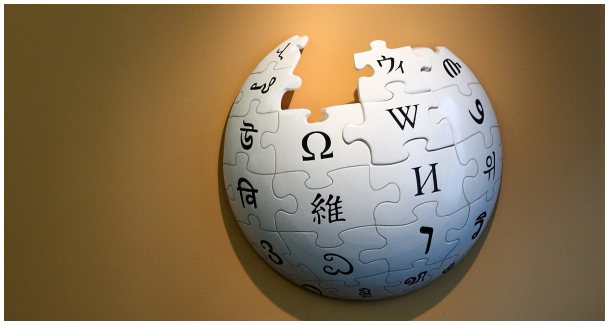
Contactez-nous

Suivez-nous sur

Réagissez à cet article

1. Source : *Les hackers privilégient le «drive-by download» – Tribune de Genève – l'actualité en direct: politique, sports, people, culture, économie, multimédia*

Les révélations de Snowden sur la NSA auraient miné la liberté de s'informer



Les révélations de Snowden sur la NSA auraient miné la liberté de s'informer

---

Selon une étude à paraître dans le Berkeley Technology Law Journal, le trafic des pages Wikipédia liées à des thématiques susceptibles d'attirer l'attention des autorités aurait chuté après les révélations d'Edward Snowden sur les programmes de surveillance massive.

La vie privée est la mère de beaucoup de libertés. Même s'il n'a rien à se reprocher, un individu qui se sait surveillé n'adoptera pas le même comportement que s'il se croit dans l'intimité, seul avec sa propre conscience. La crainte de donner la mauvaise impression sur soi ou d'attirer les suspicions incite à adopter des comportements qui écartent tout risque, et entrent dans une norme sociale. Il faut faire profil bas.
C'est donc un effet pervers attendu des révélations d'Edward Snowden sur les programmes de surveillance de la NSA, que de voir les individus changer de comportement, parce qu'ils ne savent plus très bien s'ils sont surveillés ou s'ils sont libres.
Certes, le principal effet a été d'accélérer le recours au chiffrement, ce que déplore la NSA. Mais selon l'agence Reuters, une étude qui doit être bientôt publiée dans une revue juridique de l'Université de Berkeley démontrerait aussi l'existence d'un lien entre les révélations de Snowden, et une chute de la fréquentation des pages d'informations qui n'ont rien d'illégales à consulter, mais qui peuvent attirer le soupçon des autorités.
L'étude qui doit encore être soumise à un examen par des pairs montrerait en effet que le trafic des pages Wikipédia qui concernent les groupes terroristes ou les outils qu'ils utilisent dans leurs actions aurait plongé de près de 30 %, à la suite de la découverte des programmes de surveillance massive.

bombe
L'universitaire Jonathon Penney, de l'Université de Toronto, a ainsi identifié 48 thématiques identifiées par le ministère des affaires intérieures des États-Unis, comme étant des sujets dignes d'intérêt pour traquer les terroristes sur les réseaux sociaux (le djihad, Al Quaida, la fabrication de bombe, l'État islamique, etc.). Corrélation n'est pas causalité, mais le chercheur a remarqué que dans les 16 mois précédent les premières révélations de Snowden en juin 2013, le trafic vers les pages liées à ces thématiques avait agumenté, passant de 2,2 millions de lectures à 3 millions, alors que dans les deux mois suivants, le trafic a soudainement chuté jusqu'à son niveau initial, avant de baisser encore jusqu'à 2 millions de visites, et de se stabiliser autour de 2,5 millions de vues par mois dans les 14 mois suivants.
Le trafic aurait particulièrement chuté sur les pages les plus sensibles, ce qui rejoint d'autres études qui ont montré, par exemple, que les recherches de mots clés sensibles auraient chuté de 5 % sur Google juste après les révélations d'Edward Snowden.
Cette étude démontre le risque pour la liberté d'expression identifié lors des débats sur les boîtes noires de la loi Renseignement censées détecter les comportements suspects sur Internet, sur la base d'algorithmes dont on ne sait évidemment rien, ce qui prête à tous les fantasmes et toutes les craintes. Bernard Cazeneuve avait expliqué qu'il « n'est pas question d'une surveillance de masse, mais bien d'un ciblage, sur des modes de communications et des services caractéristiques des personnes impliquées dans des activités terroristes ».

UN EFFET REDOUTÉ PAR LES EXPERTS DE L'ONU
En expliquant pourquoi ce dispositif est à nos yeux contraire aux droits de l'homme, nous avions en effet rappelé les propos du Haut commissariat aux droits de l'homme de l'Onu, Conscient du risque que la surveillance massive faisait peser sur la liberté des individus de s'informer, le HCDH avait prévenu que pour qu'une surveillance soit légale, il « ne suffit pas que les mesures soient ciblées pour trouver certaines aiguilles dans une botte de foin, ce qu'il convient d'examiner, c'est leur impact sur la botte de foin, au regard du risque de préjudice, c'est-à-dire déterminer si la mesure est nécessaire et proportionnée ».
Dans son rapport A/HCR/28/39, le Haut commissariat avait également cité ces propos de la Rapporteure spéciale sur la liberté d'expression auprès de la Commission interaméricaine des droits de l'homme :
Mme Botero a également fait observer que les politiques de surveillance pouvaient avoir une incidence sur un grand nombre de droits de l'homme. Elle a évoqué l'effet de la surveillance sur le droit à la liberté d'expression, lequel pouvait être soit direct, quand ce droit ne pouvait être exercé anonymement à cause d'une surveillance, soit indirect, quand la simple existence de mécanismes de surveillance pouvait avoir un effet paralysant, inspirer la crainte et inhiber les personnes concernées en les contraignant à la prudence dans leurs dires et leurs agissements. Le droit à la liberté d'expression étant un socle, y porter atteinte pouvait entraîner une violation d'autres droits tels que les libertés d'association, de réunion et de religion et le droit à la santé. Compte tenu de l'effet potentiel des activités de surveillance sur l'ensemble de l'architecture des droits de l'homme, il incombait aux États de revoir leur législation pour fixer les limites des programmes de surveillance en veillant à ce qu'ils soient conformes aux principes de nécessité et de proportionnalité et soient assortis de mécanismes de suivi appropriés.
C'est également le problème des mesures pénales qui visent à condamamner la simple lecture de sites terroristes, telle que celle votée le mois dernier au Sénat. Si le simple fait de s'informer est passible de sanctions, alors l'internaute devra toujours se demander si le site qu'il visite peut l'amener ou non à être poursuivi, et le doute profitera toujours à l'auto-censure… [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

Suivez nous sur

Réagissez à cet article

Source : *Les révélations de Snowden sur la NSA auraient miné la liberté de s'informer*

Des hackers proches de Daech

menacent les New-Yorkais

Des hackers proches de Daech menacent les New-Yorkais

Un groupe de hackers liés à Daech a dévoilé sur Internet une liste contenant les données personnelles de milliers de new-yorkais et a exhorté les adeptes du groupe à les cibler.

Les hackers ont mis en ligne non seulement les noms des New-Yorkais, mais aussi les lieux de résidence et leurs adresses électroniques, rapporte le Reuters, qui précise qu'une grande partie des données sont désuètes. En outre, la liste inclut les données personnelles d'un grand nombre de fonctionnaires du département d'Etat américain ainsi que de citoyens sans relations avec les services publics.
Des agents fédéraux et des policiers de New York ont contacté les personnes figurant sur la liste pour les informer, mais les forces de l'ordre ne considèrent pas cette menace comme crédible, indique la source.
« Bien que notre pratique courante consiste à refuser de commenter les questions opérationnelles et les enquêtes spécifiques, le FBI avertit régulièrement les individus et les organisations sur l'information recueillie au cours d'une enquête qui peut être perçue comme une menace potentielle », stipule la déclaration du FBI.
Précédemment, le groupe de pirates informatiques de Daech connu comme « Cyber-califat uni » a annoncé qu'il avait obtenu les informations personnelles de 50 employés du département d'Etat américain, y compris leurs noms et numéros de téléphones. Pour le prouver, les pirates ont publié des captures d'écran et ont menacé d' »écraser » les Etats-Unis, de tuer ces employés et de détruire le système de sécurité nationale. De son côté, le département d'Etat américain n'a fourni aucun commentaire.

Croyant attaquer Google, les hackers de Daech manquent leur cible
Auparavant, les Etats-Unis avaient ouvert une nouvelle ligne de combat contre l'Etat islamique, comprenant des attaques contre des réseaux informatiques de Daech. Des cyberattaques seront réalisées contre l'Etat islamique parallèlement à l'usage des armes traditionnelles.
Depuis 2013, les autorités américaines ont arrêté plus de 70 personnes pour collaboration avec l'Etat islamique… [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

Suivez nous sur

Réagissez à cet article

Source : *Des hackers proches de Daech menacent les New-Yorkais*

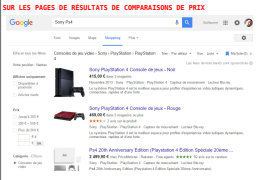
Comparateurs de prix : des obligations de transparence à partir du 1er juillet

Comparateurs de prix : des obligations de transparence à partir du 1er juillet

À compter du 1er juillet 2016, tous les comparateurs de prix sur internet devront s'astreindre à respecter un certain nombre de règles de transparence.

Le gouvernement a fait publier ce lundi au Journal Officiel un décret n° 2016-505 du 22 avril 2016 relatif aux obligations d'information sur les sites comparateurs en ligne, qui vient mettre en application une disposition de la loi Hamon. Cette dernière avait créé en 2014 un article L115-5 du code de la consommation, qui dispose que « toute personne dont l'activité consiste en la fourniture d'informations en ligne permettant la comparaison des prix et des caractéristiques de biens et de services proposés par des professionnels est tenue d'apporter une information loyale, claire et transparente, y compris sur ce qui relève de la publicité au sens de l'article 20 de la même loi ».

SUR LES PAGES DE RÉSULTATS DE COMPARAISONS DE PRIX



Le décret reprend l'essentiel de ce qui était déjà dans les codes de bonnes pratiques des comparateurs de prix, et qui devient désormais obligatoire. Ainsi à compter du 1er juillet 2016, tous les comparateurs de prix auront l'obligation d'afficher en haut de chaque page de résultats, avant la liste des prix :

1° Le critère de classement des offres utilisé par défaut ainsi que la définition de ce critère, sauf si le critère de classement utilisé par défaut est le prix. La définition est indiquée, à proximité du critère, par tout moyen approprié ;
2° Le caractère exhaustif ou non des offres de biens ou de services comparées et du nombre de sites ou d'entreprises référencés ;
3° Le caractère payant ou non du référencement.

Ils devront aussi informer les consommateurs sur les caractéristiques essentielles des biens ou services comparés, le prix total à payer par le consommateur, et les garanties commerciales offertes.
Si un marchand rémunère le comparateur de prix pour être placé plus haut dans les résultats que ce qu'il serait naturellement, le terme « Annonces » devra figurer sur la page, pour être conforme à l'article 20 de la loi pour la confiance dans l'économie numérique, qui impose d'indiquer comme telles les publicités.

SUR LE SITE INTERNET DU COMPARATEUR DE PRIX
En outre, les comparateurs devront aussi préciser leur mode de fonctionnement « dans une rubrique spécifique », « aisément accessible sur toutes les pages du site et matérialisée par une mention ou un signe distinctif ».

Ils devront au minimum préciser :
1° Les différents critères de classement des offres de biens et de services ainsi que leur définition ;
2° L'existence ou non d'une relation contractuelle ou de liens capitalistiques entre le site de comparaison et les professionnels référencés ;
3° L'existence ou non d'une rémunération du site par les professionnels référencés et, le cas échéant, l'impact de celle-ci sur le classement des offres ;
4° Le détail des éléments constitutifs du prix et la possibilité que des frais supplémentaires y soient ajoutés ;
5° Le cas échéant, la variation des garanties commerciales selon les produits comparés ;
6° Le caractère exhaustif ou non des offres de biens ou de services comparées et du nombre de sites ou d'entreprises référencés ;
7° La périodicité et la méthode d'actualisation des offres comparées.
Notez que pour une raison qui nous échappe, le décret fait systématiquement référence à l'article L111-6 du code de la consommation, relatif aux obligations générales d'information précontractuelles, plutôt qu'à l'article L111-5 qui vise plus spécifiquement les comparateurs de prix… [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

Suivez nous sur

Réagissez à cet article

Source : *Comparateurs de prix : des obligations de transparence à partir du 1er juillet*

Un casseur de 17 ans retrouvé par la police grâce à YouTube

Un casseur de 17 ans retrouvé par la police grâce à YouTube

Un jeune homme de 17 ans qui a participé au saccage du magasin Go Sport de Nantes en cachant son visage sous une capuche, a été appréhendé par la police. Il avait raconté les faits sur YouTube.

Tout ce que vous direz sur Internet pourra être retenu contre vous et heureusement, les imbéciles n'en ont pas toujours conscience. France 3 Pays-de-la-Loire rapporte ainsi que la police nantaise consulte les vidéos amateurs qui circulent notamment sur YouTube, dans lesquelles des casseurs sont visibles, voire celles dans lesquelles ils se vantent de leurs propres délits (ce qui arrive plus souvent qu'on ne l'imagine).
C'est ainsi que les policiers ont pu appréhender un jeune lycéen de 17 ans, qui s'était vanté sur une vidéo d'avoir « fait Go Sport la dernière fois » et d'avoir « eu des chaussures gratuites » en se servant dans la vitrine cassée de la boutique située à deux pas de la tour de Bretagne, au cœur de la métropole de Nantes. Le magasin de sport avait été vandalisé le 5 avril dernier et la vidéo avait été tournée après une nouvelle manifestation du 9 avril… [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

Suivez nous sur

Réagissez à cet article

Source : *Un casseur de 17 ans retrouvé par la police grâce à YouTube*