

Les outils techniques de la lutte anti-drone évoluent | Le Net Expert Informatique



Les outils techniques
de la lutte anti-drone
évoluent

Depuis octobre 2014, plusieurs dizaines de survols de sites sensibles par des drones ont été enregistrés. Des centrales nucléaires, des sites militaires ou encore le palais de l'Elysée ont été survolés par de petits engins difficiles à bloquer. Une mobilisation sans précédent a été lancée par le gouvernement et les entreprises. A l'occasion du Salon du Bourget, où des dizaines de drones civils et militaires sont présentées, 20 Minutes fait le point sur les outils techniques de la lutte anti-drones...

Vers une intégration de plusieurs dispositifs

Plusieurs systèmes regroupant des outils de détection, d'identification et d'interception sont en phase de développement. La société d'ingénierie JCPX Development a signé ce mercredi au Salon du Bourget un partenariat avec la direction des services de la navigation aérienne, Aveillant (groupe Altran), SkySoft et l'Ecole nationale de l'aviation civile (Enac) pour son système « Uwas – UAV Watch and Catch System ».

Ce dispositif comprend un radar pour détecter les engins volants, des caméras pour vérifier leur identité et les localiser, mais aussi des drones pour recueillir des données, voire les neutraliser grâce « à une claqué magnétique », explique le président de JCPX Jean-Christophe Draï.

Ce système succède à deux projets primés en mars par l'Agence nationale de la recherche pour le compte du Secrétariat général de la Défense et de la Sécurité nationale (SGDSN). Le premier, « Boreades », est développé par CS Systèmes d'information et deux PME. Il regroupe un système enregistrant la signature thermique du drone, le recueil de son image grâce à un réseau de caméras au sol, un leurre des repères GPS du drone, et une neutralisation de la télécommande de l'opérateur.

Des projets primés par l'Agence nationale de recherche

Le deuxième projet, « Angelas », est piloté par l'Onera, le centre français de recherche aérospatiale, dans le cadre d'un consortium réunissant trois industriels et quatre laboratoires publics de recherche. Ce dispositif recouvre la détection et l'identification des drones grâce à des caméras et des lasers, des équipements radars et acoustiques. Il peut utiliser le brouillage électronique.

Un brouillage des données de navigation (ondes radios, liaisons wi-fi, guidages par GPS) qui peut poser problème : « Le brouillage n'est pas directionnel. Dans la zone concernée, tout le monde le subit. Le GPS des voitures ne fonctionnera plus, les téléphones seront hors d'usage », relève Jean-Christophe Draï. La technique est difficilement utilisable en milieu urbain, où la chute d'un drone peut être dangereuse.

Le drone anti-drone

Une autre solution anti-drone est développée depuis plusieurs mois par l'entreprise française Malou Tech. Son drone « Intercepteur » fonce vers sa proie avant de la prendre dans ses filets. Mais selon une vidéo de présentation, un as du télépilotage semble pouvoir facilement échapper à ce drone anti-drone.

Le laser « tueur » de drone

Plusieurs pays, dont les Etats-Unis, la Chine et l'Allemagne ont développé des lasers anti-drones. La Chine paraît aujourd'hui en pointe dans ce domaine, avec un laser pouvant détruire, dans un rayon de deux kilomètres, des drones de petite taille. Cependant, ce système a ses limites : Difficilement utilisables par mauvais temps, les lasers ne sont pas adaptés au milieu urbain.

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.

Besoin d'informations complémentaires ?

Contactez-nous

Denis JACOPINI

Tel : 06 19 71 79 12

formateur n°93 84 03041 84

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure sécurité des systèmes informatiques et améliorer la protection juridique du chef d'entreprise.

Contactez-nous

Cet article vous plaît ? Partagez !

Un avis ? Laissez-nous un commentaire !

Source : <http://www.20minutes.fr/societe/1634983-20150618-survol-zones-sensibles-outils-techniques-lutte-anti-drone-evoluent>

Par Anne-Laëtitia Béraud

Les Samsung Galaxy vulnérables aux cyber- attaques | Le Net Expert Informatique



Twin Design /
Shutterstock.com

Les Samsung Galaxy
vulnérables aux cyber-
attaques

Les claviers virtuels SwiftKey, pré-installés sur les Samsung, pourraient être une porte ouverte pour les hackers. Une société de cybersécurité américaine a découvert une faille dans plus de 600 millions de portables.

Vous avez peut-être déjà été hacké

Le coupable : le clavier virtuel SwiftKey. Il appartient à la suite d'applications et de fonctionnalités que les Samsung rajoute à Android. Comme toute application, SwiftKey subit des mises à jour fréquentes. La société de cybersécurité NowSecure a découvert que lorsque le téléphone recherche des mises à jour à effectuer, il communique ouvertement, sans chiffrer sa requête.

Pour étayer leur dires, les chercheurs de NowSecure ont réussi à se faire passer pour le serveur qui envoie les mises à jour aux téléphones Samsung et à y injecter des programmes permettant d'exploiter les appareils à l'insu des utilisateurs. Peut-être que, sans le savoir, vous avez déjà été hacké.

Impossible à désinstaller

Cette vulnérabilité concerne les modèles Galaxy S4, S4 Mini, S5 et S6. Le problème étant que l'application SwiftKey fait partie des programmes de base livrés avec le téléphone, au même titre que les applications de Google. Il est donc impossible de la désinstaller.

En attendant que le problème soit réglé, NowSecure conseille aux utilisateurs d'« éviter les réseaux Wi-Fi non sécurisés », ou plus radicalement d'« utiliser un autre appareil mobile ». Samsung a lui annoncé une future mise à jour de sa solution de sécurité Knox, pour combler cette faille.

Actuellement, un hacker s'attaquant à votre téléphone pourrait avoir accès aux capteurs et aux ressources comme le GPS, l'appareil photo et le micro, installer secrètement des applications malveillantes, espionner les messages entrants et sortants ou les appels ou encore tenter d'accéder à des données personnelles sensibles comme les photos ou les textos.

Qu'en est-il en France ?

Contactée par Le Figaro, la société NowSecure confirme que le phénomène est « mondial », et donc que la France est concernée. Elle a notifié cette faille à Samsung en décembre 2014, ainsi qu'à l'équipe de sécurité d'Android.

Si Samsung a publié un correctif début 2015, « on ne sait pas si les opérateurs téléphoniques ont implémenté ce correctif dans les appareils de leurs réseaux », explique NowSecure. L'entreprise n'a diffusé qu'une liste des opérateurs touchés aux États-Unis.

En France, seul Bouygues Télécom a pour l'instant été en mesure de fournir une réponse des plus inquiétantes, assurant que « Samsung n'a jamais fait remonter le problème à nos équipes techniques » et qu'il est désormais « très sérieusement à l'étude ».

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.

Besoin d'informations complémentaires ?

Contactez-nous

Denis JACOPINI

Tel : 06 19 71 79 12

formateur n°93 84 03041 84

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure sécurité des systèmes informatiques et améliorer la protection juridique du chef d'entreprise.

Contactez-nous

Cet article vous plait ? Partagez !

Un avis ? Laissez-nous un commentaire !


Source : <http://news.radins.com/actualites/les-samsung-galaxy-vulnerables-aux-cyber-attaques,13394.html>

La vidéosurveillance de la ville auditée par un Infirmier | Le Net Expert Informatique

La
vidéosurveillance
de la ville
auditée par un
Infirmier



Amazon pourrait vous proposer de devenir livreur | Le Net Expert Informatique



Amazon pourrait vous proposer de devenir livreur

Après les drones, l'impression 3D et les coffres de voitures, Amazon cherche de nouveaux moyens de livrer rapidement un colis. Le groupe américain pourrait permettre à n'importe qui de livrer un produit.

Devenir livreur occasionnel, voilà ce que pourrait prochainement proposer Amazon. Le groupe américain réfléchirait à un nouveau moyen de conduire un colis d'un point A vers un point B. Baptisé en interne « Sur ma route », le dispositif s'ouvrirait à n'importe quelle personne.

Selon le Wall Street Journal, ceux qui désireraient devenir livreur d'un jour disposeraient d'une application mobile. Cet outil sera chargé de recenser les personnes qui attendent leur colis et les lieux qui disposent d'une commande en attente. On pense par exemple aux points relais ou à d'autres intermédiaires.

Cet outil soulève naturellement des questions quant à la sélection des livreurs. A l'instar d'Uber ou d'eBay, Amazon pourrait introduire un système de notation des personnes participantes. Néanmoins, la question de la responsabilité en cas de perte du colis reste entière.

La problématique du paiement des livreurs occasionnels est également importante. Amazon devra en effet les inciter à participer sans que cela fasse grimper la facture globale. L'an dernier, le groupe avait testé la livraison par le biais des véhicules Uber et des conducteurs de taxis en facturant 5 dollars le transport de chaque colis. L'expérience s'est toutefois arrêtée à l'état de test dans la seule ville de San Francisco.

Nous organisons régulièrement des actions de sensibilisation ou de formation au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.

Besoin d'informations complémentaires ?
Contactez-nous
Denis JACOPINI
Tel : 06 19 71 79 12
formateur n°93 84 03041 04

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en cybercriminalité et en déclarations à la CNIL, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la formation de vos salariés afin de leur enseigner les bonnes pratiques pour assurer une meilleure sécurité des systèmes informatiques et améliorer la protection juridique du chef d'entreprise.

Contactez-nous

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

S u r c e
http://pro.clubic.com/entreprises/amazon/actualite-770702-amazon-livraison.html?&src_node=M&src_campaign=M_clubicPro_News_10/06/2015&partner=&src_position=1024725737&src_misc=&srcID=039453874_1024725737&estat_url=http%3A%2F%2Fpro.clubic.com%2Fentreprises%2Famazon%2Factualite-770702-amazon-livraison.html


Quelques conseils pour préserver votre e-réputation | Le Net Expert Informatique



Quelques conseils pour préserver
votre e-réputation

<p>Sur le web, rien ne se perd. Toutes les données qui vous concernent sont potentiellement accessibles par tous. Or il s'agisse des photographies de votre vie étudiante festive, des archives du blog que vous aviez tenu lors d'un voyage à l'étranger, de votre participation sur la liste électorale d'un parti politique sulfureux lors d'élections locales ou encore du jugement relatant une condamnation pénale : vous laissez des traces.</p> <p>Celles-ci peuvent se révéler encombrantes. Comment faire pour qu'elles soient déréférencées des moteurs de recherche et ainsi rendues inaccessibles ?</p> <p>Tout d'abord, il peut être utile de consacrer quelques minutes au paramétrage de la confidentialité de son compte sur les réseaux sociaux, afin de préserver le caractère privé de ses publications. Celles-ci ne seront alors pas accessibles par le biais des moteurs de recherche mais réservées à vos amis et relations.</p> <p>Dans le cas où le contenu visé est publié sur un site web tiers, tel qu'un éditeur de presse, un blog ou un forum de discussion, il est possible de demander sa suppression en s'adressant directement à l'éditeur du site concerné ou, lorsque celui-ci ne réagit pas ou n'a pu être identifié, à l'hébergeur (qui assure le stockage du site sur ses serveurs).</p> <p>En cas d'échec de cette démarche, les moteurs de recherche pourront être sollicités au titre du droit à l'oubli, par le biais des différents formulaires qu'ils proposent désormais [1].</p> <p>Les principaux refus opposés par les moteurs de recherche sont justifiés par le fait que l'information litigieuse est toujours d'actualité, qu'elle ne concerne pas une personne physique, que l'internaute est un personnage public ou que le plaignant est un personnage public.</p> <p>En dernier recours, le Tribunal compétent pourra être saisi. Attention toutefois, le juge saisi analyse en détail la demande présentée afin de s'assurer qu'elle ne porte pas atteinte à la liberté d'information du public. Ainsi, le Tribunal de grande instance de Paris a rejeté une demande de suppression et de désindexation d'un article en ligne du quotidien 20 Minutes [2]. L'article litigieux, accessible sur le site internet du quotidien, intitulé « Un cavalier accusé de viol », relatait le placement en garde à vue d'un cavalier de niveau international soupçonné d'être impliqué dans le viol d'une stagiaire.</p> <p>Les juges ont rejeté la demande de droit à l'oubli, en faisant prévaloir la liberté d'information et l'intérêt légitime à divulguer des informations visant une personne exerçant une profession faisant appel au public et encadrant une activité proposée, notamment, à des enfants.</p> <p>Au contraire, dans une décision précédente, la même juridiction avait ordonné à la société Google de retirer de ses résultats de recherche un lien vers un article du Parisien évoquant la condamnation, datant de 2006, d'une internaute pour escroquerie à une peine de trois ans de prison dont trois mois fermes. La plaignante, à la recherche d'un emploi, s'était tournée vers la Justice à la suite du refus préalablement opposé par le géant américain.</p> <p>Lorsque votre demande est rejetée par le tribunal saisi, il reste possible de faire appel à des structures spécialisées qui tenteront de renvoyer au-delà de la troisième page de résultats, le contenu qui vous gêne.</p> <p>À l'heure où de plus en plus de plateformes proposent aux internautes de redevenir propriétaires de leurs données personnelles et de gagner de l'argent en louant leurs profils [3] aux marques et annonceurs, il est plus que jamais important de permettre aux internautes de retrouver la maîtrise de leur e-réputation.</p>
<p>Nous organisons régulièrement des actions de sensibilisation ou de formation au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.</p> <p>Besoin d'informations complémentaires ?</p> <p>Contactez-nous</p> <p>Denis JACOPINI</p> <p>Tel : 06 19 71 79 12</p> <p>formateur n°93 84 03041 84</p>
<p>Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en cybercriminalité et en déclarations à la CNIL, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la formation de vos salariés afin de leur enseigner les bonnes pratiques pour assurer une meilleure sécurité des systèmes informatiques et améliorer la protection juridique du chef d'entreprise.</p> <p>Contactez-nous</p>
<p>Cet article vous plaît ? Partagez !</p> <p>Un avis ? Laissez-nous un commentaire !</p> <p>Source : http://www.village-justice.com/articles/Quelques-conseils-pour-preserver,19708.html</p>

3D Prod, le nouveau site web qui vous permet d'imprimer en 3D vos pièces en vous donnant accès à toutes les technologies industrielles actuelles | Le Net Expert Informatique

	3D Prod, le nouveau site web qui vous permet d'imprimer en 3D vos pièces en vous donnant accès à toutes les technologies industrielles actuelles
---	--

L'impression 3D professionnelle maintenant accessible en 3 clics 3D Prod démocratise l'impression 3D professionnelle grâce à son nouveau site internet www.3dprod.com. Toutes les solutions actuelles d'impression 3D sont maintenant accessibles à travers une interface de commande entièrement en ligne.

Après avoir uploadé un ou plusieurs fichiers 3D, le visiteur sélectionne la technologie d'impression qu'il souhaite appliquer (stéréolithographie, frittage laser de poudres, multi-jets ou dépôt de fils). Il précise ensuite les matériaux qui doivent être utilisés ainsi que les finitions qu'il souhaite apporter à ses pièces. Un prix et une date de livraison sont instantanément calculés en fonction des options choisies. Le client peut ensuite régler en ligne et faire livrer ses pièces à l'adresse de son choix.

Cette nouvelle interface facilite également les achats groupés, contenant plusieurs impressions distinctes. Il est ainsi possible de préciser des matériaux et finitions spécifiques pour chacune des pièces appartenant à une même commande.

Ce service est aujourd'hui disponible en France et sera bientôt déployé dans d'autres pays d'Europe.

A propos de 3D Prod :

Depuis 2005, 3D Prod développe son savoir-faire dans le domaine de l'impression 3D et réalise des prototypes, maquettes et petites séries pour les professionnels de nombreux secteurs, tels que l'industrie, le design ou encore l'architecture. 3D Prod maîtrise l'ensemble des solutions actuelles d'impression 3D, notamment la stéréolithographie, le frittage laser de poudres, le multi-jets ou encore le dépôt de fils. Ces technologies lui permettent de proposer un large éventail de rendus dans des délais réduits et à des coûts maîtrisés. Entreprise à la pointe des technologies actuelles, 3D Prod se réinvente en permanence afin de disposer des dernières avancées technologiques et proposer à ses clients les solutions les plus adaptées. Le développement de cette nouvelle interface de commande en ligne s'inscrit précisément dans cette démarche.

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.

Besoin d'informations complémentaires ?

Contactez-nous

Denis JACOPINI

Tel : 06 19 71 79 12

formateur n°93 84 03041 84

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure sécurité des systèmes informatiques et améliorer la protection juridique du chef d'entreprise.

Contactez-nous

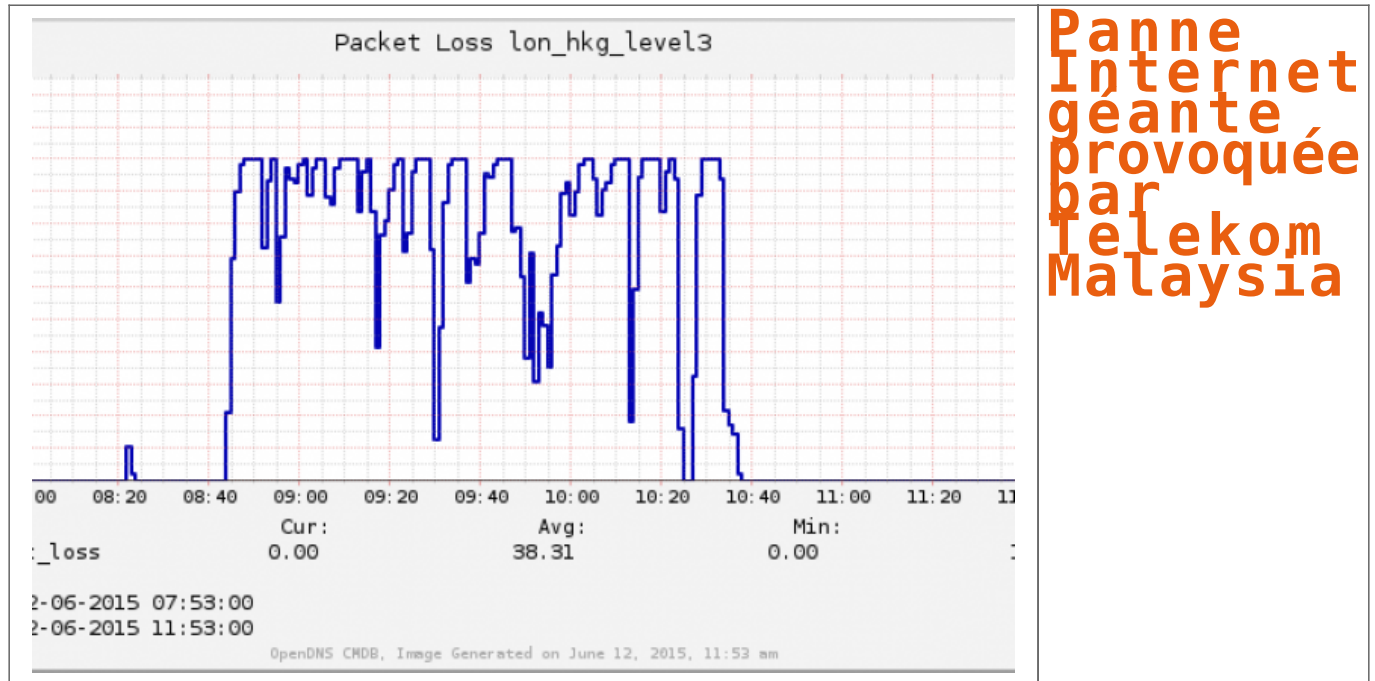
Cet article vous plait ? Partagez !

Un avis ? Laissez-nous un commentaire !

Source :

<http://www.lyon-communiques.com/communiques/3d-prod-le-nouveau-site-web-qui-vous-permet-d-imprimer-c122529.htm>

Panne Internet géante provoquée par Telekom Malaysia | Le Net Expert Informatique



Panne
Internet
géante
provoquée
par
Telekom
Malaysia

Comme en mars dernier, un opérateur a ralenti et même bloqué les requêtes IP d'un très grand nombre d'Internautes dans le monde entier et en France vendredi matin.

L'analogie du papillon trouve une nouvelle fois un débouché sur le secteur des télécoms. Des erreurs de routage BGP de l'opérateur Telekom Malaysia ont ralenti et même bloqué certains services Internet en France dans la matinée. Ce type d'erreur est courant sur le réseau des réseaux. En mars dernier c'est le FAI indien Hathway qui avait semé la panique. L'événement déclenché ce matin par l'opérateur malaisien a entraîné des pertes de paquets IP significatives dans toutes les parties du monde. Le réseau IP a connu une dégradation sévère entre la région Asie-Pacifique et le reste du monde quand Telekom Malaysia a commencé à transférer des requêtes erronées (près de 200000) à Level 3, un géant de l'Internet. Le service est revenu à la normal en fin de matinée.

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.

Besoin d'informations complémentaires ?

Contactez-nous

Denis JACOPINI

Tel : 06 19 71 79 12

formateur n°93 84 03041 84

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure sécurité des systèmes informatiques et améliorer la protection juridique du chef d'entreprise.

Contactez-nous

Cet article vous plait ? Partagez !

Un avis ? Laissez-nous un commentaire !

Source

<http://www.lemondeinformatique.fr/actualites/lire-france-la-panne-internet-geante-provoquee-par-telekom-malaysia-61465.html>

Par Serge Leblal

Des hôtels suisses victimes d'un piratage informatique. Le Wifi était-il sûr ? | Le Net Expert Informatique



Selon le groupe de sécurité informatique russe, Kaspersky, le logiciel d'espionnage « Duqu » a déjà servi à une cyberattaque en 2011. Crédit

Reuters

Des hôtels suisses
victimes d'un piratage
informatique. Le Wifi
était-il sûr ?

Nous vous avons déjà alerté sur les risques que pouvaient entraîner l'usage des Wifi public ou bien les Wifi ouverts des hôtels (cf : Est-il risqué de se connecter au wifi public ?). Voici ci-dessous exemple concret, par Atlantico, de mise en application par les pirates d'opérations d'espionnage en utilisant ces moyens de communications certes gratuits, mais non garantis en terme de sécurité et de confidentialité.

Denis JACOPINI

Les établissements qui ont abrité les négociations du P5+1 auraient été la cible de cyber-attaques, selon l'entreprise de sécurité informatique Kaspersky. Le Ministère public de la Confédération a ouvert une procédure pénale contre X.

Selon le groupe de sécurité informatique russe, Kaspersky, le logiciel d'espionnage « Duqu » a déjà servi à une cyberattaque en 2011.

Le porte-parole du Ministère public de la Confédération (MPC) André Marty a confirmé qu'une perquisition a été menée dans un hôtel genevois le 12 mai dernier et que du matériel informatique a été confisqué. « Le but de cette perquisition était d'une part de mettre à l'abri des informations et d'autre part de constater si des systèmes informatiques ont pu être infectés par des virus. »

Le MPC, qui soupçonne une activité interdite d'un service de renseignement étranger, a ouvert une procédure pénale contre X. L'entreprise de sécurité informatique Kaspersky affirme avoir découvert un virus espion très sophistiqué qui aurait touché trois des hôtels ayant accueilli les négociations sur le nucléaire iranien. L'Intercontinental et le Palais Wilson à Genève, le Beau Rivage à Lausanne ou le Royal Plaza à Montreux sont potentiellement des cibles de cette attaque. Et ces trois établissements ont un point commun : l'accueil des négociations sur le nucléaire iranien.

Selon le groupe de sécurité informatique russe, Kaspersky, le logiciel d'espionnage « Duqu » a déjà servi à une cyberattaque en 2011, montrant des similarités avec Stuxnet, un « ver » informatique qui a en partie saboté le programme nucléaire iranien en 2009-2010 en détruisant un millier de centrifugeuses servant à produire de l'uranium enrichi. Une autre attaque imputable à « Duqu », ajoute Kaspersky, est liée aux cérémonies du 70e anniversaire de la libération du camp d'Auschwitz-Birkenau, en janvier de cette année. Plusieurs chefs d'Etat et de gouvernement étaient présents.

Le P5+1 réunit les Etats-Unis, la Chine, la Russie, la France, la Grande-Bretagne, les cinq membres permanents du Conseil de sécurité des Nations unies, et l'Allemagne. « Les informations internationales sur l'implication d'Israël dans cette affaire sont sans fondement », a déclaré la vice-ministre des Transports Tzipi Hotovely. « Ce qui est beaucoup plus important », a-t-elle ajouté, « c'est d'empêcher un mauvais accord où au final, nous nous retrouvons avec un parapluie nucléaire iranien. »

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.

Besoin d'informations complémentaires ?

Contactez-nous

Denis JACOPINI

Tel : 06 19 71 79 12

formateur n°93 84 03041 84

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure sécurité des systèmes informatiques et améliorer la protection juridique du chef d'entreprise.

Contactez-nous

Cet article vous plait ? Partagez !

Un avis ? Laissez-nous un commentaire !

Source

<http://www.atlantico.fr/pepites/nucleaire-iranien-hotels-suissees-victimes-piratage-informatique-logiciel-duqu-2189164.html>

L'histoire d' « Internet de l'époque » avec Norman | Le Net Expert Informatique



L'histoire d' « Internet de l'époque » avec Norman

Dans sa dernière vidéo l'« internet de l'époque », le célèbre Youtubeur Norman Thavaud s'amuse en chanson à comparer l'Internet d'aujourd'hui à celui des années 90 et début 2000.

Pour sa dernière création, Norman sort de son appartement et enrôle avec lui d'autres célèbres Youtubeurs (Hugo tout seul, Cyprien, Natoo...). L'idée : faire un clip musical qui compare les débuts du web à aujourd'hui.

Le clip, réalisé dans un style « rétro », évoque de nombreux souvenirs comme MSN, Skyblog,... mais aussi le rappeur Kamini, qui fait une apparition, connu pour son tube « Marly-Gomont », un tabac sur YouTube en 2006.

Lire la suite...

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.

Besoin d'informations complémentaires ?

Contactez-nous

Denis JACOPINI

Tel : 06 19 71 79 12

formateur n°93 84 03041 84

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure sécurité des systèmes informatiques et améliorer la protection juridique du chef d'entreprise.

Contactez-nous

Cet article vous plait ? Partagez !

Un avis ? Laissez-nous un commentaire !

Source

<http://jactiv.ouest-france.fr/actualites/spotted/video-norman-retrace-lhistoire-internet-avec-humour-47604>

Par Guirec FLECHER.

Conférence Octopus 2015 sur la cybercriminalité : Le Conseil de l'Europe se penche sur l'accès de la justice aux données | Le Net Expert Informatique

<input type="checkbox"/>	Conférence Octopus 2015 sur la
<input type="checkbox"/>	cybercriminalité : Le Conseil de
	l'Europe se penche sur l'accès de la
	justice aux données

Comment assurer l'accès aux données, enquêter efficacement sur les infractions commises par le biais d'Internet et engager des poursuites à l'encontre de leurs auteurs lorsque les éléments de preuve se trouvent dans le « cloud » ? Du 17 au 19 juin, le Conseil de l'Europe réunira des experts du monde entier, des responsables gouvernementaux, des fonctionnaires de police et des professionnels d'internet en vue de renforcer la coopération internationale pour lutter contre la cybercriminalité.

Cette conférence portera également sur les défis liés à la protection des enfants contre leur sollicitation en ligne à des fins sexuelles (« grooming ») et sur la radicalisation sur internet.

Les 300 participants examineront, dans le cadre d'une série d'ateliers partiellement ouverts à la presse, les questions suivantes :

- Le renforcement des capacités en matière de cybercriminalité: bonnes pratiques et futurs programmes (*)
- Les preuves électroniques : accès de la justice pénale aux données
- Les victimes de la cybercriminalité: qui s'en soucie ? (*)
- La législation en matière de cybercriminalité et la mise en œuvre de la Convention de Budapest
- La coopération internationale: améliorer le fonctionnement des points de contact accessibles 24 heures sur 24 et sept jours sur sept
- Les modes opératoires normalisés pour le traitement des preuves électroniques
- Les politiques, activités et initiatives adoptées en matière de cybercriminalité par les organisations internationales et les organisations du secteur privé
- La radicalisation sur internet : le point de vue de la justice pénale
- La protection des enfants contre la violence sexuelle en ligne

Les discussions s'appuieront notamment sur un rapport publié récemment et qui se penche sur les difficultés des autorités pénales à obtenir des preuves électroniques.

La conférence sera ouverte notamment par le Secrétaire Général du Conseil de l'Europe, Thorbjørn Jagland, la Représentante Spéciale du Secrétaire Général des Nations Unies sur la violence à l'encontre des enfants, Marta Santos Pais, et le Préfet chargé de la lutte contre les cybermenaces (France), Jean-Yves Latournerie.

Contexte

La Convention sur la cybercriminalité (« Convention de Budapest ») est le seul traité international juridiquement contraignant dans ce domaine. Elle a eu des répercussions dans le monde entier, où elle a conduit au renforcement et à une plus grande harmonisation de la législation relative à la cybercriminalité.

Depuis 2001, 66 pays ont signé, ratifié ou ont été invités à adhérer à la Convention. Plus de 120 pays coopèrent avec le Conseil de l'Europe au renforcement de leur législation et de leur capacité de lutte contre la cybercriminalité.

Programme – Fiche d'information – Encore plus d'information

Lien vers la retransmission (17 juin de 9h à 12h30 dans l'hémicycle et discussions en salle 1) #octopus2015

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.

Besoin d'informations complémentaires ?

Contactez-nous

Denis JACOPINI

Tel : 06 19 71 79 12

formateur n°93 84 03041 84

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure sécurité des systèmes informatiques et améliorer la protection juridique du chef d'entreprise.

Contactez-nous

Cet article vous plaît ? Partagez !

Un avis ? Laissez-nous un commentaire !

Source

<http://www.itchannel.info/index.php/articles/156460/conference-octopus-2015-cybercriminalite-conseil-europe-penche-acces-justice-donnees.html>