Les moyens de preuves sur Internet | Le Net Expert Informatique

Les moyens de preuves sur Internet

La récente décision de la Cour d'appel de Paris du 9 octobre 2015 rappelle une fois de plus le caractère essentiel de constituer des preuves valables avant d'agir en justice, particulièrement sur Internet. En l'espèce, la société éditrice du site « Onvasortir.com » attaquait en parasitisme la société éditrice du site « dailyfriends.com » pour avoir copié le plan, la structure, les fonctionnalités, l'agencement des rubriques et le contenu de son site internet.

Afin de rendre sa décision, la Cour s'est appuyée sur des copies écran (des sites en question et d'un forum de discussion), dont la valeur probante était contestée par la partie adverse, mais que la Cour a jugé recevable dans la mesure où elles étaient « parfaitement nettes et datée ». En revanche, la Cour a rejeté un constat d'huissier du fait que l'officier ministériel avait dissimulé son identité lors de ses constats en se connectant aux sites via le compte de la société.
Que ce soit pour un site internet ou une application sur smartphone, la constitution de preuves, souvent difficiles à obtenir et pas toujours recevables, est pourtant essentielle à :
La caractérisation du délit (et donc la condamnation) ;
L'évaluation du préjudice (et donc des dommages-intérêts).

Si la preuve est libre en matière de concurrence déloyale ou de contrefaçon, toutes les preuves ne sont pas admissibles, comme en atteste cette décision, et leur force probante variable. Cet arrêt est donc l'occasion de revenir sur les règles en la matière, avec la particularité de la preuve sur Internet.

I – Les moyens de preuve irrecevables

Au préalable, il n'est pas inutile de rappeler que seules les preuves « légalement admissibles » pourront être retenues devant un tribunal.
Ainsi, il faut entendre par « légalement admissible », les preuves qui ne relèvent pas d'une obtention irrégulière telles que : les écoutes téléphoniques, la violation du secret des correspondances, la réalisation d'un constat en dehors des heures légales ou encore l'atteinte à un principe fondamental tel que la vie privée, le secret professionnel ou le secret de fabrique.
Ainsi, la Cour de cassation, par un arrêt de principe en son assemblé plénière du 7 janvier 2011 a énoncé que « l'enregistrement d'une communication téléphonique réalisé à l'insu de l'auteur des propos tenus constitue un procédé déloyal rendant irrecevable sa production à titre de preuve ».

C'est également sur ce fondement que dans sa décision la Cour d'appel a rejeté le constat dressé par l'huissier de justice qui n'a pas dévoilé son identité en se connectant au site mais a utilisé les identifiants de compte d'un tiers.

II – Les moyens de preuves sur Internet

Il existe plusieurs moyens de preuves visant à faire constater un usage sur Internet dont la force probante est plus ou moins importante.

A) Le constat d'huissier

Une fois établie et validée, cette preuve a une grande force probante.
Ainsi, l'huissier peut procéder à des constations sur Internet à la requête des particuliers. Il a cependant un rôle de simple observateur puisqu'il doit se borner à effectuer des constations purement matérielles.

Le constat sur Internet a cependant posé la question des limites de ce qu'il pouvait constater.
Constat d'un site internet ou d'une application sur smartphone : Sous réserve de respecter certaines conditions techniques (vider le dossier cache du navigateur, absence de serveur proxy…), l'huissier peut faire une description des sites internet accessibles au public, et notamment des produits argués de contrefaçon, et des captures écran des pages du site.

Constat d'achat sur internet : Cette pratique a posé certaines questions en cas de commande sur internet par l'huissier de produits litigieux.
Certains arrêts avaient admis qu'un huissier puisse commander un produit sur un site internet afin d'établir un constat d'achat aux vues de constituer une preuve de la contrefaçon. Cependant, des arrêts, plus récents [1] ont contesté la licéité de cette pratique au motif que l'huissier s'était engagé activement par l'ouverture d'un compte client et l'acquisition du produit litigieux, et avait ainsi outrepassé ses pouvoirs de simple constatation.

C'est en ce sens que va l'arrêt du 7 octobre 2015, qui a dénié toute validité au constat d'huissier qui n'avait indiqué ni sa qualité ni son identité en se connectant au site.
Pour acheter un produit sur internet, l'huissier doit impérativement et comme en matière de constat achat dans les magasins, décliner de manière claire et visible son identité et sa qualité avant de procéder à un acte d'achat. Certaines décisions ont cependant, admis que le seul fait de faire libeller la facture au nom de l'huissier était suffisant pour identifier l'huissier [2].

Sauf à y être expressément autorisé, l'huissier n'a pas le droit d'ouvrir un compte client et, d'acquérir à dessein, un produit allégué de contrefaçon [3].
Le site internet est assimilé à un magasin, comme un lieu privé et, sans autorisation du juge, l'huissier ne peut procéder à ses constatations que depuis la voie publique. Peut-être pourra-t-on procéder comme en matière de constat d'achat en magasin c'est-à-dire, faire procéder à l'ouverture d'un compte client par un tiers sous surveillance de l'huissier qui constatera les démarches effectuées dans le but d'acheter le produit incriminé ? Il faudra également que l'huissier soit présent lors de la réception du colis…ce qui complique les choses.

B) Le constat par un agent assermenté

Il consiste en la description par un agent assermenté d'un acte de contrefaçon. Il pourra être demandé à l'Agence pour la Protection des Programmes (APP) qui dispose d'agents assermentés.
Ce moyen de preuve est particulièrement utilisé en matière de droit d'auteur et de droits voisins et a été admis en matière de propriété industrielle. Ces constats peuvent servir à contourner la difficulté des achats sur internet effectués par un huissier.
Néanmoins, ces constats n'ont pas la force probante des constats effectués par un officier ministériel, et sont par conséquent soumis à l'appréciation souveraine du tribunal.

C) La copie-écran

Enfin, la copie-écran peut également être pertinente même si elle a une force probante moindre, elle représente une bonne solution pour étayer un constat d'huissier ou lorsqu'un constat d'huissier est invalidé comme dans la présente décision du 9 octobre 2015.

Il est donc impératif de connaître les limites d'investigations de l'huissier pour ne pas se voir déclarer irrecevable le constat. Le droit, à l'origine applicable à la vie réelle, essaie tant bien que mal de s'adapter aux contraintes et aux particularités du monde virtuel, et les constats d'huissier ne font pas exception. Attention donc à bien connaître ces spécificités avant d'intenter toute action au fond !

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

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

Source : http://www.village-justice.com/articles/Les-moyens-preuves-sur-Internet,20821.html
Colombe Dougnac – Conseil en Propriété Industrielle

Plus de 2 millions d’internautes victimes de phishing en 2015 | Le Net Expert Informatique

Plus de 2 millions d’internautes victimes de phishing en 2015

Pour renforcer la lutte contre le phishing, le Ministère de l'Intérieur a signé le 5 novembre, une convention de partenariat avec l'association Phishing Initiative, soutenue par Lexsi et Microsoft France. Cet accord vise à mutualiser les informations entre sa propre plateforme, PHAROS, et celle de Phishing Initiative qui a identifié de son côté plus de 150 000 adresses uniques de sites frauduleux visant la France depuis sa création en 2011.

Une convention commune pour renforcer la lutte contre le Phishing

En signant la convention de lutte anti-phishing, Catherine Chambon, sous-directeur de la lutte contre la cybercriminalité et Jérôme Robert, président de Phishing Initiative souhaitent renforcer la sensibilisation des internautes aux risques liés à cette malveillance majeure. « La complémentarité de nos actions rend évidente la nécessité d'un rapprochement et d'une coordination entre nos deux organisations », explique Jérôme Robert. « PHAROS et Phishing Initiative opèrent en effet tous deux des plateformes de signalement à destination du grand public. Il est par conséquent possible d'instaurer des conditions de partage de l'information de manière à optimiser d'une part, la recherche de données et d'autre part, la protection de l'internaute. »

Suite à la signature de cette convention et à l'engagement des parties prenantes, le Ministère de l'Intérieur et Phishing Initiative travailleront également à la rédaction d'un rapport commun et à l'élaboration d'un suivi des tendances au service de la protection des internautes.

Phishing Initiative et PHAROS : l'union des expertises

Elaborée et construite sous l'impulsion de Madame Catherine Chambon, Madame Valérie Maldonado, chef de l'OCLCTIC, Messieurs Jérôme Robert, Directeur Marketing, Vincent Hinderer, Expert Cybersécurité chez Lexsi, et Bernard Ourghanlian, directeur technique et sécurité de Microsoft, la convention a pour objectif d'augmenter le nombre d'URLs traitées et analysées. Avec respectivement 60 000 et 30 000 URLs traitées depuis début 2015, Phishing Initiative et PHAROS unissent leurs forces pour protéger les internautes et rendre le web plus sûr. « L'association de nos dispositifs de lutte contre la fraude sur Internet représente une avancée majeure dans la protection des particuliers comme des entreprises » précise Bernard Ourghanlian de Microsoft France. « Face à la malveillance et à la fraude organisée, chaque citoyen et chaque entreprise est acteur d'un Internet plus sûr au bénéfice de tous. » La Sous-Direction de la Lutte contre la Cybercriminalité (SDLC) a développé deux dispositifs destinés aux particuliers : la Plateforme d'Harmonisation d'Analyse et de Recoupement et d'Orientation des Signalements (PHAROS), lancée en janvier 2009, et Info-Escroqueries, une hotline téléphonique dédiée aux arnaques. PHAROS a notamment pour mission de recueillir et traiter les signalements de contenus et de comportements illicites détectés sur Internet.

Phishing Initiative, un programme de lutte européen

Cofinancé par le Programme de Prévention et de Lutte contre le Crime de l'Union Européenne, Phishing Initiative offre à tout internaute la possibilité de lutter contre les attaques d'hameçonnage en signalant de manière simple les liens lui paraissant suspects en un clic sur www.phishing-initiative.fr .

Chaque signalement fait l'objet d'une analyse par les experts Lexsi qui, s'il se révèle frauduleux, est transmis aux partenaires de Phishing Initiative, notamment Microsoft. Ces derniers enrichissent alors leurs listes noires, de sorte que le lien frauduleux est bloqué par les principaux navigateurs Web (Edge, Internet Explorer, Chrome, Firefox et Safari).

Phishing Initiative en chiffres

A ce jour, plus de 400 000 adresses suspectes ont été signalées dans le cadre de la Phishing Initiative, dont plus de 300 000 uniques. Depuis le début de l'année 2015, 110 000 signalements ont déjà été transmis, représentant plus de 60 000 nouvelles adresses uniques. Parmi elles, plus de 35 000 URLs uniques ont été confirmées comme faisant partie d'une campagne de phishing, soit près de 120 adresses distinctes par jour. A noter que le temps médian nécessaire aux analystes pour catégoriser un nouveau cas signalé est de moins de 20 minutes. Microsoft rafraîchit sa liste noire toutes les 20 minutes au sein d'Internet Explorer et Edge, ce qui protège en moyenne les internautes en moins de 40 minutes suite à un signalement sur www.phishing-initiative.fr.

Des milliers d'internautes contribuent anonymement à ce projet chaque année et plusieurs centaines d'individus ont créé depuis la rentrée un compte personnel sur le site Phishing Initiative. Il leur permet désormais de signaler des URLs suspectes plus simplement et d'accéder à des informations, statistiques et services additionnels, relatifs notamment aux signalements effectués par leurs soins. Ces internautes peuvent, par exemple, suivre l'état du site en temps réel et demander à être prévenus du caractère frauduleux ou non d'une adresse ainsi soumise, mais surtout participer à la lutte anti-phishing et empêcher que d'autres internautes soient victimes de ce fléau.

A propos de Phishing Initiative

Créé sous l'impulsion conjointe du cabinet Lexsi, de Microsoft et de PayPal Europe en 2011, Phishing Initiative, association à but non lucratif, offre à tout internaute la possibilité de vérifier un site suspect et lutter contre les attaques de phishing. En signalant l'adresse d'un site suspecté d'héberger un cas de phishing francophone, vous contribuez à diminuer l'impact de cette cybercriminalité en évitant que d'autres internautes soient piégées par ces attaques. Chaque adresse différente fera en effet l'objet d'une vérification humaine et si confirmée comme frauduleuse d'un envoi pour blocage dans les listes noires des principaux navigateurs Plus d'informations sur : https://phishing-initiative.fr

---

Denis JACOPINI est Expert Informatique assermenté, consultant et formateur en sécurité informatique, en mise en conformité de vos déclarations à la CNIL et en cybercriminalité.

Nos domaines de compétence :

• **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;

• **Consultant** en sécurité informatique, cybercriminalité, en accompagnement aux mises en conformité et déclarations à la CNIL ;

• **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL et accompagnement de Correspondant Informatique et Libertés.

Contactez-nous

Cet article vous plait ? Partagez !

Un avis ? Laissez-nous un commentaire !

Source : http://www.globalsecuritymag.fr/Plus-de-2-millions-d-internautes,20151105,57293.html

Kaspersky Decryptor : un outil pour décrypter les fichiers des ransomware Coinvault et Bitcryptor | Le Net Expert Informatique

Kaspersky Decryptor : un outil pour décrypter les fichiers des ransomware Coinvault et Bitcryptor

L'éditeur d'outils de sécurité a réussi à récupérer toutes les clés de décryptage de deux malwares qui corrompent les fichiers utilisateurs.

Kaspersky Decryptor : un outil pour décrypter les fichiers des ransomware Coinvault et Bitcryptor
Dans la liste des logiciels malveillants les ransomware font partie des plus redoutables pour extorquer de l'argent aux victimes. Kaspersky propose toutefois un outil pour venir à bout de deux d'entre eux tout en offrant la possibilité de décrypter les fichiers corrompus.

Coinvault et Bitcryptor sont deux malwares de type « ransomware ». Ils prennent place sur l'ordinateur en trompant l'utilisateur puis appliquent un chiffrement sur les fichiers de l'utilisateur qui deviennent inaccessibles sans clé de déverrouillage. Les malfaiteurs proposent de délivrer la clé contre le paiement d'une rançon, d'où le nom ransomware.

Ransomware Coinvault
Depuis plusieurs mois Kaspersky collabore avec les les forces de l'ordre néerlandaises pour récupérer des clés de décryptage. Après avoir récupéré quelques échantillons en début d'année, ils annoncent aujourd'hui que toutes les clés de décryptage, plus de 14000, sont à présent disponibles. Cela permettra aux utilisateurs infectés de se débarasser du logiciel malveillant tout en retrouvant l'accès à leurs fichiers.

Kaspersky Decryptor
La procédure (en anglais https://noransom.kaspersky.com/static/CoinVault-decrypt-howto.pdf) explique la marche à suivre. Le logiciel malveillant est tout d'abord éliminé en utilisant la suite Kaspersky Internet Security (http://www.cnetfrance.fr/telecharger/kaspersky-internet-security-39184140s.htm) puis le logiciel Kaspersky Ransomware Decryptor (https://noransom.kaspersky.com/) déchiffre les fichiers de l'ordinateur grâce à la liste qu'il récupère ou dans un dossier désigné par l'utilisateur.

Tous les logiciels malveillants agissant de cette façon ne sont toutefois pas concernés. Il est donc recommandé pour éviter tout problème de sauvegarder régulièrement ses fichiers personnels sur un support externe tel qu'un disque amovible ou un service de stockage en ligne.

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

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

Source :
http://www.cnetfrance.fr/news/kaspersky-decryptor-un-outil-pour-decrypter-les-fichiers-des-ransomware-coinvault-et-bitcryptor-39827670.htm

---

Nouvelle réglementation Européenne sur la protection des données personnelles | Le

Net Expert Informatique

Nouvelle réglementation Européenne sur la protection des données personnelles

Comment être prêt à répondre aux exigences de la nouvelle réglementation européenne sur la protection des données personnelles ?

Les apports du projet de règlement UE sur la protection des données personnelles en matière de gestion de crise sont nombreux et les entreprises peuvent d'ores et déjà se préparer à plusieurs niveaux.
Vous êtes le dirigeant d'une entreprise de la grande distribution, vôtre RSSI vous informe que malgré les mesures de sécurité mises en œuvre, l'entreprise est victime d'un vol massif de données clients. Vous avez conscience que c'est impactant pour votre entreprise mais heureusement les législations européennes et françaises, en matière de violation des données à caractère personnel, ne visent que les fournisseurs de communication électronique. Vous êtes épargnés d'un point de vue réglementaire… Certes, mais plus pour longtemps.
Le projet de règlement sur la protection des données destiné à remplacer la Directive 95/46/CE doit actuellement repasser devant la Commission et son adoption ne saurait tarder. Le règlement vise désormais toutes les organisations traitant des données à caractère personnel et en lien avec l'UE (territorial, résidents UE…).
Celui-ci impose notamment, que si les conséquences de la compromission de données, constituent un risque élevé pour les droits et libertés des personnes physiques concernées, l'organisation doit les informer au plus vite. Elle doit aussi en informer les autorités compétentes en matière de protection des données à caractère personnel. Pour ce faire plusieurs actions doivent être réalisées en étroite collaboration avec le soutien du Data Privacy Officer (DPO) de l'organisation.

La qualification de l'incident
L'objectif est de déterminer si le risque est élevé pour les personnes concernées. Pour ce faire il convient en premier lieu de répondre à deux questions :
• Les données volées rendent-elles les personnes concernées identifiables ?
• Les personnes concernées peuvent-elles connaître des conséquences significatives voire irrémédiables (discrimination, vol/usurpation d'identité, perte financière, atteinte à la réputation) ?
A l'issue de cette première phase, si le risque est élevé pour les personnes concernées (données identifiables et conséquences majeures), il faudra procéder à la notification de l'autorité compétente et des personnes concernées.
L'organisation ne sera toutefois pas tenue de notifier les personnes concernées par la violation si :
• Le responsable du traitement a mis en œuvre des mesures de protection technologiques appropriées rendant les données incompréhensibles à toutes personnes non autorisées à y avoir accès (ex : chiffrement) ;
• Ou si la notification risque d'entrainer des mesures disproportionnées eu égard notamment au nombre de cas concernés ;
• Ou si la notification risque de porter atteinte à un intérêt public important.

La notification de l'incident
Pour la notification à l'autorité en charge de la protection des données, la CNIL en France, l'organisation victime de l'attaque dispose d'un délai de 72 heures. Cette notification devra notamment comporter les éléments suivants :
• La nature de la violation
• Le nombre approximatif de personnes et des enregistrements concernés
• La description des conséquences probables de la violation
• La description des mesures prises

Pour la notification aux personnes concernées, celles-ci doivent aussi être averties sans retard injustifié. Trois éléments principaux doivent être communiqués :
• La nature de la violation des données à caractère personnel
• Les mesures prises ou proposées pour remédier à la violation
• Les recommandations afin d'atténuer les effets négatifs de la violation

Durant toute la gestion de la crise ainsi que durant la sortie de crise, le responsable du traitement doit alimenter puis conserver une trace documentaire de la violation des données à caractère personnel en indiquant son contexte, ses effets et les mesures prises pour y remédier. Ce document aura valeur juridique et pourra être opposable.

En parallèle à ces actions, la gestion de la crise comporte également une gestion technique de l'attaque, une campagne de communication de crise afin de sauvegarder la réputation, ainsi qu'une démarche judiciaire et assurantielle notamment si l'organisation a adopté une cyber-assurance.

Le rôle du DPO
En temps de crise, le Data Privacy Officer (DPO) pourra veiller à ce que les mesures adaptées et la notification à l'autorité de contrôle et aux personnes concernées soient réalisées. Il pourra par ailleurs effectuer toutes les procédures requises auprès de la CNIL ainsi que suivre le dossier. En outre, les relations entre le CIL et la CNIL déjà établies en amont de la crise permettent d'alléger les procédures.

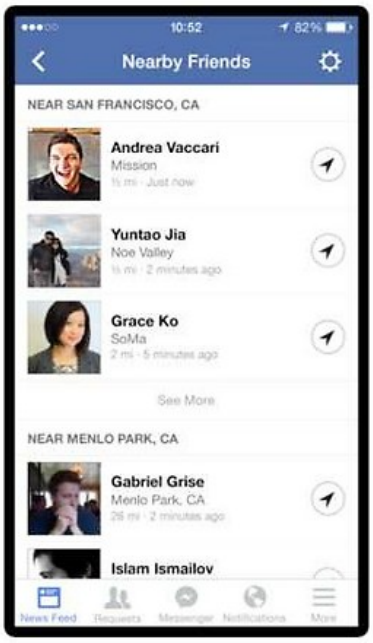
L'existence du CIL dans les entreprises peut être ainsi un élément favorisant l'adoption de réponses adaptées en temps de crise et pouvant réduire le montant de la sanction administrative dans le cas où la responsabilité du responsable de traitement ou du sous-traitant est démontrée.

Comme tout professionnel de l'informatique et de l'Internet, il est de mon devoir de vous informer que vous devez mettre en conformité et déclarer à la CNIL tous vos traitement de données à caractère personnel (factures, contacts, emails…).
Même si remplir un formulaire de déclaration à la CNIL est simple et gratuit, il vous engage cependant, par la signature que vous apposez, à respecter point par point la loi Informatique et Libertés. Cette démarche doit commencer par une analyse précise et confidentielle de l'ensemble de vos systèmes de traitements de données. Nous pouvons vous accompagner pour vous mettre en conformité avec la CNIL, former ou accompagner un C.I.L. (correspondant CNIL) ou sensibiliser les agents et salariés à l'hygiène informatique.
Besoin d'informations complémentaires ?
Contactez-nous
Denis JACOPINI
Tel : 06 19 71 79 12
formateur n°93 84 03041 84

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

Source : http://www.itpro.fr/a/nouvelle-reglementation-ue-sur-protection-donnees-personnelles/
Par Francesca Serio – Consultante spécialisée en Gestion de crise et Continuité d'Activité – Provadys

Avec Facebook, on peut désormais savoir quand nos amis sont à proximité.. et lui aussi ! | Le Net Expert Informatique



Avec Facebook, on peut désormais savoir quand nos amis sont à proximité… et lui aussi !

Le réseau social propose ce mardi sur son application mobile une option baptisée « Nearby Friends » qui envoie une notification quand un ami se trouve à proximité.

Facebook veut savoir où nous sommes et souhaite également que nos amis le sachent. A partir de ce mardi, une nouvelle option apparaît sur le réseau social : « Nearby Friends », soit une bonne méthode pour scruter les activités de vos amis. L'application va ainsi envoyer une notification quand un ami de l'utilisateur se trouve à côté de lui.

Option désactivée par défaut

Les réseaux sociaux ne laissent donc plus de place aux mensonges. Impossible d'éviter un ami encombrant : « Lorsque vous allez au cinéma, 'Friends Nearby' vous dit si des amis à vous sont proches pour que vous alliez voir le film ensemble ou pour vous retrouver ensuite », indique Facebook.

Pour l'instant, il s'agit d'une option non-obligatoire, c'est à dire qu'elle est désactivée par défaut. En revanche, il est impossible de savoir à partir de combien de kilomètres Facebook considérera qu'un ami se trouve « à proximité ».

Avec cette option, le réseau social pourrait également franchir une nouvelle étape dans la collecte des données personnelles, alors que la nouvelle application débarque au lendemain d'une injonction de la justice belge . Cette dernière a ordonné Facebook d'arrêter de tracer tous les internautes, dont ceux qui ne sont pas connectés au réseau social.

Nouvelle tendance

La nouvelle option Facebook semble s'inscrire dans une nouvelle tendance. Il y a quelques jours, c'est Google qui annonçait le lancement d'une nouvelle application indiquant aux amis d'un utilisateur si celui-ci est disponible pour sortir manger, boire un verre, etc. Baptisée « Who's Down », l'option n'est disponible qu'aux Etats-Unis et constitue un premier test pour Google. Pour Facebook en revanche, cette phase a déjà été réalisée : l'option « Nearby Friends » a été l'ancée dès 2014 chez les anglo-saxons.

Facebook Messenger intègre la reconnaissance faciale

En Australie, le réseau social va encore plus loin en proposant une nouvelle application sur Facebook Messenger. Baptisée « Photo Magic », il s'agit d'un outil permettant de partager facilement des photos où apparaissent les personnes avec lesquelles on discute. Facebook utilise pour cela la reconnaissance faciale et scanne toutes les photos stockées sur le téléphone de l'utilisateur. Si un ami Facebook est détecté sur l'une des photos, l'application propose de la partager à la personne identifiée. Pour l'instant la fonctionnalité est optionnelle et ne devrait pas arriver tout de suite en France. Facebook a en effet cessé la reconnaissance faciale en Europe pour respecter la législation sur la protection des données personnelles.

Comme tout professionnel de l'informatique et de l'Internet, il est de mon devoir de vous informer que vous devez mettre en conformité et déclarer à la CNIL tous vos traitement de données à caractère personnel (factures, contacts, emails…).
Même si remplir un formulaire de déclaration à la CNIL est simple et gratuit, il vous engage cependant, par la signature que vous apposez, à respecter point par point la loi Informatique et Libertés. Cette démarche doit commencer par une analyse précise et confidentielle de l'ensemble de vos systèmes de traitements de données. Nous pouvons vous accompagner pour vous mettre en conformité avec la CNIL, former ou accompagner un C.I.L. (correspondant CNIL) ou sensibiliser les agents et salariés à l'hygiène informatique.
Besoin d'informations complémentaires ?
Contactez-nous
Denis JACOPINI
Tel : 06 19 71 79 12
formateur n°93 84 03041 84

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

Source : http://www.lesechos.fr/tech-medias/hightech/021468123566-grace-a-facebook-on-peut-desormais-savoir-quand-nos-amis-sont-a-proximite-1174043.php

---

La CDP malienne venue s'inspirer de l'expérience

sénégalaise | Le Net Expert Informatique

	La CDP malienne venue s'inspi08rer de l'expérience sénégalaise

La Commission de Protection des Données Personnelles du Sénégal (CDP) a reçue la visite du 02 au 04 Novembre 2015 de son homologue malien, l'Autorité de Protection des Données à caractère Personnel (APDP), venu s'inspirer de son expérience et de sa pratique. Cette visite s'inscrit en effet dans le cadre du renforcement de la coopération et des échanges d'expériences entre les deux institutions qui ont en charge la protection des données à caractère personnel.

La délégation de l'Autorité malienne, avec à sa tête son Président, M. Oumarou A.G Mouhamed Ibrahim AIDARA, était composé de cinq personnes. Cette visite s'explique selon le Président de l'autorité malienne par la volonté de s'imprégner de l'expérience enregistrée par le Sénégal depuis quelques années en matière de protection des données personnelles. Elle se justifie également par les ressemblances constatées dans les deux pays.

M. Oumarou A.G Mouhamed Ibrahim AIDARA a remercié les autorités sénégalaises de leur accueil chaleureux et précisé qu'ils étaient venus pour apprendre du Sénégal.

De son côté, le Président de la CDP, le Dr Mouhamadou LO, a magnifié le début d'une fructueuse collaboration entre les deux institutions, tout en invitant ses responsables à œuvrer pour que le respect de la vie privée des personnes entre dans les habitudes quotidiennes des Maliens. Les deux autorités de protection ont émis le souhait de nouer une collaboration étroite et un appui mutuel dans le cadre de la lutte contre la violation de la vie privée au sein des deux pays.

Comme tout professionnel de l'informatique et de l'Internet, il est de mon devoir de vous informer que vous devez mettre en conformité et déclarer à la CNIL tous vos traitement de données à caractère personnel (factures, contacts, emails…).
Même si remplir un formulaire de déclaration à la CNIL est simple et gratuit, il vous engage cependant, par la signature que vous apposez, à respecter point par point la loi Informatique et Libertés. Cette démarche doit commencer par une analyse précise et confidentielle de l'ensemble de vos systèmes de traitements de données. Nous pouvons vous accompagner pour vous mettre en conformité avec la CNIL, former ou accompagner un C.I.L. (correspondant CNIL) ou sensibiliser les agents et salariés à l'hygiène informatique.
Besoin d'informations complémentaires ?
Contactez-nous
Denis JACOPINI
Tel : 06 19 71 79 12
formateur n°93 84 03041 84

Source : http://www.dakaractu.com/Protection-des-Donnees-Personnelles-La-CDP-malienne-venue-s-inspirer-de-l-experience-senegalaise_a100379.html

---

Une attaque DDos a duré

quasiment deux semaines | Le Net Expert Informatique

Une attaque DDos a.duré quasiment deux semaines

Même si la plupart des attaques DDos ne durent guère plus longtemps que 24 heures, le nombre de ce genre d'attaques de longue durée croît nettement. La plus longue au troisième trimestre a ainsi duré pas moins de 320 heures.

Voilà ce que communique l'entreprise de sécurité Kaspersky Lab dans son rapport trimestriel DDos à propos des trois derniers mois écoulés.
Les attaques DDos se manifestent surtout dans un nombre limité de pays: 91 pour cent des systèmes agressés se trouvent dans 10 pays. Les pays les plus souvent touchés par des attaques DDos sont la Chine, les Etats-Unis et la Corée du Sud. Ces attaques proviennent principalement du même pays où se trouve la cible. La Chine, les Etats-Unis et la Corée du Sud forment donc le trio de tête au classement des attaques lancées. Il s'agit là d'une pratique complètement différente de celle d'autres cyber-attaques, comme les vols de données. Dans ce dernier cas, les attaques émanent de très nombreux pays et certainement pas aussi souvent du pays où se trouve la victime.

La plupart des attaques visent à perturber les activités de la cible, mais le nombre d'attaques de longue durée pouvant entraîner la faillite de la victime, est en augmentation. Elles vont aussi parfois de pair avec des demandes de rançon.

Denis JACOPINI est Expert Informatique assermenté, consultant et formateur en sécurité informatique, en mise en conformité de vos déclarations à la CNIL et en cybercriminalité.
Nos domaines de compétence :

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

Contactez-nous

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

Source :
http://datanews.levif.be/ict/actualite/une-attaque-ddos-a-dure-quasiment-deux-semaines/article-normal-432941.html

La NSA assure divulguer les vulnérabilités découvertes. Avant ou après attaque ? | Le Net Expert Informatique

La NSA assure divulguer les vulnérabilités découvertes

L'agence de renseignement US assure communiquer aux éditeurs 91% des failles qu'elle découvre dans les logiciels. La NSA ne précise pas en revanche quand ces données sont transmises et si les failles ont été exploitées au préalable.

L'agence de renseignement américaine est une grande consommatrice de failles de sécurité. Celles-ci lui permettent en effet de récolter des informations. Mais la NSA, en ne dévoilant pas ces vulnérabilités, laisse aussi les entreprises US exposées à des attaques.
Après les révélations d'Edouard Snowden, ces pratiques ont été examinées. Pas sûr cependant qu'elles ne changent comme l'explique Reuters. Sur son site Internet, la NSA justifie sa démarche, estimant ainsi qu'il y « a des avantages légitimes et des inconvénients à la décision de divulguer les vulnérabilités ».

Combien de temps la NSA garde-t-elle le secret ?

Et les arbitrages entre une divulgation rapide et la rétention de cette information « peut avoir des conséquences significatives ». En dévoilant une vulnérabilité, la NSA précise ainsi qu'elle renonce à la possibilité de collecter du renseignement crucial : attaque terroriste, vol de propriété intellectuelle ou découverte d'autres failles encore plus dangereuses.
Néanmoins, la NSA assure, « historiquement », avoir communiqué plus de 91% des vulnérabilités identifiées dans les produits soumis à son audit interne, développés ou utilisés aux Etats-Unis. Et les autres ? Il s'agit de failles déjà corrigées ou gardées secrètes pour des raisons de sécurité nationale, explique l'agence.
Mais comme le souligne Reuters, la question est plus de savoir quand les vulnérabilités sont communiquées aux éditeurs et ainsi corrigées. D'après un ancien officiel de la Maison-Blanche, il est raisonnable de penser que ces 91% de failles sont préalablement exploitées avant de faire l'objet d'une divulgation.
La NSA n'apporte aucun commentaire sur ce point. Mais la faille Heartbleed est une illustration de ces pratiques. La NSA aurait eu connaissance de cette faille critique et l'aurait exploitée pour ses opérations au moins deux ans avant qu'elle ne soit connue publiquement. L'agence de renseignement réfute cependant.

Denis JACOPINI est Expert Informatique assermenté, consultant et formateur en sécurité informatique, en mise en conformité de vos déclarations à la CNIL et en cybercriminalité.
Nos domaines de compétence :

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

Contactez-nous

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

Source :
http://www.zdnet.fr/actualites/la-nsa-assure-divulguer-les-vulnerabilites-decouvertes-avant-ou-apres-attaque-39827840.htm

Les cybercriminels ciblent le paiement mobile | Le Net Expert Informatique

Il y a quelques semaines, nous avons traité, du e-Commerce. C'est un registre si vaste et varié que nous choisissons, cette semaine aussi, d'y consacrer quelques réflexions, histoire de susciter chez nos lecteurs quelque intérêt pour une problématique appelée à devenir incontournable. Malgré l'essor du e-Commerce, les modes de paiement mobile peinent à décoller dans de nombreux pays développés. En cause, le conservatisme et la peur de l'inconnu.

L'inconnu, selon de nombreux spécialistes, c'est la cybercriminalité qui donne des sueurs froides aux fournisseurs de solutions. Dans un excellent article au titre très évocateur publié récemment, « Le paiement mobile, nouvel eldorado des escrocs », Benoît Huet de la rédaction de lemondeinformatique.fr nous amène faire une immersion dans les méandres d'un secteur pourtant promu à un bel essor. Les résultats du paiement mobile, il faut bien le concéder, sont assez modestes.

Dans son article, Benoît Huet écrit : « Selon l'institut d'études GFK, qui a mené une enquête dans 17 pays auprès de 17 000 consommateurs, seulement 5% des transactions mondiales sont réellement effectuées avec un appareil mobile ». Presqu'un désert ! Dans un pays comme la France, notre référence à tous, « les transactions via le paiement mobile sont souvent estimées à moins de 1% par les différents cabinets d'études ».

Et pourtant, précise l'article de notre confrère, ce n'est pas faute d'avoir essayé. De nombreuses applications permettant de payer avec un smartphone existent : le service PayByPhone pour payer le stationnement et le parking à Boulogne, Nice et dans d'autres villes, ainsi que des commerces qui ont mis en place un terminal NFC (Paiement Sans Contact) pour régler diverses courses.

La première raison, et nous l'évoquions plus haut, le conservatisme culturel : « Si le paiement mobile a encore du mal à percer en France, c'est déjà parce que les moyens de paiement sont très liés à la culture des pays. La France est par exemple un pays fortement tourné vers l'usage de la carte bleue Visa alors qu'en Belgique, c'est la Mastercard qui règne, quant à l'Allemagne, le paiement en liquide est encore très courant ».

Sans vouloir défier la technologie, « Les français ne sont pas encore prêts à payer avec leur mobile, c'est à la fois un problème culturel et un manque de confiance dans les technologies, ils préfèrent donc payer en caisse avec une carte, de l'espèce ou en chèque ».

La seconde raison qui plombe l'essor du paiement mobile vient d'être lâchée : le manque de confiance dans les technologies. Par instinct de survie, la majorité des français boudent le paiement mobile, moins sécurisé à leurs yeux, de peur d'être victime des cyberescrocs qui ont plus d'un tour dans leur sac.

Sans l'affirmer, les conclusions de l'étude donnent raison aux cyber-sceptiques qui semblent se perdre dans la jungle des technologies de communication sans contact comme les balises (Beacons utilisant le Bluetooth) ; le RFID ; le NFC (qu'utilise Apple, entre autres, avec Apple Pay et Google avec Google Wallet) ; le QR code (comme le Flash'NPay créé par Auchan) ; la transmission magnétique (Samsung Pay exploite la technologie transmission magnétique suite au rachat de LoopPay mais aussi le NFC) ; les systèmes de portefeuilles électroniques mobiles comme Orange Cash (Orange et Visa) ; PayPal Mobile et Paylib (initié par les banques françaises). Jungle, il faut bien l'admettre, est vraiment un doux euphémisme pour évoquer cet univers ! Face à un tel environnement, banques et entreprises n'ont d'autres choix que de perfectionner la sécurité des systèmes de paiement mobiles afin de donner davantage d'assurance aux consommateurs. Cette assurance semble passer par des systèmes de cryptage des données très évolués et les dispositifs de détection prédictive de malwares. Notre confrère cite PayPal qui vient de racheter la start-up israélienne CyActive qui a mis au point une technologie capable d'anticiper les futures attaques grâce à des algorithmes permettant d'analyser et de comprendre les processus de piratage.

En parallèle, les fournisseurs ne ménagent pas leurs efforts en apportant, au niveau du terminal, des mécanismes à double authentification comme Apple qui exploite l'empreinte digitale en plus d'un code de sécurité unique et des quatre derniers numéros de la carte de sécurité sociale de l'utilisateur. On le voit bien, il y a de gros efforts en cours pour tendre vers le risque zéro, même s'il n'existe pas.

Les entreprises du secteur et les banques gagneraient à collaborer plus étroitement pour améliorer la sécurité des transactions au plan national et international, tout comme elles sont condamnées à imaginer des standards qui détectent à mille lieues les criminel et les neutralisent sans coup férir.

Enfin, chaque entreprise qui propose des solutions de paiement mobile devrait assortir son plan d'expansion d'une campagne de communication qui permettrait aux utilisateurs d'éviter de tomber dans les pièges, de plus en plus perfectionnés, des cybercriminels.

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

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

Source : http://malijet.com/la_societe_malienne_aujourdhui/139922-chronique-du-web-les-cybercriminels-ciblent-le-paiement-mobile.html
Par Serge de MERIDIO

Un rançongiciel Linux s’attaque aux webmasters, en chiffrant les données des répertoires contenant les pages web | Le Net Expert Informatique

Un rançongiciel Linux s’attaque aux webmasters, en chiffrant les données des répertoires contenant les pages web

Un nouveau rançongiciel s’attaque aux machines Linux et cible en particulier les dossiers contenant les pages web. Le procédé du logiciel malveillant appelé Linux.Encoder est simple. Le rançongiciel crypte les répertoires de MySQL, Apache ainsi que le répertoire home/root. Le système demande alors de payer un seul bitcoin pour déverrouiller les fichiers.

Une fois que la rançon est payée, le système reçoit une instruction lui faisant parcourir les répertoires pour déchiffrer leurs contenus. Pour s’exécuter, la ransomware a besoin des privilèges d’administrateur et éventuellement d’une autorisation de la part d’un administrateur système pour qu’un tel programme puisse s’exécuter sans restriction. Selon le site drweb.com, une fois que le rançongiciel est lancé avec les privilèges d’administrateur, le logiciel télécharge le contenu des dossiers ciblés et crée un ficher contenant le lien vers une clé RSA publique. Le rançongiciel commence alors à supprimer les fichiers originaux et la clé RSA est utilisée pour générer une clé AES qui sera utilisée pour chiffrer les fichiers sur l’ordinateur infecté.

Source : Dr.WEB

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

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

Source :
http://www.developpez.com/actu/92220/Un-rancongiciel-Linux-s-attaque-aux-webmasters-en-chiffrant-les-donnees-des-repertoires-contenant-les-pages-web/