Cyber-attaques : Denis Jacopini, expert, alerte – Article dans Midi Libre Gard…

13

	Cyber-attaques : Denis Jacopini, expert, alerte – Article dans Midi Libre Gard…

Avec Denis Jacopini, expert informatique près la cour d'appel de Nîmes et consultant auprès des entreprises, après une série de piratages de site internet en France et dans le Gard.Après les attentats du 7 janvier, de nombreux sites internet d'institutions locales ou religieuses en France ont été piratés par des groupes de hackers se présentant comme des islamistes, dont celui du palais des Papes à Avignon, victime d'un défaçage (remplacement de la page d'accueil du site) par un groupe dénommé Fallaga team . Ces phénomènes de piratage ne sont pas nouveaux et s'accentuent. Ils sont imputables à différents types de malfaiteurs et se matérialisent de manière très différente. Décryptage des cyber-attaques avec Denis Jacopini, expert judiciaire près la cour d'appel de Nîmes et des juridictions du Gard, du Vaucluse, de l'Ardèche et de la Drôme. Denis Jacopini : « Les chefs d'entreprise ne sont pas assez sensibilisés. » DR Qu'est-ce qu'une cyber-attaque ? C'est une attaque informatique utilisant les réseaux de télécommunication et cela existe depuis qu'Internet s'est répandu dans le…

Bagnols — Midi Libre midilibre.fr — MERCREDI 11 FÉVRIER 2015 — 3

Cyber-attaques : « Les sociétés ne se protègent pas »

Entretien | Avec Denis Jacopini, expert informatique près la cour d'appel de Nîmes et consultant auprès des entreprises, après une série de piratages de site internet en France et dans le Gard.

Contexte

Qu'est-ce qu'une cyber-attaque ?

« On peut stopper le phénomène si on change les mentalités »

Il semble impossible, quelle que soit la structure attaquée, de s'en prémunir.

A-t-on une idée du nombre de victimes que font ces attaques ?

Mais cette lutte coûte cher pour de petites structures comme une mairie !

GROS PLAN

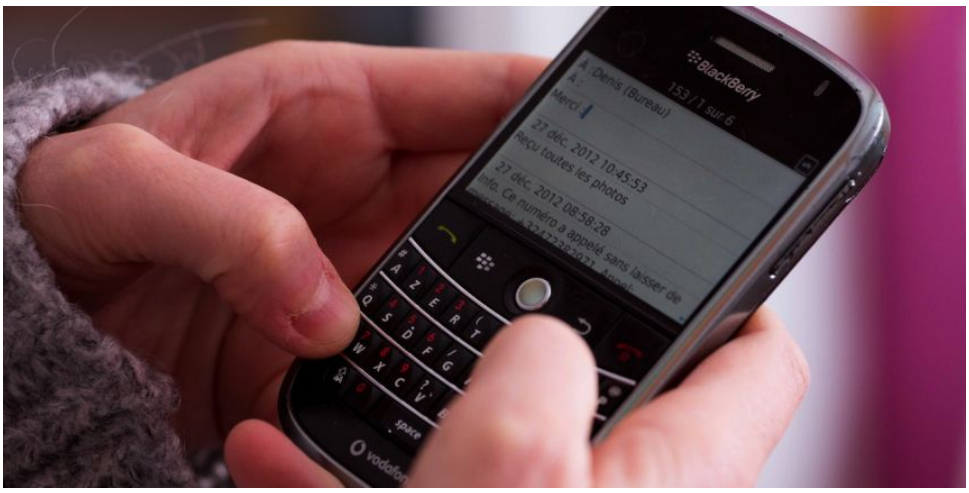
La e-reputation

Gard : 20 faits de piratage de sites en 2014 et cinq en 2015

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.midilibre.fr/2015/02/11/cyber-attaques-les-societes-ne-se-protegent-pas,1123222.php

Attention, votre employeur a désormais le droit de fouiller dans les SMS de votre téléphone pro !



Il faudra désormais prendre garde à ce que vous écrivez depuis votre téléphone portable professionnel… Photo : Sipa

Attention, votre employeur a désormais le droit de fouiller dans les SMS de votre téléphone pro !

La Cour de cassation a récemment rendu un arrêt qui donne aux SMS échangés sur les téléphones portables mis à disposition par les employeurs une présomption de « caractère professionnel ». Si vous voulez être certain que vos textos privés ne puissent être utilisés contre vous, il faudra désormais inscrire les mots « personnel » ou « perso » dans vos messages…

C'est une décision passée totalement inaperçue, mais qui concerne des centaines de milliers de salariés : tous ceux qui se sont vus mettre à disposition un téléphone portable par leur employeur. La Cour de cassation, dans un arrêt rendu le 10 février, que metronews s'est procuré, a validé le principe selon lequel les SMS envoyés ou reçus par cet appareil « sont présumés avoir un caractère professionnel ». Conséquence : « l'employeur est en droit de les consulter en dehors de la présence de l'intéressé, sauf s'ils sont identifiés comme étant personnels ».

Un processus pas « déloyal »

La plus haute juridiction de l'ordre judiciaire était invitée à statuer sur le litige opposant deux sociétés de courtage, GFI Securities Limited et Newedge. Cette dernière, reprochant à son concurrent d'avoir été déloyal en débauchant « un grand nombre » de ses salariés, avait utilisé comme preuve pour l'attaquer des SMS échangés entre ses anciens employés, qui évoquaient leur départ concerté de l'entreprise. En l'occurrence, Newedge négociant des produits financiers, tous les messages envoyés et reçus par ses salariés étaient automatiquement enregistrés sur un serveur informatique, conformément à la législation en vigueur.

Cette filiale de la Société Générale n'a donc eu qu'à effectuer une recherche à base de mots-clé pour retrouver et faire constater par huissier les SMS en question. Qui, pour la cour de Cassation comme pour la Cour d'appel de Paris dans un arrêt rendu il y a deux ans, constituent bien des preuves recevables : leur utilisation ne peut être considérée comme un « processus déloyal » ni « être assimilée à l'enregistrement d'une communication téléphonique privée effectuée à l'insu de l'auteur des propos ».

Pour les emails, c'était déjà le cas

Si dans cette affaire, les SMS avaient la particularité d'être stockés sur un serveur, la décision « est destinée à faire jurisprudence » pour tous les salariés à qui l'employeur a mis un téléphone portable à disposition, assure à metronews maître Jean-Philippe Duhamel, avocat au Conseil d'Etat et à la Cour de cassation. Avec cette décision souligne-t-il, la justice a manifesté « un souci de cohérence et de simplicité ». La Cour de cassation avait en effet déjà pris des arrêts similaires en ce qui concerne les fichiers détenus sur un ordinateur de travail ou les emails envoyés par un salarié depuis sa boîte pro. Depuis mai 2013 ainsi, l'employeur est dans son droit s'il ouvre en dehors de la présence de son employé un courrier électronique qui n'a pas été identifié comme personnel.

Comment éviter que vos textos privés ne puissent être utilisés contre vous ? La seule solution, explique Jean-Philippe Duhamel, est d'y intégrer « une mention les identifiant comme personnels, par exemple en les faisant commencer par les mots 'personnel' ou 'perso' ». Un peu contraignant pour des messages courts qui, contrairement aux emails, ne comportent le plus souvent pas de champ « objet ». Il existe toutefois une autre solution, plus radicale : réserver vos communications privées à votre téléphone personnel.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.metronews.fr/info/attention-votre-employeur-a-desormais-le-droit-de-fouiller-dans-les-sms-de-votre-telephone-pro/mobs!1pxxcsNP7VEA/
Par Gilles DANIEL

Microsoft donne un coup de fouet au HTTPS dans Internet Explorer

Microsoft donne un coup de fouet au HTTPS dans Internet Explorer

Microsoft renforce la sécurité et la consultation des sites Internet au sein de son navigateur Web Internet Explorer en déployant le système HSTS.

Le support du HTTP Strict Transport Security (HSTS) fait son entrée dans la version d'Internet Explorer proposée au sein de la mouture de test de Windows 10.
Ce système renforce la sécurité des communications entre l'internaute et les serveurs Web. Il permet de s'assurer que la connexion est sécurisée. Si le certificat de chiffrement n'est pas correct, la connexion au site ne sera pas possible.
De plus, le mélange de contenus sécurisés et en clair au sein d'une même page Web n'est pas permis par le HSTS.
Une liste de sites Web devant utiliser le HTTPS par défaut est fournie avec Internet Explorer.
Elle s'appuie sur celle créée pour le projet Chromium. Des mécanismes spécifiques permettent également de s'assurer que l'internaute ne basculera pas en HTTP lorsqu'il a débuté sa visite sur un site en HTTPS, explique Silicon.fr.
L'objectif est de s'assurer que la séance de surf sur un site Web s'effectue de bout en bout de façon sécurisée, en HTTPS, c'est-à-dire de manière chiffrée.
Les mauvaises langues remarqueront que Microsoft a pris son temps. Le HSTS est en effet pris en compte depuis les versions 4 de Firefox, Chrome et Chromium, soit depuis plusieurs années déjà.
Les serveurs Web open source les plus populaires (Apache, Nginx, etc.) sont aujourd'hui compatibles avec ce protocole de sécurité. L'offre IIS de Microsoft peut également être configurée pour prendre en compte le HSTS.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.itespresso.fr/internet-explorer-microsoft-donne-un-coup-de-fouet-au-https-88802.html#ZlJQDlMwDry82Trz.99

Comment détecter et se débarrasser de l'espion Superfish dans les ordinateurs de marque Lenovo ?

Comment détecter et se débarrasser de l'espion Superfish dans les ordinateurs de marque Lenovo ?

L’adware installé par défaut par Lenovo sur plusieurs de ses PC n’est pas seulement intrusif, il expose aussi ses clients à des risques de sécurité. Mais Superfish et ses certificats peuvent être supprimés : mode d’emploi. Vendre des PC ne suffisait semble-t-il pas à Lenovo, qui voulait également dégager des revenus grâce à l’installation sur certaines de ses machines d’un logiciel publicitaire ou adware. Problème : cet outil, baptisé Superfish, n’est pas seulement intrusif, il présente aussi un important risque de sécurité pour les utilisateurs.
Les possesseurs d’un ordinateur Lenovo et désireux de détecter rapidement s’ils sont ou non concernés par Superfish peuvent se tourner vers LastPass, un éditeur spécialisé dans la gestion des mots de passe.

Les certificats Superfish : le risque principal
Ce dernier a mis en ligne un outil Web (téléchargeable sur https://lastpass.com/superfish) qui va donc très facilement détecté la présence de l’adware Superfish sur l’ordinateur. Celui-ci repéré, encore faut-il ensuite le supprimer. Le programme en lui-même se désinstalle sans complication depuis le panneau de configuration de Windows et en cherchant « Superfish Visual Discovery » dans la liste des programmes installés.

Le logiciel intrusif effacé, reste encore une tâche essentielle : supprimer les certificats de sécurité liés à Superfish et qui présentent le principal risque pour l’utilisateur. Dans le menu Démarrer de Windows, puis la boîte de recherche, tapez « certmgr.msc ». Lancez ensuite le programme certmgr.msc, cliquez sur Autorités de certification racines et enfin Certificats. C’est parmi cette liste que vous trouverez les certificats. Repérez ceux mentionnant Superfish Inc et supprimez-les.
Pour être certain que tout est en ordre, fermez le navigateur et refaites un nouveau test sur LastPass (téléchargeable sur https://lastpass.com/superfish). D’après les informations remontées par les utilisateurs sur des forums, ces différentes configurations de Lenovo, au moins, seraient concernées par la présence de Superfish : Y50, Z40, Z50, G50 et les modèles Yoga 2 Pro.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.zdnet.fr/actualites/guide-detecter-le-superfish-de-lenovo-et-le-supprimer-39815074.htm

---

TrueCrypt n’est pas mort, l’audit bouge encore

TrueCrypt n’est pas mort, l’audit bouge encore

Les développeurs chargés d'auditer la sécurité de TrueCrypt ont donné quelques nouvelles de leur avancement. Le développement du logiciel de chiffrement avait été interrompu brusquement durant l'été 2014, soulevant de nombreuses inquiétudes quant à la fiabilité du programme.

L'affaire TrueCrypt fait partie des mystères de la cybersécurité: en mai, le site web distribuant le logiciel annonçait la fin du développement, ajoutant que TrueCrypt n'était « plus sûr » et que les utilisateurs qui décidaient de s'appuyer dessus s'exposaient « à des failles de sécurité non comblées.»
Une nouvelle version du logiciel était distribuée par la même occasion, fortement déconseillée par la plupart des experts en cybersécurité. Un coup dur : TrueCrypt était l'un des projets considérés comme les plus solide en matière de protection des données et, aux dernières nouvelles, donnait encore du fil à retordre aux analystes de la NSA selon des documents datés de 2012.

Doutes et remises en question
Un audit de TrueCrypt avait néanmoins été initié en 2013, en s'appuyant sur un crowdfunding réalisé auprès de la communauté afin de financer un examen en profondeur du code source du logiciel. Si celui-ci avait été lancé bien avant l'arrêt brutal du développement, ses résultats sont aujourd'hui très attendus par les utilisateurs de TrueCrypt. Mais depuis juin 2014, aucune nouvelle n'avait émané du projet, suscitant les interrogations de la communauté.
Sentant monter l'inquiétude, Matthew Green, le chercheur à l'origine du projet d'audit a posté une mise à jour faisant le point sur l'avancement des travaux du groupe. Et c'est bien la moindre des choses : le financement de cet audit a été réalisé sur une opération de crowdfunding, qui avait rassemblé 70.000 dollars au mois de décembre 2013. Compte tenu de la somme récoltée auprès de donateurs et de l'actualité inquiétante du développement de Truecrypt, l'initiative menée par Matthew Green et Kenn White est surveillée de très près.
L'annonce de l'arrêt du développement a d'ailleurs suscité de nombreuses interrogations au sein du groupe chargé de l'audit du code : « L'annonce de l'abandon du projet par l'équipe de Truecrypt nous a poussé à reconsidérer notre approche. Etait-ce vraiment la bonne manière d'utiliser nos ressources ? Ne devrions-nous pas nous pencher au contraire sur les forks de Truecrypt qui émergeaient alors ? »
Matthew Green explique que le projet d'audit a donc connu une longue période de remise en question, mais que le projet est aujourd'hui à nouveau sur les rails, au travers d'un partenariat avec la société NCC Group North America, qui reprend en charge la poursuite de l'audit. Celui-ci entre dans sa seconde phase, après la publication d'une première partie qui avait noté quelques vulnérabilités mais aucune backdoor sérieuse au sein du code de la dernière version de TrueCrypt jugée fiable, la version 7.1a du logiciel.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.zdnet.fr/actualites/chiffrement-truecrypt-n-est-pas-mort-l-audit-bouge-encore-39815118.htm
Par Louis Adam

Lenovo accusé d'infecter ses

propres PC. Le protocole sécurisé SSL aurait été atteint

	Lenovo accusé d’infecter ses propres PC. Le protocole sécurisé SSL aurait été atteint

Très mauvaise publicité pour le premier fabricant mondial. Lenovo a été contraint d'admettre qu'il a installé secrètement un logiciel de publicité sur ses ordinateurs, lors de leur fabrication. Problème : ce logiciel aurait un effet pervers en mettant en péril la sécurité du protocole de sécurisation SSL. Face au tollé, Lenovo fait une courbe rentrante.

Lenovo, ce n'est pas n'importe qui. Il s'agit ni plus ni moins du premier fabricant mondial de PC. 60 millions de PC vendus l'an passé tout de même… Le groupe chinois est connu pour avoir racheté il y a quelques années la division PC d'IBM, ce qui lui a permis de faire son entrée dans la cour des grands. Ensuite, il a particulièrement bien tiré son épingle du jeu grâce à du matériel de qualité. Mais là, son image en prend un coup …

Toujours plus gourmand ?
Le logiciel installé secrètement par Lenovo, appelé Superfish, aurait pour but de créer un canal d'affichage de publicités ciblées lors des recherches effectuées sur certains moteurs de recherche. On appelle cela un « Adware ».

Le but ? Probablement faire de la concurrence à des systèmes bien connus comme Adwords, et créer une source de revenus complémentaires pour le fabricant qui pourrait ainsi entrer dans le marché très rentable de la publicité en ligne. Un péché de gourmandise ?
Le groupe ne nie pas mais minimise. Selon lui, il s'agirait d'améliorer « l'expérience utilisateur » selon l'expression consacrée, en permettant d'afficher du contenu publicitaire qui lui convient vraiment. Du marketing ciblé en un mot.

Contre publicité
Jusque-là, les enjeux sont éthiques (les publicitaires diront que les enjeux touchent l'image de l'entreprise), outre bien entendu un problème potentiel au niveau de la protection des données personnelles de l'utilisateur. Il y a tout de même des règles à respecter dans le cas de l'utilisation de données à caractère personnel à des fins de marketing. Il y a aussi des développements potentiels en droit des contrats si l'on considère que le PC livré ne correspond pas à ce qui a été vendu puisqu'un module supplémentaire, secret et indiscret est livré avec.
Il s'agit toutefois d'une contre-publicité remarquable, car plusieurs commentateurs rappellent que Lenovo a déjà été accusé plusieurs fois d'infecter ses PC lors de leur fabrication en modifiant les microprocesseurs afin de créer une porte d'entrée dérobée. Derrière cela, il y aurait le gouvernement chinois et de sombres opérations d'espionnage et/ou de cyber-guerre. Difficile de savoir si ces accusations ont quelque fondement ou s'il s'agit d'un fantasme lié à l'origine chinoise du fabricant, mais la rumeur est solide. Tel le monstre du Loch Ness, la rumeur est réapparue plus forte que jamais ces jours-ci, suite à l'affaire Superfish.

Un risque grave pour la sécurité
L'affaire Superfish se corse car des chercheurs ont révélé un effet pervers majeur du logiciel superfish : il mettrait en péril le protocole de sécurisation SSL.

Le protocole SSL – abréviation de Secure Socket Layer – est une application des outils cryptographiques, largement utilisée pour les paiements électroniques en ligne, bien qu'il n'a pas été créé spécifiquement pour cela. Le système – intégré par défaut à presque tous les logiciels de navigation – crée un canal de communication sécurisé entre le serveur du vendeur et l'ordinateur du client, assurant entre eux la transmission cryptée des informations communiquées (par exemple : le numéro facial de la carte de crédit, la date d'expiration et le nom du titulaire).

Le protocole SSL présente principalement les avantages suivants :
• coût réduit : le protocole est intégré dans les logiciels récents de navigation sur l'internet (MS Internet Explorer, Netscape, Opera, etc.) et ne requiert donc pas d'équipement particulier ;
• simplicité d'utilisation : l'intégration au logiciel de navigation dispense l'acheteur de toute démarche particulière. La présence d'un logo représentant un cadenas fermé sur l'écran du logiciel confirme le recours à une transmission cryptée ;
• authentification du vendeur : le protocole SSL assure avant tout l'authentification du vendeur ce qui permet, dans une certaine mesure, de décourager les escrocs qui se font généralement vite repérer par les sociétés émettrices de cartes de crédit ;
• cryptage : l'utilisation de la cryptographie asymétrique permet de sécuriser les transmissions sur le réseau.

Toute médaille ayant son revers, ces avantages et la simplicité d'utilisation constituent également les principales faiblesses du système :
• il n'y a aucune vérification de l'identité du client ;
• le numéro apparent de la carte est transmis au vendeur, ce qui laisse subsister le risque d'une utilisation frauduleuse par ce dernier, ni ne résout le danger d'une intrusion dans le serveur du vendeur par un tiers désireux de faire main basse sur les informations bancaires des clients ;
• l'efficacité de la protection en cours de transmission dépend essentiellement de la clef de cryptage retenue.
• L'importance de SSL est considérable. S'il fallait l'exprimer en quelques mots, on pourrait dire qu'à l'heure actuelle, ce protocole protège quasiment toutes les transactions sur l'internet. Qu'il s'agisse d'acheter des billets de trains, de réserver un spectacle, de télécharger de la musique payante, de commander un livre … SSL est derrière l'immense majorité des opérations. Presque tous les sites qui opèrent le paiement par la transmission du numéro facial de carte de crédit, utilisent SSL. Ce protocole n'est pourtant pas le seul, mais il est le plus utilisé.

En raison de sa conception (recours à des certificats auto signés, en utilisant de surcroît la même clef privée sur tous les ordinateurs équipés de ce logiciel), le logiciel Superfish peut déchiffrer des connexions supposées sécurisées afin d'insérer des contenus publicitaires sans que l'utilisateur ne soit averti d'une telle intrusion, et briser ainsi la sécurité du protocole (plus d'infos en faisant une recherche sur votre moteur préféré avec les mots-clef « superfish ssl »).

Lenovo fait une courbe rentrante
Face au tollé général, le fabricant chinois a été contrainte de reconnaître les faits en les minimisant, et d'assurer que depuis ce mois de janvier, les nouvelles machines ne sont plus équipées de ce logiciel. (voir le communiqué http://news.lenovo.com/article_display.cfm?article_id=1929)

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.droit-technologie.org/actuality-1698/lenovo-accuse-d-infecter-ses-propres-pc-le-protocole-de-securise-ssl.html
Par Etienne Wery, Avocat aux barreaux de Bruxelles et Paris (cabinet Ulys)

Facebook devra s'expliquer devant la Commission de protection de la vie privée

Facebook devra s'expliquer devant la Commission de protection de la vie privée

Le réseau social a décidé d'être « clair » avec ses utilisateurs en affichant jusqu'où il allait dans leur vie privée. Une bonne volonté qui ne suffit pas à rassurer ceux-ci. Alain Jennotte a répondu à vos questions.

« Facebook devra s'expliquer devant la Commission de protection de la vie privée »
Une réunion a eu lieu entre le secrétaire d'Etat à la vie privée et des représentants de Facebook, qui ont nié que les données collectées sont transmises à des fins publicitaires. Est-ce exact ?
Facebook écrit certes noir sur blanc ses conditions d'utilisation, mais cela ne suffit pas. Il ne peut être exempté de respecter les lois sur la protection des données personnelles. Il n'y a d'ailleurs pas qu'en Belgique que la question du respect des règles par Facebook en matière de vie privée se pose.

Facebook a-t-il déjà revendu des données personnelles ?
Que fait Facebook des données ? Avec ses partenaires ? Avec les gouvernements ? C'est une question importante. Facebook met en place un réseau social et le valorise avec de la pub, donc il doit profiler les internautes pour pouvoir cibler. Facebook se défend de vendre des photos, mais ce qui est sûr c'est qu'il vend des profils, qui ont une énorme valeur, vu qu'il y a plus d'un milliard d'utilisateurs.

Peut-on encore parler de vie privée ?
Chaque fois qu'on se connecte, on laisse derrière soi une empreinte constituée d'un tas de détails donnés par ces appareils, et Facebook collecte toutes ces données. Le problème est qu'en additionnant toutes les données, on crée une empreinte numérique de plus en plus précise, tellement précise qu'on peut identifier l'appareil.

Pourquoi Facebook a-t-il sollicité Bart Tommelein ?
Facebook aurait dû répondre aux questions de la Commission de protection de la vie privée. Ce régulateur peut contraindre Facebook à s'expliquer. Facebook a choisi de solliciter le secrétaire d'Etat qui a tutelle sur le régulateur, pour faire en sorte qu'il tempère le dossier, mais Bart Tommelein a précisé à Facebook qu'il devrait s'expliquer devant la Commission.

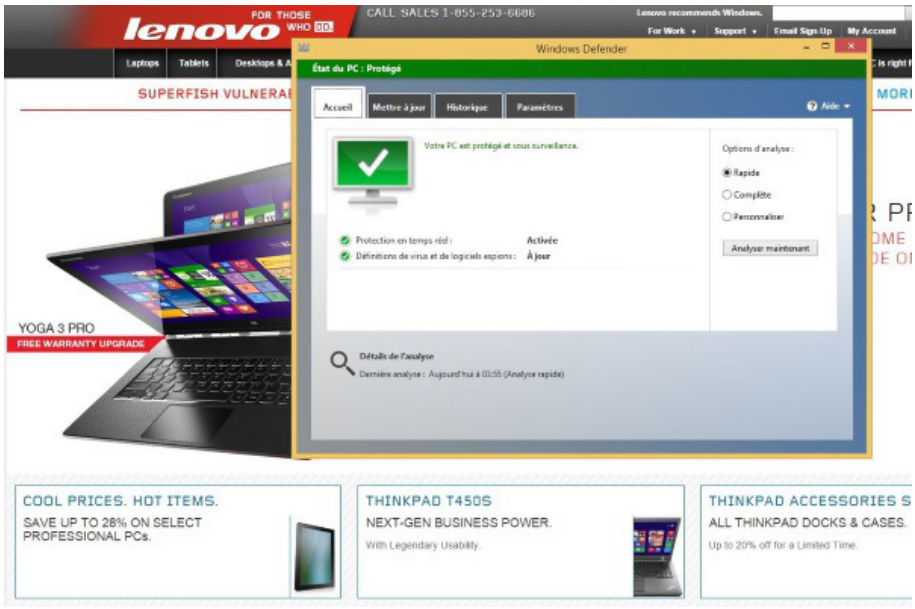
Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.lesoir.be/798498/article/economie/vie-du-net/2015-02-18/11h02-qu-on-y-soit-inscrit-ou-pas-on-est-rattrape-par-facebook

---

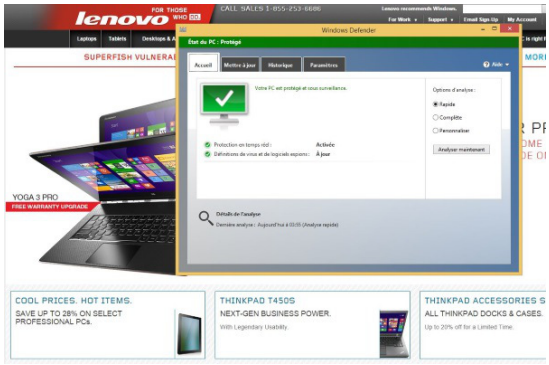
Les ordinateurs Lenovo

contaminés d’usine…



Les ordinateurs Lenovo contaminés d’usine…

Possédez-vous un ordinateur grand public récent vendu par Lenovo? Si oui, il y a de fortes chances pour que votre appareil ait été livré avec Superfish, un logiciel publicitaire dangereux, qui pourrait notamment permettre à des pirates malintentionnés d'accéder à vos connexions web sécurisées. S'il était jusqu'ici difficile de se prémunir contre cette faille, Microsoft et Lenovo viennent de simplifier la chose, grâce à une mise à jour rapide de l'antivirus Windows Defender et à la mise en ligne d'un outil pour enlever le logiciel.C'est une semaine difficile qui se termine pour Lenovo, qui a volontairement équipé tous ses ordinateurs grand public vendus entre septembre 2014 et janvier 2015 de ce logiciel. Superfish n'a toutefois jamais été installé sur les ordinateurs ThinkPad et les ordinateurs pour entreprises de la compagnie.Pire, même si Lenovo a publié hier sur son site web un tutoriel pour expliquer comment enlever Superfish de ses ordinateurs, ce processus manuel ne corrige pas complètement le problème pour les ordinateurs déjà infectés.
C'est plutôt Microsoft qui a pris la chose en mains en premier aujourd'hui, avec une mise à jour de son antivirus Windows Defender, qui permet de désinstaller Superfish, en plus de mettre à jour les certificats SSL de l'ordinateur. Il suffit donc de mettre à jour Windows Defender et d'analyser son appareil pour s'en débarrasser.



Lenovo a finalement aussi publié un outil vendredi en soirée pour enlever convenablement Superfish. Celui-ci peut être télécharger automatiquement ici.
Les propriétaires d'un ordinateur Lenovo qui souhaitent savoir si leur appareil est affecté par Superfish peuvent suivre ce lien directement.
Voici la liste complète, mais peut-être pas exhaustive, des ordinateurs Lenovo livrés avec Superfish :
E-Series:
E10-30
Flex-Series:
Flex2 14, Flex2 15
Flex2 14D, Flex2 15D
Flex2 14 (BTM), Flex2 15 (BTM)
Flex 10
G-Series:
G410
G510
G40-70, G40-30, G40-45
G50-70, G50-30, G50-45
M-Series:
Miix2 – 8
Miix2 – 10
Miix2 – 11
S-Series:
S310
S410
S415; S415 Touch
S20-30, S20-30 Touch
S40-70
U-Series:
U330P
U430P
U330Touch
U430Touch
U540Touch
Y-Series:
Y430P
Y40-70
Y50-70
Yoga-Series:
Yoga2-11BTM
Yoga2-11HSW
Yoga2-13
Yoga2Pro-13
Z-Series:
Z40-70
Z40-75
Z50-70
Z50-75

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://journalmetro.com/opinions/vie-numerique/724584/securite-informatique-microsoft-sattaque-a-superfish/
Par Maxime Johnson

Le « shaming » sur le Net va-t-il trop loin?

Le « shaming » sur le Net va-t-il trop loin?

Les réseaux sociaux ont ceci de réjouissant: ils montrent que, face aux injustices, les citoyens ont pleinement gardé leur capacité d'indignation. Mais ils deviennent inquiétants quand la virulence parait, soudain, hors de proportion.

Le « shaming », c'est l'humiliation publique à l'ère du web 2.0. Le weekend dernier, le New York Times publiait un long article sur l'affaire Justine Sacco, survenue il y a un an et qui reste un cas d'école. Responsable de la communication d'un groupe de médias, à New York, Justine Sacco, 30 ans, embarque sur un vol vers Le Cap en Afrique du Sud. En escale à Londres, elle tweete une mauvaise blague raciste (que je vous épargne).
Quand elle arrive au Cap, elle découvre, en réponse, des dizaines de milliers de tweets la prenant à partie. Quelques internautes sont même allés l'attendre à l'aéroport. Son téléphone portable déborde de messages. En quelques heures, Justine Sacco s'est retrouvée au centre d'une vague d'indignation mondiale. Elle perd son boulot et quelques amis.
Le New York Times l'a rencontrée ainsi que l'homme qui, le premier, avait dénoncé son tweet. Il dit qu'à ses débuts sur Twitter, cette « colère collective » lui semblait juste et efficace. Les réseaux sociaux permettaient de « briser les hiérarchies sociales ». Mais aujourd'hui, dit-il, le « shaming » est devenu « une fin en soi », une « punition jubilatoire ».


Mail Online

'I lost my job, my reputation and I'm not able to date anymore': Former PR worker reveals how she destroyed her life one year after sending 'racist' tweet before trip to Africa

- Justine Sacco, 30, from New York, became a global hate figure
- Thousands angered by tweet sent by the PR consultant
- She said tweet to her 170 followers was misinterpreted
- She lost her job and was trolled by thousands

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.rtbf.be/info/emissions/article_le-journal-du-web-le-shaming-sur-le-net-va-t-il-trop-loin?id=8910669

Cybercriminalité : Une stagiaire dérobe 1 million de FCFA à son patron

Cybercriminalité : Une stagiaire dérobe 1 million de FCFA à son patron

Mardi 17 février 2015-Kadija Koné stagiaire dans une agence Rechercher agence de transfert d'argent a été épinglée par la Police de Lutte contre la Cybercriminalité (PLCC), pour escroquerie Rechercher escroquerie , faux et usage de faux Rechercher faux et usage de faux portant sur la somme d'un 1000 000 FCFA dérobé à son patron.

En effet, et pour subvenir aux soucis financiers de son ex compagnon, la stagiaire en question a frauduleusement retiré la somme de 1 581 550 FCFCA, sur le compte géré par son patron entre septembre 2014 et janvier 2015. Le patron ayant constaté les faits a avisé la PLCC Rechercher PLCC et porter plainte contre X.
Après enquêtes, la PLCC Rechercher PLCC a fini par mettre le grappin sur Kadija Koné, qui d'ailleurs ne mettra aucune difficulté pour reconnaitre les faits qui lui sont reprochés.
« Je voulais octroyer un prêt à usure à mon ex copain. J'ai retiré 1 000 000 FCFA sur le compte géré par mon patron. En retour et comme convenu j'ai reçu en récompense un acompte de 450 000 FCFA, ensuite mon ex devait me rembourser à hauteur de 1 200 000 FCFA », aurait-elle révélé dans les locaux de la PLCC. La stagiaire a été déférée devant le parquet pour escroquerie, faux et usage de faux.
Selon la nouvelle loi sur la cybercriminalité, cette dernière risquerait une peine allant jusqu'à 20 ans de prison ferme, et une amende de 40 millions de FCFA.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://koaci.com/cote-divoire-cybercriminalite-stagiaire-derobe-million-fcfa-patron-pour-aider-copain-elle-risque-prison-98895.html
Par Donatien Kautcha, Abidjan