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.

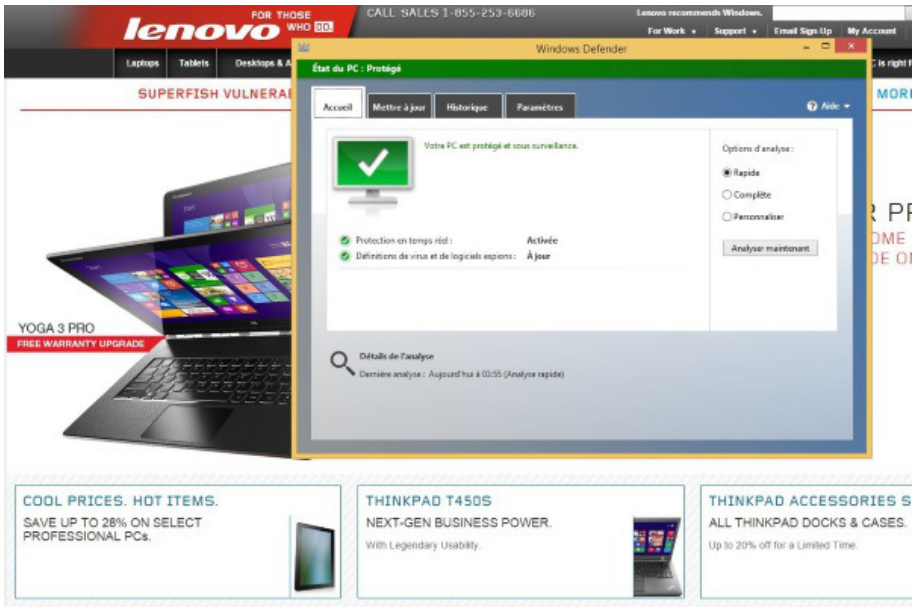
Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

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

---

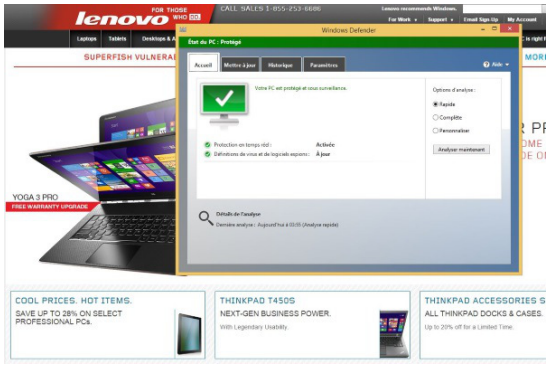
Les ordinateurs Lenovo

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

Le système de suivi numérique des passagers aériens prêt en fin d’année

Seul, le Royaume-Uni a déjà commencé à alimenter une base PNR. (Crédit D.R.)

Le système de suivi numérique des passagers aériens prêt en fin d’année

Malgré les incertitudes sur le respect de la vie privée et les doutes sur son utilité, le projet de suivi des passagers qui entrent ou sortent de l'Union européenne à travers une série de bases de données nationales devrait devenir réalité d'ici la fin de l'année. Au Parlement européen, seuls les Verts s'y opposent encore.

Depuis les récentes attaques terroristes à Paris et Copenhague au cours desquelles 19 personnes ont été tuées, la volonté de créer des bases de données nationales ayant accès aux données des dossiers passagers (ou PNR pour Passenger Name Record) s'est encore accentuée.
Les pays de l'Union européenne ont fait valoir que le stockage de données pour suivre les déplacements des personnes, permettrait de mieux appliquer la loi en matière de prévention, de détection, d'investigation et de poursuite des infractions terroristes et de la criminalité transnationale.
Selon les termes du projet, les compagnies aériennes devront envoyer les données PNR qu'elles recueillent lors des procédures de réservation et d'enregistrement d'un vol par un passager, y compris son itinéraire de voyage, les informations sur le billet et ses détails de contact, à une autorité du pays concerné. Cette autorité sera chargée d'analyser les données et de partager ses résultats avec d'autres autorités compétentes, en Europe et dans d'autres pays. Si certains pays comme le Royaume-Uni disposent déjà d'une base de données PNR, ce n'est pas le cas pour d'autres. Et il n'existe actuellement aucun système pour partager cette information. Jeudi dernier, lors d'une réunion informelle sur le terrorisme, les chefs d'État et de gouvernement européens ont convenu de poursuivre les discussions pour doter l'UE d'un tel système. « Nous avons défini de nouvelles priorités en matière de lutte contre le terrorisme. En premier lieu, nous devons trouver un accord sur l'échange des informations sur les passagers dans l'Union européenne. Et nous en avons besoin rapidement », a déclaré dans un communiqué le président du Conseil européen, Donald Tusk. Les chefs d'État ont demandé aux législateurs de l'UE d'adopter d'urgence une directive PNR européenne forte et efficace avec de solides garanties pour la protection des données.

Le Parlement européen prêt à finaliser le projet PNR
Dans le cas présent, la protection des données est une question clef. En 2013, un précédent projet d'échange de données sur les passagers entre pays de l'UE avait été rejeté par le Parlement européen, au motif que ces dispositions pouvaient empiéter sur les droits fondamentaux. Mais depuis les derniers attentats, la Commission européenne a modifié le projet pour convaincre le Parlement d'aller de l'avant, promettant une meilleure protection de la vie privée. Et cela semble avoir porté ses fruits. Mercredi dernier, avant la réunion du Conseil, le Parlement avait adopté une résolution par laquelle il s'engageait à travailler « à la finalisation d'une directive PNR de l'UE d'ici la fin de l'année ». Le Parlement veut s'assurer que la collecte et le partage des données seront conformes à un cadre cohérent en terme de protection des données et qu'il comportera des obligations de protection des données personnelles juridiquement contraignantes au sein de l'UE.

Les opposants au projet d'accès aux données des dossiers passagers avaient contesté sa légalité, car dans son objectif, les questions posées sont similaires à celle d'une directive européenne invalidée par la Cour de justice européenne (CJUE). En effet, la Cour de justice avait invalidé une directive sur la conservation des données, ou Data Retention Directive, qui demandait aux opérateurs de télécommunication de conserver les informations sur la destination et la durée des communications, au motif qu'elle portait atteinte à des droits fondamentaux à la vie privée. L'utilité d'un système PNR a également été remise en question par les opposants, lesquels affirment qu'un tel système n'aurait pas empêché les attentats de Paris. « En plaidant pour une directive européenne PNR, le Parlement veut pousser l'UE vers une plus grande centralisation des données et plus de rétention de données, sans motif établi, et en ignorant la jurisprudence de la CJUE », a déclaré mercredi dernier dans un blog Alexander Sander, le directeur général du groupe de défense des droits digitaux allemand Digitale Gesellschaft.

Les Verts font toujours bande à part
Au sein du Parlement, seul le parti des Verts s'oppose encore à un système PNR au niveau européen. Plutôt que d'investir 500 millions d'euros dans la surveillance des passagers aériens, les Verts demandent que cet argent soit dépensé pour le travail de terrain et la coopération entre la police et les autorités de sécurité. Mais sa représentation sera insuffisante pour faire pencher la balance. Dans le même temps, les chefs d'État de l'UE ont estimé que la loi devait renforcer le partage d'informations et la coopération opérationnelle, et que la coopération des services de sécurité entre les pays membres devait également être accentuée. Par ailleurs, ils ont convenu que les autorités devaient intensifier leur action de traçage des flux financiers et geler les actifs utilisés pour financer le terrorisme. La détection et la suppression des contenus Internet faisant l'apologie du terrorisme, en coopération avec des entreprises Internet, est également une priorité pour les États membres. En avril, date à laquelle la Commission présentera ses plans sur la sécurité, le projet devrait franchir une nouvelle étape. C'est au mois de juin que le Conseil devrait exposer en détail comment seront mises en oeuvre les mesures proposées.

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

Source : http://www.lemondeinformatique.fr/actualites/lire-ue-le-systeme-de-suivi-des-passagers-aeriens-pret-en-fin-d-annee-60253.html
Par Jean Elyan

Une attaque « très sophistiquée » cible une centaine de banques – 1 milliard de dollars dérobés…

Une attaque « très sophistiquée » cible une centaine de banques – 1 milliard de dollars dérobés…

Des pirates se sont infiltrés dans les systèmes d'information d'une centaine de banques en 2013, ont dérobé au moins 300 millions de dollars, et agissent encore aujourd'hui, apprend Kaspersky.

C'est l'une des cyberattaques les plus sophistiquées jamais identifiées par Kaspersky. L'éditeur de solutions antivirus russe a dévoilé auprès du New York Times, lundi, les résultats d'une enquête menée depuis 2013 en partenariat avec Interpol et Europol. Conclusions : de 300 millions à 1 milliard de dollars ont été dérobés à une centaine de banques dans trente pays. Active depuis près de deux ans, la cyberattaque a toujours cours.

Pour ces raisons, l'éditeur reste volontairement imprécis sur les informations divulguées, ne fournissant pas, par exemple, le nom des établissements concernés. Les institutions sont basées principalement en Russie, au Japon, aux Etats-Unis et en Suisse. D'après le quotidien américain, JP Morgan Chase figure parmi les cibles.
Ce cybergang basé en Russie, Chine et Ukraine, « a franchi un nouveau cap » dans la méthode employée, souligne Kaspersky, en dérobant des fonds aux banques sans avoir à passer par les clients. L'attaque aurait débuté avec des infections classiques par hameçonnage, quand des employés de banque téléchargeaient malgré eux sur leur poste le malware nommé « Carbanak » – c'est également le nom de ce groupe de pirates.

Observer et imiter les transferts d'argent
Une fois bien installés sur les ordinateurs chargés des transferts de fonds ou de la compatibilité, il peuvent observer discrètement et patiemment les routines des employés et les processus des banques. Les pirates remontent ensuite sur les machines des responsables des transferts et des comptes, où ils installent un outil d'administration à distance (RAT) afin d'en prendre le contrôle et « d'imiter les activités normales ».
Ainsi, les assaillants peuvent créer de faux comptes pour y transférer de l'argent, a priori sans éveiller de soupçons. Si le hameçonnage n'a rien d'exceptionnel en soi, c'est l'aspect méthodique et la patience des pirates que Kaspersky pointe du doigt dans son rapport. De quoi leur avoir évité de s'être fait pincer à ce jour.
Ce qui a déclenché l'enquête remonte à la fin 2013 lorsqu'un distributeur s'est mis à émettre des billets en plein Kiev, en Ukraine. Alertée, la banque concernée a alors missionné Kaspersky. Lequel découvrira assez tôt que cette avarie allait en fait devenir, comparé à l'ampleur de la cyberattaque, le dernier souci de la banque.

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

S o u r c e
http://pro.clubic.com/it-business/securite-et-donnees/actualite-754433-kaspersky-cyber-attaque-banques.html?&svc_mode=M&svc_campaign=NL_ClubicPro_New_17/02/2015&partner=-&svc_position=86524329&svc_misc=-&crmID=639453874_86524329&estat_url=http%3A%2F%2Fpro.clubic.com%2Fit-business%2Fsecurite-et-donnees%2Factualite-754433-kaspersky-cyber-attaque-banques.html

---

Vous allez pouvoir décider du sort de votre Facebook après votre mort

Vous allez pouvoir décider du sort de votre Facebook après votre mort

Le réseau social va vous permettre de nommer un légataire pour qu'il puisse gérer votre page après votre décès. Il aura accès à presque tout sauf aux messages privés.

Facebook pense à tout, même à votre vie après la mort. Le plus gros réseau social du monde a déployé jeudi une mise à jour qui permet de désigner un « légataire », permettant de prendre le contrôle du profil du défunt et même de publier des messages en son nom.
« Facebook est un endroit pour partager et se rapprocher de sa famille et de ses amis. Et, pour plusieurs d'entre nous, il s'agit d'un endroit pour se souvenir et rendre à hommage à ceux qui nous ont quittés », a annoncé le réseau social sur son blog (en anglais).

Aucun accès aux messages privés
Auparavant, Facebook créait une page commémorative lorsqu'elle était informée du décès d'un membre, mais celle-ci ne pouvait être gérée par une tierce personne. Mais « après avoir parlé avec des gens qui ont vécu la perte d'un proche, nous avons réalisé que nous pouvions en faire davantage pour les personnes endeuillées et pour ceux qui veulent garder le contrôle sur leur compte après leur mort ».
Pour les utilisateurs qui le désirent, le « légataire » pourra publier un message afin d'annoncer un service funéraire ou partager un message spécial. La personne qui gère le compte pourra aussi mettre le profil à jour et changer la photo de couverture, ainsi que répondre aux demandes d'amitié de membres de la famille et d'amis qui n'étaient pas encore connectés.

Problème de stockages de données personnelles
En désignant un légataire, le membre pourra aussi donner la permission de télécharger les photos, ainsi que l'information du profil partagés sur Facebook. Cependant, « le légataire ne pourra se connecter directement au compte du défunt ou voir ses messages privés. »
L'annonce survient au moment où l'inquiétude croît quant au sort des « avoirs numériques » après la mort. Des experts légaux indiquent que la propriété des données stockées dans le « cloud » (dans les serveurs de Facebook), les courriels et les archives en ligne de musique et de livres demeurent sujets à interprétation. Par ailleurs, des utilisateurs remontent régulièrement à quel point les pages de proches décédés peuvent être une source de tristesse quand elles restent en ligne après leur mort.

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

S o u r c e :
http://lexpansion.lexpress.fr/high-tech/facebook-pense-a-votre-vie-apres-la-mort_1651127.html?PMSRC_CAMPAIGN=20150217130355_08_nl_lexpansion_high_tech_11437&xtor=EPR-3125-%5B20150217130355_08_nl_lexpansion_high_tech_11437_000YKDN5D-20150217-%5B_____Vous_allez_pouvoir_decider_du_sort_de_votre_Facebook_apres_votre_mort_____002TC1L%5D-20150217120800#LBdEJLMBMIkXokbR.99

La CNIL place un conseiller pour encadrer le blocage de sites terroristes

La CNIL place un conseiller pour encadrer le blocage de sites terroristes

Dans le but d'encadrer le blocage de sites faisant l'apologie du terrorisme, la CNIL a nommé un magistrat en tant que conseiller honoraire à la Cour de cassation.

Le blocage des sites internet faisant l'apologie du terrorisme est une mesure contestée par les défenseurs des libertés sur le net. C'est sa nature qui laisse penser à une censure du web, d'autant plus que ce dispositif administratif n'a pas besoin de l'intervention d'un juge, qui fait débat.
Pour replacer un représentant de la loi au centre de ce dispositif contesté, la Commission nationale de l'informatique et des libertés (CNIL) vient de nommer Alexandre Linden en tant que conseiller honoraire à la Cour de cassation. Le rôle de ce magistrat sera d'encadrer le blocage des sites internet faisant l'apologie du terrorisme, une manière détournée de placer un représentant de la loi pour juger de la pertinence de chaque mesure.
Alors qu'une première liste de 10 à 50 URL doit être soumise à l'Unité de coordination de la lutte antiterroriste, les décrets publiés le 6 février dernier précisent que l'office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC) est chargé de mettre en œuvre la loi. Les fournisseurs d'accès auront 24 heures pour bloquer l'accès à ces sites suite à la décision de l'office.
Alexandre Linden aura donc son mot à dire dans ces décisions, mais reste à savoir les moyens qu'il aura à disposition pour agir.

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

Source : http://www.linformatique.org/la-cnil-place-un-conseiller-pour-encadrer-le-blocage-de-sites-terroristes/