La Cnil épingle Windows 10 sur la collecte des données personnelles

	La Cnil épingle Windows 10 sur la collecte des données personnelles

Constatant plusieurs manquements dont la collecte de données excessives et non pertinentes par Windows 10, la Cnil a mis en demeure Microsoft de se conformer à la loi dans un délai de 3 mois.

A quelques jours de la fin de la gratuité pour migrer sur Windows 10, la Cnil s'invite dans le débat sur le dernier OS de Microsoft. Et le moins que l'on puisse dire est que le régulateur n'est pas content des méthodes de l'éditeur américain. Elle vient de mettre en demeure Microsoft de se conformer dans un délai de 3 mois à la Loi Informatique et Libertés.

Alertée sur la collecte de données de Windows 10 (dont nous nous étions fait l'écho à plusieurs reprises : « pourquoi Windows 10 est une porte ouverte sur vos données personnelles » ou « Windows 10 même muet il parle encore »), la Cnil a effectué une série de contrôles entre avril et juin 2016 pour vérifier la conformité de Windows 10 à la loi.

De ces contrôles, il ressort plusieurs manquements. Le premier concerne une collecte des données excessives et non pertinentes. Elle reproche par exemple à Microsoft de connaître quelles sont les applications téléchargées et installées par un utilisateur et le temps passé par l'utilisateur sur chacune d'elles. Microsoft s'est toujours défendu de collecter des données personnelles en mettant en avant des relevés de « télémétrie » pour améliorer son produit.

Défaut de sécurité, absence de consentements et référence au Safe Harbor

Autre point soulevé par le régulateur, un défaut de sécurité a été trouvé dans le code PIN à 4 chiffres. Ce dernier est utilisé pour s'authentifier sur l'ensemble des services en ligne. Or le nombre de tentatives de saisie du code PIN n'est pas limité.

De plus, la Cnil constate une absence de consentement des personnes notamment sur le ciblage publicitaire lors de l'installation de Windows 10. Idem pour le dépôt de cookies déposés sur les terminaux des utilisateurs.

Enfin, cerise sur le gâteau, Microsoft est enjoint par la Cnil d'arrêter de se baser sur le Safe Harbor pour transférer les données personnelles aux Etats-Unis. Cet accord a été invalidé par la Cour de Justice de l'Union européenne en octobre 2015. Il a été remplacé par le Privacy Shield qui doit bientôt rentrer en vigueur.

La balle est maintenant dans le camps de Microsoft.

Article original de Jacques Cheminat

Réagissez à cet article

Original de l'article mis en page : La Cnil épingle Windows 10 sur la collecte des données

Détecter les futurs terroristes sur Internet ? L’Europe veut s’inspirer d’Israël

Détecter les futurs terroristes sur Internet ? L’Europe veut s’inspirer d’Israël

Le coordinateur de l'anti-terrorisme pour lUnion européenne, Gilles de Kerchove, s'est rendu en Israël pour trouver des solutions technologiques qui permettraient de détecter automatiquement des profils suspects sur les réseaux sociaux, grâce à des algorithmes de plus en plus intrusifs.

Plus les attentats en Europe se multiplient, plus on découvre que les profils psychologiques et sociaux des kamikazes et de leurs associés sont très divers, jusqu'à paraître indétectables. Le cas de Mohamed Lahouaiej-Bouhlel, dont on ne sait pas toujours très bien s'il s'agit d'un déséquilibré qui se cherchait un modèle ultra-violent à imiter, ou d'un véritable djihadiste islamiste radicalisé à une vitesse inédite, laisse songeur. Bisexuel, amant d'un homme de 73 ans, mangeur de porc, aucune connexion connue avec des réseaux islamistes… l'auteur de l'attentat de Nice était connu des services de police pour des faits de violence de droit commun, mais n'avait rien de l'homme que l'on pourrait soupçonner d'organiser une tuerie motivée par des considérations idéologiques.
Or c'est un problème pour les services de renseignement à qui l'on demande désormais l'impossible, à la Minority Report, c'est-à-dire de connaître à l'avance le passage à l'acte d'un individu, pour être capable de l'appréhender avant son méfait, même lorsqu'objectivement rien ne permettait de présager l'horreur.

C'EST POUR ÇA QUE JE SUIS ICI. NOUS SAVONS QU'ISRAËL A DÉVELOPPÉ BEAUCOUP DE MOYENS DANS LE CYBER

Néanmoins, l'Union européenne ne veut pas se résoudre à la fatalité, et va chercher en Israël les méthodes à appliquer pour détecter sur Internet les terroristes susceptibles un jour de passer à l'acte. « C'est un défi », explique ainsi à l'agence Reuters Gilles de Kerchove, le coordinateur de l'UE pour l'anti-terrorisme, en marge d'une conférence sur le renseignement à Tel Aviv. « Nous allons trouver bientôt des moyens d'être beaucoup plus automatisé » dans la détection des profils suspects sur les réseaux sociaux, explique-t-il. « C'est pour ça que je suis ici ».
« Nous savons qu'Israël a développé beaucoup de moyens dans le cyber », pour faire face aux attaques d'Israéliens par des Palestiniens, ajoute le haut fonctionnaire européen, et l'UE veut s'en inspirer.

ÉTABLIR DES PROFILS SOCIOLOGIQUES ET SURVEILLER LES COMMUNICATIONS

Selon un officiel israélien interrogé par l'agence de presse, il s'agit d'établir constamment des profils types de personnes à suspecter, en s'intéressant non plus seulement aux métadonnées qui renseignent sur le contexte des communications et les habitudes d'un individu, mais bien sur le contenu-même des communications sur les réseaux sociaux.
Mis à jour quotidiennement au gré des nouveaux profils qui émergent, des paramètres comme l'âge de l'internaute, sa religion, son origine socio-économique et ses liens avec d'autres suspects, seraient aussi pris en compte par les algorithmes israéliens – ce qui semble difficilement compatible en Europe avec les textes internationaux protégeant les droits de l'homme, que l'Union européenne s'est engagée à respecter.

DES BOÎTES NOIRES TOUJOURS PLUS INTRUSIVES ?

En somme, c'est exactement ce que nous redoutions avec les fameuses boîtes noires permises par la loi Renseignement en France, dont le Conseil constitutionnel n'a su que dire, et qui se limitent officiellement aux métadonnées. Là aussi, il s'agit d'utiliser des algorithmes, dont on ne sait pas du tout sur quoi ils se basent, pour détecter des profils suspects.

Eagle Security & Defense, une société israélienne proposant des solutions de surveillance sur Internet, a reçu la visite de Christian Estrosi en début d'année.
Il n'est toutefois pas dit que la technologie israélienne soit importée telle quelle, d'autant que M. De Kerchove a lui-même rappelé que le droit européen n'autoriserait pas un tel degré d'intrusion dans la vie privée. Mais le mécanisme décrit par l'officiel d'Israël est très proche.
Il vise tout d'abord à réaliser une première détection sommaire des profils suspects, puis à déterminer parmi eux ceux qui doivent faire l'objet d'une surveillance individualisée. C'est exactement ce que prévoit la loi Renseignement, qui autorise l'installation de boîtes noires chez les FAI ou les hébergeurs et éditeurs pour détecter des comportements suspects d'anonymes, avant de permettre une identification des personnes dont il est confirmé qu'elles méritent une attention particulière.
En Israël, le ratio serait d'environ 20 000 personnes considérées suspectes pour 1 million d'internautes, sur lesquelles ressortiraient entre 10 et 15 profils nécessitant une surveillance étroite.

CHRISTIAN ESTROSI DÉJÀ INTÉRESSÉ

L'information de Reuters confirme ce qu'indiquaient Les Échos le week-end dernier dans un reportage bien informé. « L'Etat hébreu, dont la population a connu sept guerres et deux Intifada depuis sa création, est bel est bien devenu un cas d'école, dans sa façon de gérer une situation d'insécurité permanente. Une expertise dans la mire des décideurs européens », écrivait le quotidien,
Il précisait qu'en février dernier, l'ancien maire de Nice et actuel président de la région Provence-Alpes-Côte d'Azur, Christian Estrosi, s'était déjà rendu en Israël, où il aurait rencontré le PDG de la société Eagle Security and Defense, Giora Eiland, qui est aussi ex-directeur du Conseil de sécurité nationale israélien.
Lors de cette visite, Christian Estrosi aurait insisté sur la nécessité « d'être à la pointe de la lutte par le renseignement contre la cybercriminalité lorsqu'on sait que la radicalisation se fait par le biais des réseaux sociaux ». On imagine que cette conversation lui est revenue en mémoire lorsque sa ville a été meurtrie.
Article original de Guillaume Champeau

Réagissez à cet article

Original de l’article mis en page : Détecter les futurs terroristes sur Internet ? LEurope veut sinspirer dIsraël – Politique – Numerama

---

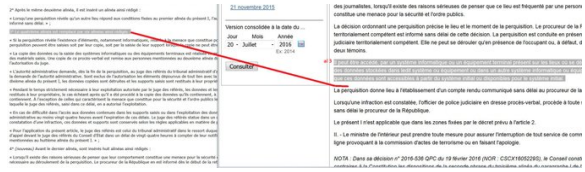
État d’urgence : la police pourra bien copier des données trouvées dans le Cloud

État d’urgence : la police pourra bien copier des données trouvées dans le Cloud

---

Contrairement à ce que nous écrivions mardi avec étonnement, il sera bien possible pour la police d'utiliser l'ordinateur ou le smartphone d'un suspect pour accéder à tous ses services en ligne, puis de copier les informations obtenues pour les exploiter si elles sont pertinentes.

Il faudrait toujours retourner son clavier sept fois sur le bureau avant de donner un satisfecit au gouvernement. Mardi, nous détaillions le cadre prévu dans le projet de loi de prorogation de l'état d'urgence, pour la copie des données informatiques dont Manuel Valls avait annoncé le retour. Il fallait vérifier si les exigences du Conseil constitutionnel en matière de respect de la vie privée étaient bien respectées.
À cette occasion, nous faisions remarquer à tort que le gouvernement n'avait pas prévu la possibilité de copier des données stockées dans les services en ligne des suspects, se limitant curieusement aux seules « *données contenues dans tout système informatique présent sur les lieux de la perquisition* ».
Pris dans un élan de naïveté, nous n'avions pas fait attention au fait que l'ensemble du dispositif n'était pas réécrit, et que le gouvernement avait laissé intacte une disposition non censurée par le Conseil constitutionnel, qui change toute l'analyse. Elle dit qu'en cas de perquisition administrative, « *il peut être accédé, par un système informatique ou un équipement terminal présent sur les lieux où se déroule la perquisition, à des données stockées dans ledit système ou équipement ou dans un autre système informatique ou équipement terminal, dès lors que ces données sont accessibles à partir du système initial ou disponibles pour le système initial* ». Créé en novembre 2015, cet alinéa de l'article 11 de la loi du 3 avril 1955 relative à l'état d'urgence n'a pas été supprimé, comme le fait justement remarquer Marc Rees deNext Inpact :
Voir l'image sur Twitter



Suivre

marc rees @reesmarc
. @p_estienne j'ajoute que PJL #EtatdUrgence ne supprime pas accès au cloud cc @gchampeau (gauche PJL droite, L55)
11:03 – 20 Juil 2016
•
•
77 Retweets
•
1 j'aime
Il reste donc possible pour la police d'accéder sur place à toutes données disponibles sur le Cloud, en profitant des sessions ouvertes sur des services en ligne (ou dont le mot de passe est mémorisé). Dès lors, à partir du moment où ils sont affichés à l'écran ou téléchargés, ces messages Facebook, e-mails, documents Google Docs, historiques WhatsApp ou autres fichiers stockés à distance deviennent bien des « *données contenues dans tout système informatique présent sur les lieux de la perquisition* », qui peuvent être copiées et analysées après autorisation du juge, dans le cadre désormais fixé.
Article original de Guillaume Champeau

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Original de l'article mis en page : État d'urgence : la police pourra bien copier des données trouvées dans le Cloud – Politique – Numerama

Les campagnes de sensibilisation à la cybersécurité portent (petit à petit) leurs fruits

Les campagnes de sensibilisation à la cybersécurité portent (petit à petit) leurs fruits

Une étude souligne que les primo-adoptants de nouvelles technologies demandent l'autorisation avant d'amener de nouveaux équipements au travail.

Sachant que plus de 25 % des attaques identifiées en entreprise devraient associer l'Internet des objets d'ici à 2020 [1] et, pour nombre d'entre elles, s'inviter sur le lieu de travail, les conclusions de cette étude marquent une évolution significative dans la bonne direction et prouvent que les collaborateurs cernent mieux le rôle qui leur incombe dans le domaine de la cybersécurité.
Néanmoins, les résultats de cette enquête menée auprès de cadres en entreprise – les plus susceptibles, de par leur rémunération et leur état d'esprit, à être des primo-adoptants des nouvelles technologies – sont contrastés puisque 39 % d'entre eux auraient tendance à se soustraire au contrôle du service informatique. Ce qui laisse une énorme marge de risque.
Pire, parmi les collaborateurs qui se disent prêts à court-circuiter le service informatique, un sur huit « ne révélerait à personne » son intention d'introduire un nouvel appareil au sein de l'entreprise ou d'installer un outil professionnel, messagerie électronique par exemple, sur un équipement non sécurisé.

L'attitude a une incidence sur le respect des règles
L'étude révèle que le respect des règles de cybersécurité, telles que celles concernant l'introduction d'un nouvel équipement, est largement fonction des attitudes et opinions de chacun vis-à-vis de la technologie. Les professionnels ayant dérogé, dans le passé, aux règles de cybersécurité de leur entreprise justifient essentiellement leur geste par leur volonté de recourir à un outil ou un service plus efficace, ou considéré à l'époque comme le meilleur sur le marché. Les entreprises doivent élargir, et non restreindre, le choix de leurs collaborateurs, en s'appuyant sur la technologie et la formation pour gérer les risques.

Les intérimaires exigent une surveillance à temps complet
Les sous-traitants constituent le groupe contournant le plus souvent les règles de cybersécurité, 16 % des participants affirmant avoir vu un intérimaire se soustraire à celles-ci.
« Le concept BYOD a beau aujourd'hui avoir fait ses preuves, nombre d'individus continuent à éprouver des difficultés à dissocier clairement l'accès aux données personnelles de celui aux données professionnelles sur les appareils leur appartenant. Quantité d'entreprises ont déployé des solutions d'administration pour leur parc d'équipements, mais c'est la connectabilité de ces derniers qui pose véritablement problème, d'autant que la ligne de démarcation entre les services cloud orientés métier et les services personnels s'estompant, des passerelles méconnues sont jetées entre les réseaux d'entreprise et l'Internet en général. Une sécurité dernier cri doit être en mesure d'empêcher que toute communication à partir d'un équipement ne se transforme en faille et diminuer le plus possible les risques encourus par l'entreprise. » Greg Day, vice-président et responsable de la sécurité (CSO) pour la zone Europe, Moyen-Orient et Afrique (EMEA) chez Palo Alto Networks

Recommandations
Les entreprises doivent poursuivre leurs actions de sensibilisation auprès de leurs collaborateurs afin de faire en sorte que ceux positionnés en première ligne défensive possèdent les compétences nécessaires pour déceler les menaces.
Les professionnels de la sécurité doivent encadrer étroitement les activités des collaborateurs non permanents ou des sous-traitants, et veiller à ce que leur soient communiquées les mêmes informations que celles dispensées au personnel à temps complet.
Les entreprises doivent intégrer des solutions de sécurité modernes, en harmonie avec les nouvelles évolutions technologiques, afin d'écarter les fragilités inhérentes à un environnement informatique en constante évolution.
Les entreprises doivent réfléchir à la façon dont elles recensent et favorisent l'utilisation, dans de bonnes conditions de sécurité, d'applications et de services cloud dignes de confiance ou approuvés par leurs soins, et gèrent celle de ceux qu'elles ne jugent pas dignes de leur confiance ou n'avalisent pas.
Méthodologie de recherche
L'enquête a été menée en ligne, par Redshift Research en octobre 2015, auprès de 765 décideurs d'entreprises comptant plus d'un millier de salariés au Royaume-Uni, en Allemagne, en France, aux Pays-Bas et en Belgique.
Article original de edubourse.com

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Original de l'article mis en page : Les campagnes de sensibilisation à la cybersécurité portent (petit à petit) leurs fruits

---

Trois histoires vrais de vies inquiétées par du piratage informatique ciblé

Trois histoires vrais de vies inquiétées par du piratage informatique ciblé

L'expérience le prouve : même les vieux habitués d'Internet n'arrivent pas toujours à se protéger des piratages ciblés. Étant donné que notre vie quotidienne devient de plus en plus connectée à Internet et à d'autres réseaux, la sécurité en ligne s'est convertie comme un besoin impératif.

La plupart d'entre nous ont un email, un compte sur les réseaux sociaux et une banque en ligne. On commande sur le web, et utilisons notre mobile pour nous connecter à Internet (par exemple, dans les solutions de l'authentification à deux facteurs) et pour d'autres choses tout aussi importantes. Malheureusement, aucun de ces systèmes n'est 100% sûr.
Plus nous interagissons en ligne et plus nous devenons les cibles de hackers sournois. Les spécialistes en sécurité appellent ce phénomène « la surface d'attaque ». Plus la surface est grande et plus l'attaque est facile à réaliser. Si vous jetez un coup d'œil à ces trois histoires qui ont eu lieu ces trois dernières années, vous comprendrez parfaitement le fonctionnement de cette attaque.

1. Comment détourner un compte : faut-il le pirater ou simplement passer un coup de fil ?

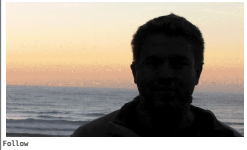
Un des outils les plus puissants utilisés par les hackers est le « piratage humain » ou l'ingénierie sociale. Le 26 février dernier, le rédacteur en chef de Fusion Kevin Roose, a voulu vérifier s'il était aussi puissant qu'il n'y paraissait. Jessica Clark, ingénieure sociale spécialisée en piratage informatique et l'expert en sécurité Dan Tentler ont tout deux accepté ce défi.
Jessica avait parié qu'elle pouvait pirater la boîte mail de Kévin rien qu'avec un email, et sans grande difficulté elle y est arrivé. Tout d'abord, l'équipe de Jessica a dressé un profil de 13 pages qui définissait quel genre d'homme il était, ses goûts, etc, provenant de données collectées de diverses sources publiques.
Après avoir préparé le terrain, Jessica a piraté le numéro mobile de Kévin et appelé sa compagnie de téléphone. Pour rendre la situation encore plus réelle, elle ajouta un fond sonore d'un bébé en train de pleurer.
Jessica se présenta comme étant la femme de Roose. L'excuse inventée par cette dernière fut qu'elle et son « mari » devaient faire un prêt, mais qu'elle avait oublié l'email qu'ils utilisaient en commun, en se faisant passer pour une mère de famille désespérée et fragile. Accompagnée des cris du bébé, Jessica ne mit pas longtemps à convaincre le service technique de réinitialiser le mot de passe du mail et ainsi d'y avoir pleinement accès.
Dan Tentler a accompli cette tâche avec l'aide de l'hameçonnage. Tout d'abord, il avait remarqué que Kevin possédait un blog sur Squarespace et lui envoya un faux email officiel depuis la plateforme, dans lequel les administrateurs de Squarespace demandaient aux utilisateurs de mettre à jour le certificat SSL (Secure Sockets Layer) pour des questions de « sécurité », permettant ainsi à Tentler d'accéder à l'ordinateur de Kévin. Dan créa de nombreux faux pop-up demandant à Roose des informations bien spécifiques et le tour était joué.
Tentler réussit à obtenir l'accès à ses données bancaires, son email, ses identifiants sur les sites web, ainsi que ses données de cartes de crédit, son numéro de sécurité sociale. De l'écran de son ordinateur, il capturait des photos toutes les deux minutes et ce pendant 48h.
View image on Twitter

Follow

Kaspersky Lab
@kaspersky
What is phishing and why should you care? Find outhttps://kas.pr/6bpe #iteducation #itsec
8:05 PM – 11 Dec 2015
•
•
1717 Retweets
•
77 likes

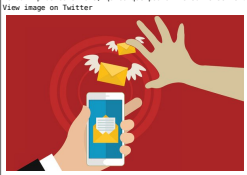
2. Comment détourner de l'argent à un ingénieur informatique en moins d'une nuit

Au printemps 2015, le développeur de logiciels Partap Davis a perdu 3000$. Durant une nuit, en seulement quelques heures, un hacker inconnu a obtenu l'accès de ses comptes mail, son numéro de téléphone et son Twitter. Le coupable a contourné habilement le système de l'authentification à deux facteurs et littéralement vidé le portefeuille des bitcoins de Partap. Comme vous devez sans doute l'imaginer, Davis a passé une mauvaise journée le lendemain.
Il est important de noter que Partap est une pointure concernant l'usage d'Internet : il choisit toujours des mots de passe fiables et ne clique jamais sur des liens malveillants. Son email est protégé avec le système d'authentification à deux facteurs de Google, ce qui veut dire que lorsqu'il se connecte depuis un nouvel ordinateur, il doit taper les six numéros envoyés sur son mobile.



Follow

The Verge
@verge
Anatomy of a hack: a step-by-step account of an overnight digital heist http://www.theverge.com/a/anatomy-of-a-hack …
4:02 PM – 4 Mar 2015
•
•
6969 Retweets
•
7171 likes
Davis gardait ses économies sur trois portefeuilles Bitcoin, protégés par un autre service d'authentification à deux facteurs, conçu par l'application mobile Authy. Même si Davis utilisait toutes ces mesures de sécurité prévoyantes, ça ne l'a pas empêché de se faire pirater.
Suite à cet incident, Davis était très en colère et a passé plusieurs semaines à la recherche du coupable. Il a également contacté et mobilisé des journalistes de The Verge pour l'enquête. Tous ensemble, ils sont parvenus à trouver comment le piratage avait été exécuté. Davis utilisait comme mail principal l'adresse suivante : Patrap@mail. Tous les mails furent envoyés à une adresse Gmail plus difficile à mémoriser (étant donné que Patrap@gmail était déjà utilisé).
Pendant plusieurs mois, quiconque pouvait ensuite se rendre sur la page Hackforum et acheter un script spécial afin d'obtenir les mots de passe qui se trouvaient dans la boite mail. Apparemment, le script était utilisé pour contourner l'authentification à deux facteurs et changer le mot de passe de Davis.
View image on Twitter



Follow

Kaspersky Lab
@kaspersky
Unfortunately two-factor authentication can't save you from#banking Trojans https://kas.pr/S4jV #mobile
4:40 PM – 11 Mar 2016
•
•
2828 Retweets
•
1515 likes
Ensuite, l'hacker a fait une demande de nouveau mot de passe depuis le compte de Davis et demandé au service client de transférer les appels entrants à un numéro de Long Beach (ville en Californie). Une fois le mail de confirmation reçu, le service technique a donné le contrôle des appels à l'hacker. Avec une telle technique, il n'était pas bien difficile de contourner l'authentification à deux facteurs de Google et avoir accès au compte Gmail de Davis.
Pour surmonter cet obstacle, l'hacker a tout simplement réinitialisé l'application sur son téléphone en utilisant une adresse mail.com et une nouvelle confirmation de code, envoyée de nouveau via un appel vocal. Une fois que l'hacker mit la main sur toutes les mesures de sécurité, il changea les mots de passe des portefeuilles Bitcoin de Davis, en utilisant Authy et l'adresse email .com afin de lui détourner de l'argent.
L'argent des deux autres comptes est resté intact, l'un des services interdisant le retrait des fonds 48h après le changement du mot de passe, et l'autre demandant une copie du permis de conduire de Davis, que l'hacker n'avait pas en sa possession.

3. La menace rôde sur nos vies

Comme l'a écrit le journal Fusion en octobre 2015, la vie de la famille Straters s'est retrouvée anéantie à cause d'une pizza. Il y a plusieurs années, des cafés et restaurants locaux se sont installés sur leur arrière-cour, les envahissant de pizzas, tartes et toute sorte de nourriture.
Peu de temps après, des camions de remorquage ont déboulé munis de grandes quantités de sable et de gravier, tout un chantier s'était installé sans aucune autorisation au préalable. Malheureusement, il ne s'agissait que de la partie visible de l'iceberg comparé au cauchemar des trois années suivantes.
Follow

Techmeme @Techmeme
How the Strater family endured 3 years of online harassment, hacked accounts, and swatting http://fusion.net/story/212802/haunted-by-hackers-a-suburban-familys-digital-ghost-story/ …http://www.techmeme.com/151025/p4##a151025p4 …
6:36 PM – 25 Oct 2015

Haunted by hackers: A suburban family's digital ghost story
A suburban Illinois family has had their lives ruined by hackers.
fusion.net
•
•
88 Retweets
•
66 likes
Paul Strater, ingénieur du son pour une chaine de télé locale et sa femme, Amy Strater, ancienne directrice générale d'un hôpital, ont été tout deux victimes d'un hacker inconnu ou de tout un groupe. Il s'avérait que leur fils Blair était en contact avec un groupe de cybercriminels. Les autorités ont reçu des menaces de bombe signées du nom du couple. Les hackers ont utilisé le compte d'Amy pour publier une attaque planifiée dans une école primaire, dans lequel figurait ce commentaire « Je tirerai sur votre école ». La police faisait des visites régulières à leur domicile, n'améliorant en rien les relations du couple avec leur voisinage, qui à force se demandait ce qu'il se passait.
Les hackers ont même réussi à pirater le compte officiel de Tesla Motors et posté un message qui encourageait les fans de la page à appeler les Strater, en échange de gagner une voiture Tesla. Les Strater « croulaient sous les appels téléphoniques », environ cinq par minute, provenant des « admirateurs » de Tesla, désireux de gagner la voiture. Un jour, un homme s'est même présenté au domicile des Strater en demandant aux propriétaires d'ouvrir leur garage, prétendant qu'ils cachaient la Tesla à l'intérieur.
Follow

r00t @rootworx
Again, There is no free car, I did not hack Elon Musk or Tesla's Twitter account. A Finnish child is having fun at your (and my) expense.
12:51 AM – 26 Apr 2015
•
•
1414 Retweets
•
1818 likes
Paul tenta de démanteler le groupe d'hackers en changeant tous les mots de passe de ses comptes et en donnant l'ordre aux patrons des restaurants locaux de ne rien dévoiler sur leur adresse. Il contacta également le Département de Police d'Oswego en leur demandant de vérifier à l'avance si une urgence était bien réelle, avant d'envoyer des renforts. En conséquence de tous ces problèmes, Paul et Amy finirent par divorcer.
Les attaques ont continué par la suite. Les réseaux sociaux d'Amy ont été piratés et utilisés pour publier toute une série de revendications racistes, ce qui a causé la perte de son emploi. Elle fut licenciée malgré avoir dit à ses supérieurs qu'elle et sa famille étaient les victimes de hackers et que leur vie s'était transformée en un véritable cauchemar.
Amy réussit à temps à reprendre le contrôle de son LinkedIn et à supprimer son compte Twitter. Malheureusement, elle était incapable de retrouver un travail dans sa branche à cause de ce qui s'était passé. Elle fut contrainte de travailler chez Uber pour arrondir ses fins de mois, mais disposait de ressources insuffisantes pour payer son loyer.
« Avant, lorsqu'on tapait son nom sur Google, on pouvait voir ses nombreux articles scientifiques et son travail admirable » a déclaré son fils Blair au journal Fusion. « Désormais, on ne voit plus que des hackers, hackers, hackers ».
De nombreuses personnes ont critiqué Blair Strater pour avoir été impliqué lui-même dans de nombreux réseaux de cybercriminels, où il n'arrivait pas à se faire d'amis. Dans le cas précis de la famille Strater, les parents de Blair ont payé pour les « crimes » de leur fils, alors qu'eux n'avaient absolument rien à voir avec les hackers.
Article original de Kate Kochetkova

Denis JACOPINI ne peut que vous recommander d'être prudent.
Si vous désirez être sensibilisé aux risques d'arnaques et de piratages afin d'en être protégés, n'hésitez pas à nous contacter, nous pouvons animer conférences, formations auprès des équipes dirigeantes et opérationnelles.
La sécurité informatique et la sécurité de vos données est plus devenu une affaire de Qualité (QSE) plutôt qu'un problème traité par des informaticiens.
Vous souhaitez être aidé ? Contactez-nous

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Original de l’article mis en page : Comment pirater, détourner de l’argent et rendre la vie de quelqu’un impossible sur Internet : trois histoires inquiétantes de piratages ciblés. | Nous utilisons les mots pour sauver le monde | Le blog officiel de Kaspersky Lab en français.

Obligation de résultat de la part d’un éditeur de logiciels. Autre cas d’école

Obligation de résultat de la part d’un éditeur de logiciels. Autre cas d’école

---

Le tribunal de commerce de Nanterre a condamné le groupe d'assurance mutualiste à verser plus de 1,4 million d'euros à l'éditeur et intégrateur d'un progiciel métier.
La Mutuelle assurance des commerçants et industriels de France et des cadres et salariés de l'industrie et du commerce (Macif) n'a pas obtenu gain de cause. Dans un jugement du 24 juin 2016 repéré par Legalis, le tribunal de commerce de Nanterre (Hauts-de-Seine) l'a condamnée pour résiliation abusive d'un contrat d'intégration et du contrat de licence et de maintenance associé.

Contrat d'intégration mal ficelé
En 2012, la Macif a lancé un appel d'offres pour doter sa filiale Macifilia d'une nouvelle solution de gestion d'assurance IARD (incendie, accidents et risques divers). L'éditeur et intégrateur IGA Assurance l'a remporté. C'est au terme d'un contrat de cadrage destiné à préciser le périmètre fonctionnel de son progiciel (ERP) Veos, que les parties ont conclu, le 8 février 2013, un contrat d'intégration d'un montant forfaitaire supérieur à 4 millions d'euros hors taxes.
Parallèlement, un contrat de licence et de maintenance a été signé. Mais à la suite d'échanges multiples, de retards et de modifications de planning, la Macif met en demeure, le 23 juillet 2013, IGA de livrer toutes les spécifications fonctionnelles détaillées (SFD) de la V1 (sur quatre prévues) sous 30 jours. IGA indique, le mois suivant, que 62 SFD sur 75 ont été livrées… Considérant qu'IGA n'a pas respecté le délai imparti et que la moitié des besoins exprimés ont été couverts, la Macif prononce en septembre 2013 la résiliation du contrat pour faute grave et répétée d'IGA. Le prestataire a contesté.
À la demande de la Macif, le tribunal de commerce a donc nommé un expert judiciaire pour clarifier le cadre contractuel sur lequel s'oppose l'assureur et son prestataire. Dans son rapport, l'expert a notamment indiqué que « la Macif était contractuellement responsable de la validation de l'exhaustivité des SFD, mais que IGA aurait dû vérifier l'exhaustivité ou la suivre et la gérer avec la Macif ».

Adapter ses processus à l'outil
C'est dans ces circonstances que la Macif a assigné son prestataire, en juin 2015, pour tenter d'obtenir la résolution judiciaire des contrats du 8 février 2013 aux torts d'IGA Assurance. Mais le tribunal ne l'a pas suivie, bien au contraire. Selon lui, « en faisant le choix de la solution progicielle Veos à l'issue d'une phase préalable d'analyse comparative, la Macif a nécessairement entendu adapter majoritairement ses modes de fonctionnement et ses processus au nouvel outil et non l'inverse ».
Dans ce contexte, l'obligation de résultat se limitait aux développements et aux adaptations à apporter à la version standard du progiciel. Le contrat n'imposant pas au prestataire de livrer des spécifications détaillées pour l'ensemble des besoins exprimés par la Macif. Le tribunal de commerce a donc prononcé la résolution des contrats du 8 février 2013 aux torts de la Macif et l'a condamnée.
Le groupe d'assurance mutualiste devra verser 1,14 million d'euros de dommages et intérêts à l'éditeur et intégrateur du progiciel : la SARL IGA Assurance. Et lui régler 276 120 euros pour une facture impayée de septembre 2013, plus 226 190 euros au titre des frais de justice.
Article original de Ariane Beky

Réagissez à cet article

Original de l’article mis en page : La Macif condamnée pour rupture abusive de contrat d’intégration

---

Directive européenne sur la sécurité des réseaux et des systèmes d’information

	Directive européenne sur la sécurité des réseaux et des systèmes d’information

---

Les entreprises qui fournissent des services essentiels, par exemple l'énergie, les transports, les services bancaires et de santé, ou numériques, tels que les moteurs de recherche et les services d'informatique en nuage, devront améliorer leur capacité à résister à des cyber-attaques, selon les premières règles de cybersécurité à l'échelle européenne, approuvées par les députés mercredi.

L'établissement de normes de cybersécurité communes et renforcer la coopération entre les pays de l'Union aidera les entreprises à se protéger elles-mêmes, et aussi à prévenir les attaques contre les infrastructures interconnectées des pays européens, estiment les députés.

« Des incidents de cybersécurité possède très souvent un aspect transfrontalier et concernent donc plus d'un État membre de l'Union européenne. Une protection fragmentaire de la cybersécurité nous rend tous vulnérables et pose un risque de sécurité important pour l'Europe dans son ensemble. Cette directive établira un niveau commun de sécurité de réseau et d'information et renforcera la coopération entre les États membres. Cela contribuera à prévenir à l'avenir les cyberattaques sur les infrastructures interconnectées européennes importantes », a déclaré le rapporteur du Parlement Andreas Schwab (PPE, DE).

La directive européenne sur la sécurité des réseaux et des systèmes d'information « est également l'un des premiers cadres législatifs qui s'applique aux plates-formes. En phase avec la stratégie du marché unique numérique, elle établit des exigences harmonisées pour les plates-formes et veille à ce qu'elles puissent observer des règles similaires quel que soit l'endroit de l'Union européenne où elles opèrent. C'est un énorme succès et une première étape importante vers l'établissement d'un cadre réglementaire global pour les plates-formes dans l'Union », a-t-il ajouté.

Les pays de l'UE devront lister les entreprises de « services essentiels »
La nouvelle législation européenne prévoit des obligations en matière de sécurité et de suivi pour les « opérateurs de services essentiels » dans des secteurs tels que ceux de l'énergie, des transports, de la santé, des services bancaires et d'approvisionnement en eau potable. Les États membres de l'UE devront identifier les entités dans ces domaines en utilisant des critères spécifiques, par exemple si le service est essentiel pour la société et l'économie, et si un incident aurait des effets perturbateurs considérables sur la prestation de ce service.

Certains fournisseurs de services numériques – les marchés en ligne, les moteurs de recherche et les services d'informatique en nuage – devront aussi prendre des mesures pour assurer la sécurité de leur infrastructure et devront signaler les incidents majeurs aux autorités nationales. Les exigences de sécurité et de notification sont, cependant, plus légères pour ces fournisseurs. Les micro- et petites entreprises numériques seront exemptées de ces exigences.

Mécanismes de coopération à l'échelle européenne
Les nouvelles règles prévoient un « groupe de coopération » stratégique pour échanger l'information et aider les États membres à renforcer leurs capacités en matière de cybersécurité. Chaque pays de l'Union devra adopter une stratégie nationale relative à sécurité des réseaux et des systèmes d'information.

Les États membres devront aussi mettre en place un centre de réponse aux incidents de sécurité informatique (CSIRT) pour gérer incidents et risques, discuter des questions de sécurité transfrontalière et identifier des réponses coordonnées. L'Agence européenne pour la sécurité des réseaux et de l'information (ENISA) jouera un rôle clé dans la mise en œuvre de la directive, en particulier en matière de coopération. La nécessité de respecter les règles de protection des données est réitérée tout au long de la directive.

Prochaines étapes
La directive sur la sécurité des réseaux et des systèmes d'information sera bientôt publiée au Journal officiel de l'Union européenne et entrera en vigueur le vingtième jour suivant sa publication. Les États membres auront alors 21 mois pour transposer la directive dans leur législation nationale et six mois supplémentaires pour identifier les opérateurs de services essentiels.

Directive sur la sécurité des réseaux et des systèmes d'information – texte approuvé par le Parlement et le Conseil
http://data.consilium.europa.eu/doc/document/ST-5581-2016-REV-1/fr/pdf
Procédure: codécision, seconde lecture
Source : Parlement européen

Réagissez à cet article

Original de l’article mis en page : Cybersécurité: les députés soutiennent les règles pour aider les entreprises de services clés à… – Linkis.com

---

Quel cadre pour l’État d’urgence et la copie des données informatiques ?

Quel cadre pour l’État d’urgence et la copie des données informatiques ?

Le gouvernement a entendu le Conseil constitutionnel, et fixé cette fois-ci un cadre très précis à la copie et l'utilisation des données informatiques saisies lors des perquisitions administratives réalisées dans le cadre de l'état d'urgence.

Ce mardi matin, nous expliquions que pour faire revenir la possibilité de saisir des données informatiques lors de perquisitions administratives organisées dans le cadre l'état d'urgence, le gouvernement aurait l'obligation de se conformer aux demandes d'encadrement fixées par le Conseil constitutionnel dans sa décision du 19 février 2016. Celui-ci avait en effet censuré le dispositif prévu à l'origine en novembre 2015, qui autorisait de copier les données accessibles sur place, sans aucun encadrement, ni sur la forme, ni sur le fond.

Nous avions ainsi résumé les préconisations des sages du Palais Royal :
« N'autoriser la copie que si une infraction est constatée lors de la perquisition administrative ;
• Limiter la copie aux données en lien avec l'infraction constatée ;
• Prévoir un cadre strict de conservation et d'exploitation des données saisies ;
• Faire entrer le juge dans la boucle. »

Jean-Jacques Urvoas, ministre de la Justice, au Sénat

Or il faut reconnaître au gouvernement, sans doute influencé en ce sens par le ministre de la justice Jean-Jacques Urvoas, d'avoir su prendre parfaitement acte des demandes du Conseil constitutionnel. Tel que présenté en conseil des ministres et tel qu'il devrait être adopté par le Parlement, le projet de loi prorogeant l'état d'urgence fixe un cadre très précis, même s'il ne va pas aussi loin dans le filtrage que ce qu'ont souhaité les membres du Conseil.

PAS D'ACCÈS AU CLOUD, CONSULTATION OBLIGATOIRE D'UN JUGE…

Nous avons mis en gras les éléments les plus importants du projet de loi, qui concernent notamment l'obligation de motiver la copie des données et de ne les consulter qu'après l'aval d'un juge administratif qui aura 48 heures pour se prononcer. On notera au passage que la copie est désormais limitée aux seules « données contenues dans tout système informatique présent sur les lieux de la perquisition », ce qui doit exclure en principe l'accès aux données stockées dans le Cloud – auparavant celle-ci était prévue par une référence aux « données accessibles à partir du système initial ou disponibles pour le système initial », qui a disparu.

« Si la perquisition révèle l'existence d'éléments, notamment informatiques, relatifs à la menace que constitue pour la sécurité et l'ordre publics le comportement de la personne concernée, les **données contenues dans tout système informatique ou équipement terminal présent sur les lieux** de la perquisition peuvent être saisies, soit par leur copie, soit par la saisie de leur support lorsque la copie ne peut être réalisée ou achevée pendant le temps de la perquisition.
La copie des données ou la saisie des systèmes informatiques ou des équipements terminaux est réalisée en présence de l'officier de police judiciaire. L'agent sous la responsabilité duquel est conduite la perquisition rédige un procès-verbal de saisie qui **en indique les motifs** et dresse l'inventaire des matériels saisis. Une copie de ce procès-verbal est remise aux personnes mentionnées au deuxième alinéa du présent I. Les données et les supports saisis sont conservés sous la responsabilité du chef du service ayant procédé à la perquisition. **À compter de la saisie, nul n'y a accès avant l'autorisation du juge.**
L'autorité administrative **demande au juge des référés du tribunal administratif d'autoriser en tant sa partie leur exploitation.** Au vu des éléments révélés par la perquisition et, s'il l'estime utile, des données et matériels saisis, il **statue dans un délai de quarante-huit heures** à compter de sa saisine sur la régularité de la saisie et la demande de l'autorité administrative. **Sont exclus de l'autorisation les éléments découverts de tout lien avec la menace** que constitue le comportement de la personne concernée pour la sécurité et l'ordre publics. **En cas de refus** du juge des référés, et sous réserve de l'appel mentionné au dixième alinéa, **les données copiées sont détruites** et les supports saisis sont restitués à leur propriétaire.
Pendant le temps strictement nécessaire à leur exploitation autorisée par le juge des référés, les données et les supports saisis sont conservés sous la responsabilité du chef du service ayant procédé à la perquisition et à la saisie. Les systèmes informatiques ou équipements terminaux sont **restitués à leur propriétaire**, le cas échéant après qu'il a été procédé à la copie des données qu'ils contiennent, **à l'issue d'un délai maximal de quinze jours** à compter de la date de leur saisie ou de celle à laquelle le juge des référés, saisi dans ce délai, a autorisé l'exploitation des données qu'ils contiennent. **À l'exception de celles qui caractérisent la menace que constitue pour la sécurité et l'ordre publics le comportement de la personne concernée, les données copiées sont détruites à l'expiration d'un délai maximal de trois mois** à compter de la date de la perquisition ou de celle à laquelle le juge des référés, saisi dans ce délai, en a autorisé l'exploitation.
En cas de difficulté dans l'accès aux données contenues dans les supports saisis ou dans l'exploitation des données copiées, lorsque cela est nécessaire, les délais prévus à l'alinéa précédent peuvent être prorogés, pour la même durée, par le juge des référés saisi par l'autorité administrative au moins quarante-huit heures avant l'expiration de ces délais. Le juge des référés statue dans un délai de quarante-huit heures sur la demande de prorogation présentée par l'autorité administrative. **Si l'exploitation ou l'examen des données et des supports saisis conduisent à la constatation d'une infraction, ils sont conservés selon les règles applicables** en matière de procédure pénale.
Pour l'application des dispositions du présent article, le juge des référés est celui dans le ressort duquel se trouve le lieu de la perquisition. Il statue dans les formes prévues au livre V du code de justice administrative, sous réserve des dispositions du présent article. **Ses décisions sont susceptibles d'appel** devant le juge des référés du Conseil d'État dans un délai de 48 heures à compter de leur notification. Le juge des référés du Conseil d'État statue dans le délai de 48 heures. En cas d'appel, les données et les supports saisis demeurent conservés dans les conditions mentionnées au huitième alinéa du présent article. »
Dans ces conditions, il paraît vraisemblable qu'en cas de contestation, le Conseil constitutionnel ne trouvera rien à redire à la copie des données réalisées par les policiers.
Article original de Guillaume Champeau

Original de l'article mis en page : État d'urgence et copie des données informatiques : le cadre prévu par le gouvernement – Politique – Numerama

---

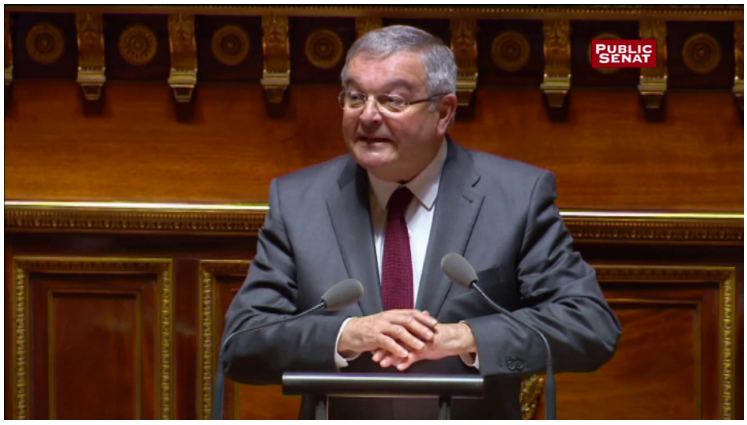
Quelles sont les limites d'accès aux données de connexion en situation d'État d'urgence ?

Quelles sont les limites d'accès aux données de connexion en situation d'État d'urgence ?

Mercredi, le Sénat examinera le projet de loi de prorogation de l'état d'urgence, et discutera à cette occasion d'un amendement qui vise à donner à la police le pouvoir d'obtenir en temps réel les données de connexion de tout suspect de terrorisme, sans aucun contrôle même administratif.

Au nom du comité de suivi de l'état d'urgence dont il est le rapporteur spécial, le sénateur Michel Mercier (UDI-UC) a présenté mardi la substance des amendements qu'il entend présenter devant la commission des lois ce mercredi, pour compléter le projet de loi de prorogation de l'état d'urgence déposé par le gouvernement. Ces amendements ont de fortes chances d'être adoptés par la majorité de droite du Sénat.

Parmi eux, M. Mercier explique qu'un « *amendement aura pour objet de remédier aux rigidités et lourdeurs dans la mise en œuvre de la technique de recueil de renseignements, créée par la loi du 24 juillet 2015, permettant de recueillir en temps réel, sur les réseaux des opérateurs de communications électroniques, les données de connexion relatives à une personne préalablement identifiée comme présentant une menace terroriste* ».



Il s'agit de la procédure créée par la loi Renseignement et codifiée à l'article L851-2 du code de la sécurité intérieure, qui permet « *pour les seuls besoins de la prévention du terrorisme* » d'autoriser « *le recueil en temps réel* » des « *informations ou documents* » détenus par les opérateurs télécoms et les hébergeurs « *relatifs à une personne préalablement identifiée comme présentant une menace* ».

C'EST CE CADRE POURTANT DÉJÀ CRITIQUÉ PAR LES DÉFENSEURS DES DROITS FONDAMENTAUX QUE MICHEL MERCIER ESTIME CONSTITUER DES « RIGIDITÉS ET LOURDEURS »

Même s'il y a débat juridique pour savoir jusqu'où vont ces « informations ou documents », et s'ils vont jusqu'au contenu-même des communications (en principe non), il s'agit au minimum de l'ensemble des données de connexion : adresses IP, numéros de téléphones composés, durées et heures des appels, géolocalisation du téléphone mobile, nombre de SMS échangés, avec qui, de quelle longueur, etc. Potentiellement ce sont donc des données très intrusives dans la vie privée des individus, qui permettent de renseigner sur les habitudes, les déplacements et les contacts.

Actuellement, pour avoir accès en temps réel à ces données, les services de renseignement doivent obligatoirement ***obtenir au préalable une autorisation du Premier ministre****, elle-même délivrée après avis de la Commission nationale de contrôle des techniques de renseignement (CNCTR). L'avis de la CNCTR doit intervenir dans les 24 heures ou pour les cas les plus complexes, dans les 72 heures. Mais en cas « d'urgence absolue », il est même* ***possible de se passer de l'avis de la CNCTR****.*

Or c'est ce cadre pourtant déjà critiqué par les défenseurs des droits fondamentaux (en raison de l'absence de contrôle d'un juge indépendant) que Michel Mercier estime constituer des « rigidités et lourdeurs » qu'il faudrait supprimer en cas d'état d'urgence.

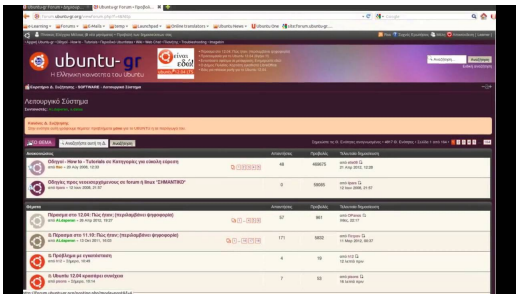
Article original de Guillaume Champeau

Réagissez à cet article

Original de l’article mis en page : État d’urgence : open bar pour la police sur les données de connexion ? – Politique – Numerama

---

Deux millions de données d’utilisateurs Ubuntu dérobées



Deux millions de données d’utilisateurs Ubuntu dérobées

Le forum de la distribution Ubuntu a été victime d'une grave attaque informatique. Deux millions d'utilisateurs se sont fait voler leurs données.

Le butin du pirate est plus qu'impressionnant. Noms, mots de passe, adresse mails et IP, les données de deux millions d'utilisateurs du forum d'Ubuntu se sont envolées. La nouvelle a été annoncée jeudi dans un communiqué par Canonical l'éditeur d'Ubuntu. *« A 20h33 UTC le 14 Juillet 2016, Canonical et l'équipe ont été informés par un membre du Conseil Ubuntu que quelqu'un prétendait avoir une copie de la base de données des forums. Après enquête initiale, nous avons été en mesure de confirmer qu'il y avait bien eu une exposition des données et nous avons fermé les forums par mesure de précaution. »*

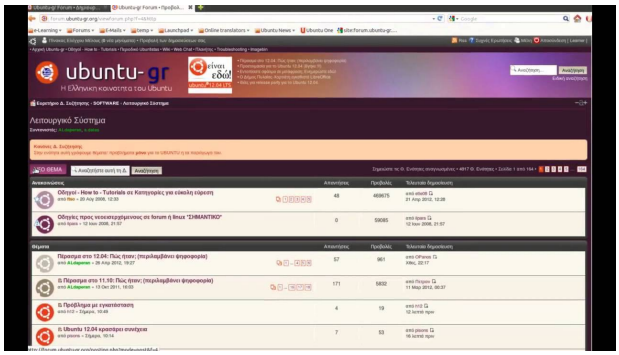
Une attaque par injection SQL

Une enquête plus poussée a révélé que la méthode employée est une injection SQL. Le pirate a pu injecter des requêtes SQL formatées dans la base de données des forums pour ensuite télécharger les datas.

Cependant, le communiqué précise que le hacker n'a pas pu accéder aux mots de passe utilisateur valides ni au référentiel de code Ubuntu ou au mécanisme de mise à jour. Moins certain, le rapport précise que normalement les services Canonical ou Ubuntu en sortent indemnes, comme certains forums.

Tout est plus ou moins rentré dans l'ordre

Des mesures correctives ont été prises et les forums restaurés. Les mots de passe du système et de la base de données ont été réinitialisés et ModSecurity, une Web Application Firewall vient renforcer le dispositif de sécurité. Selon Canonical, ça va mieux, même si après ce genre de vol il est légitime de penser que le mal est fait.



Article original de Victor Miget

Réagissez à cet article

Original de l'article mis en page : Ubuntu : les données de

deux millions d’utilisateurs dérobées