Le « friend finder » de Facebook devient illégal en Allemagne

Le « friend finder » de Facebook devient illégal en Allemagne

La plus haute cour de justice allemande a déclaré illégal l'outil de recherche d'amis « friend finder » du réseau social américain Facebook.

Le comité de la Cour fédérale d'Allemagne a jugé que la fonction de recherche d'amis de Facebook viole la loi sur la publicité, a rapporté le journal britannique The Guardian.

© FLICKR/ MOMPL

Facebook: cachez-moi cette sirène que je ne saurais voir!

En accédant au carnet d'adresses de l'utilisateur, le « friend finder » récolte tous les contacts et leur envoie des invitations leur proposant de s'inscrire sur le réseau social. C'est ce mécanisme de collecte d'adresses électroniques et son utilisation dans un but marketing qui a été condamné.

La cour a conclu que cette pratique de marketing était trompeuse, confirmant les décisions de deux tribunaux de Berlin de 2012 et 2014, qui avaient constaté que Facebook violait les lois allemandes sur la protection des données et sur les pratiques commerciales déloyales.

La Cour fédérale a également déclaré que Facebook n'avait pas informé d'une façon adéquate les membres du réseau sur le mécanisme qui utilise les données de leurs contacts.

© AP PHOTO/ DAPD, JOERG KOCH

Facebook dévoile les sujets de discussion les plus populaires en 2015

Le représentant officiel de Facebook en Allemagne a, à son tour, déclaré que la société attendait le rapport explicatif de la décision finale et qu'elle l'étudierait les solutions « pour évaluer tout impact sur les services ».

C'est une vraie victoire pour l'association de protection des consommateurs allemands VZBV (Verbraucherzentrale Bundesverband) qui menait ce combat depuis 2010. En outre, elle ne compte pas arrêter sa lutte contre les géant d'Internet et souhaite maintenant vérifier les mécanismes de LinkedIn et Twitter.

« En plus de Facebook, d'autres services utilisent cette forme de publicité pour attirer de nouveaux utilisateurs. Ils doivent maintenant probablement repenser leurs systèmes », a déclaré Klaus Mueller, président de VZBV.

Réagissez à cet article

Source : *Le « friend finder » de Facebook devient illégal en Allemagne*

Loi Numérique : les amendes de la CNIL restent plafonnées à 150 000 euros

	Loi Numérique : les amendes de la CNIL restent plafonnées à 150 000 euros

Les députés de la commission des lois ont renforcé cette semaine les attributions de la Commission nationale de l'informatique et des libertés (CNIL), mais n'ont pas augmenté le montant des amendes pouvant être infligées par l'institution.

Le pouvoir de réprimande de la CNIL, qui peut actuellement prononcer des sanctions pécuniaires de 150 000 euros maximum en cas de premier manquement, c'est « cacahuète », dixit Axelle Lemaire ! Pour autant, l'intéressée s'est opposée dans le cadre de l'examen du projet de loi numérique à revoir ce niveau de sanctions… La secrétaire d'État au Numérique a en effet émis un avis défavorable sur les amendements visant à relever ce plafond (de 20 millions à 100 millions d'euros, selon les propositions des parlementaires).
En cause ? L'adoption imminente du règlement européen sur les données personnelles, sur lequel les institutions européennes sont parvenues à un accord fin 2015. « *La logique qui est poursuivie par le gouvernement jusqu'à présent, c'est de n'anticiper cette entrée en vigueur du texte européen que lorsqu'une marge de manœuvre est laissée à l'État membre. Ce n'est pas le cas en l'occurrence, même si je comprends tout à fait l'objectif posé par ces amendements* », s'est justifiée Axelle Lemaire. Le problème est surtout que le règlement n'a pas encore été officiellement traduit en français, ce qui ne permet pas de graver dès aujourd'hui dans le marbre des dispositions dont le législateur ne peut être certain qu'elles seront conformes au règlement européen…

« Marquer le coup maintenant face à des gens qui se gavent toujours plus chaque mois »

Pour certains députés, à l'instar de Philippe Gosselin (Les Républicains) et Isabelle Attard (Écologiste), la France aurait pourtant intérêt à anticiper l'entrée en vigueur du règlement – qui sera d'application directe mais sous deux ans à compter de l'adoption définitive du texte. « *Je pense que c'est important de marquer le coup maintenant face à des gens qui se gavent toujours plus chaque mois* » a ainsi plaidé l'élue du Calvados, reprenant une demande de la CNIL elle-même.

Crédits : Assemblée nationale

Invités par la secrétaire d'État au Numérique à retirer leurs amendements, les députés Gosselin, Attard et Martin-Lalande n'ont pas plié, Axelle Lemaire ne leur ayant donné que trop peu de gages. « *Je peux prendre l'engagement de tenter d'avancer sur ce sujet, sans vous assurer d'avoir une rédaction propre et définitive qui arrive dans quelques jours* [pour les débats en séance publique, ndlr]. *Je crois que les amendements que vous avez déposés ont le mérite de poser cette question. Si elle n'est pas suffisamment mûre à l'Assemblée nationale, elle aura peut-être mûri au Sénat, notamment parce que la traduction officielle sera disponible à ce moment-là* » a-t-elle déclaré, expliquant qu'un amendement gouvernemental sur ce sujet devrait être préparé en interministériel, notamment avec l'appui de la Chancellerie.
Tous leurs amendements ont cependant été rejetés (87, 265 et 454).

Vote de la saisine parlementaire de la CNIL, publicité de ses avis…

D'autres amendements concernant la CNIL ont en revanche été adoptés. L'autorité administrative pourra par exemple être consultée par le président de l'Assemblée nationale ou du Sénat sur une proposition de loi, sauf si le parlementaire à l'origine du texte s'y oppose. La gardienne des données personnelle est également autorisée à saisir l'ARCEP sur toute question relevant de sa compétence, et inversement.
Les amendements rendant obligatoire la publication des avis de la CNIL sur les projets de loi, alors que l'institution ne le fait aujourd'hui que sur demande du président de la commission des lois du Sénat ou de l'Assemblée nationale, ont d'autre part été votés. Il en ira de même pour les délibérations portant sur des décrets ou arrêtés pour lesquels la loi prévoit un avis de la gardienne des données personnelles.

Réagissez à cet article

Source : *Loi Numérique : les amendes de la CNIL restent plafonnées à 150 000 euros | Tech24*

La France aurait-elle peur de Intelligence artificielle ?

La France aurait-elle peur de Intelligence artificielle ?

L'intelligence artificielle caractérisée par l'autonomie croissante des machines, ça vous fait peur ? 65% d'un panel de Français répondent oui. Mais pour quelles raisons sont-ils inquiets ? Et aujourd'hui, l'IA, c'est quoi au juste ? Pas sûr qu'une majorité de Français puissent cette fois répondre.

	Plutôt d'accord	Plutôt pas d'accord
· L'intelligence artificielle est amenée à prendre un essor considérable avec le Big Data	69%	31%
· Le Big Data fera l'objet d'une utilisation très importante à long terme par les pouvoirs publics et les entreprises (profilage des individus, surveillance)	68%	32%
· Le Big Data présente des avantages à court terme pour la santé et le bien-être des individus (meilleure prévention des maladies et des risques, traitements plus adaptés, découvertes scientifiques, etc.)	67%	33%
· L'intelligence artificielle caractérisée par l'autonomie croissante des machines (comme les drones armés ou la voiture Google) vous inquiète	65%	35%

Non, ne paniquez pas, vous n'êtes pas pris dans une boucle spatiotemporelle et de retour en février 76, avec sur l'écran, face à vous, Roger Gicquel. Relativisons dès à présent. La France n'a pas peur de l'intelligence artificielle.
Mais une majorité de Français d'un panel de 10004 personnes se déclare plutôt d'accord lorsqu'on lui demande si l'intelligence artificielle « caractérisée par l'autonomie croissante des machines (comme les drones armés ou la voiture Google) » l'inquiète.

Des effets de génération dans les craintes

Et effectivement selon le sondage IFOP commandé par « L'Observatoire B2V des Mémoires », 65% se déclarent inquiets. Ce sentiment ne se diffuse cependant pas de façon uniforme d'un français à un autre.
Ainsi les 25-34 ans sont, en proportion, aussi inquiets (69%) que les 65 ans et plus (70%), bien plus en tout cas que les 18-245 ans (50%). De même, les résultats de l'étude font état de disparité géographique et en fonction du niveau de diplôme sur cette question.
« Il existe donc des effets de génération dans les craintes qui ne tiennent pas simplement à la jeunesse, à l'âge et au niveau d'éducation » commente dans un communiqué Jean-Gabriel Ganascia, professeur à l'Université Pierre et Marie Curie (Paris VI).
Les Français sondés sont donc en majorité inquiets, soit. Mais, et la question n'est pas pédante, combien de ces Français sont au fait des travaux autour de l'IA et de ses usages concrets ? Très certainement une très faible portion, car les notions et savoirs scientifiques associés à ce domaine de recherche s'avèrent d'une très grande complexité.
« Aujourd'hui beaucoup d'entreprises, dont Facebook, partagent cette même vision, à savoir que les problèmes que nous cherchons à résoudre sont infiniment complexes. Et même si nous employons les meilleurs talents, ce n'est pas suffisant pour résoudre ces problèmes comme celui de l'apprentissage non supervisé » expliquait ainsi Florent Perronnin, directeur du laboratoire de recherche parisien de Facebook dédié à l'intelligence artificielle.

« **La peur est dans la population parce qu'elle ne sait pas de quoi on parle** »

Mais celui qui résume le mieux le résultat de cette étude, c'est peut-être Michel Nachez dans une interview à Rue 89 :
« La séduction [à l'égard de l'IA] est du côté de ceux qui sont dans le milieu de l'informatique robotique, et chez les fans de science-fiction. La peur est dans la population parce qu'elle ne sait pas de quoi on parle. Elle est influencée par la littérature, le cinéma, les séries, où la machine finit par tourner mal, se retourne contre l'homme et le détruit. »
Cela ne signifie pas néanmoins que l'intelligence artificielle ne puisse pas être une source légitime d'inquiétude ou de questionnement, mais alors pour des risques bien différents de ceux qui pourraient être imaginés par certains, comme des machines douées de conscience se retournant contre leur créateur.
« Ceux d'entre nous en première ligne dans la fourniture de code sont très excités par l'intelligence artificielle, mais nous ne voyons pas de chemin réaliste permettant à notre logiciel d'acquérir une conscience » déclarait d'ailleurs à ce sujet Andrew Ng, un spécialiste renommé du machine learning (apprentissage automatique).

Et si le risque c'était l'homme et non l'IA ?

Plusieurs personnalités de l'univers des technologies, comme Bill Gates et Elon Musk, ont pourtant argué des dangers représentés par l'IA. Mais pour Jean-Gabriel Ganascia, interrogé par Le Monde, ces « allégations ne reposent sur rien […] Ce n'est même pas que je suis en désaccord sur le plan scientifique, c'est qu'il n'y a rien sur le plan scientifique. »
« Une machine peut être autonome au sens technique du terme : elle peut effectuer une chaîne d'actions (capter des informations, prendre une décision puis agir) sans que l'homme intervienne, à part en amont. Cela n'est pas dangereux en soi, car la machine est soumise au but que l'homme lui a donné » ajoutait-il.
Des dérives découlant de l'utilisation de ces technologies sont possibles. La FTC, le régulateur américain du commerce, souligne ainsi dans un rapport récent les risques potentiels d'exclusion engendrés par l'exploitation d'algorithmes (qui peuvent faire appel à de l'IA) appliqués au Big Data.
Mais la source de ces risques n'est pas alors l'IA elle-même, mais l'auteur ou l'exploitant des algorithmes, par exemple au travers d'un usage tourné essentiellement vers la maximisation du profit, et négligeant l'intérêt des consommateurs, la législation ou portant « atteinte à des valeurs fondamentales d'inclusion et d'équité. »
Et ces risques sont sans doute bien plus plausibles que l'émergence d'une intelligence artificielle malfaisante asservissant la race humaine. « Il pourrait y avoir, dans un futur lointain, une race de robots tueurs, mais je ne travaille pas aujourd'hui à éviter de rendre l'IA malveillante pour la même raison que je ne m'inquiète pas du problème de surpopulation sur la planète Mars » commentait Andrew Ng lors de la conférence GTC 2015.

Réagissez à cet article

Source : *Intelligence artificielle – La France a peur. Mais de quoi au juste ?*

Nissan victime d'une cyberattaque

Nissan victime d'une cyberattaque

Victime d'une cyber-attaque, le constructeur auto nippon a annoncé mercredi qu'il suspendait l'accès à tous ses sites internet. Les hackers d'Anonymous ont revendiqué l'action. Elle serait liée à la nouvelle campagne de chasse à la baleine par des navires japonais.

Anonymous contre Nissan, le tout sur fond de chasse à la baleine. Info ou intox ?

Les vérifications sont en cours mais la piste semble très sérieuse. Le constructeur auto nippon a annoncé mercredi qu'il suspendait l'accès à ses sites internet (www.nissan-global.com) « en raison d'une potentielle attaque par déni de service » (saturés par un nombre insurmontable de requêtes simultanées, les serveurs de la cible deviennent indisponibles, Ndlr) lancée la veille.

Un activiste se réclamant de la mouvance des Anonymous a posté sur son compte Twitter un message revendiquant l'action en faisant référence à la chasse aux baleines. « Nous sommes en train d'examiner la situation, nous ne savons pas pour l'heure si c'est vraiment lié à Anonymous », a précisé à l'AFP un porte-parole de Nissan.

Mercredi matin, Anonymous a levé le doute en confirmant l'attaque sur son compte Twitter. Mais pas encore le motif qui devrait faire l'objet d'un prochain post sur Tweeter.

Et ce n'est pas une première. Selon la chaîne japonaise NHK qui cite la police, Anonymous a déjà pris pour cible une centaine d'organisations dans l'archipel au cours du dernier trimestre 2015, l'accès au site officiel du bureau du Premier ministre Shinzo Abe a même été perturbé en décembre.

Une faille dans le moratoire

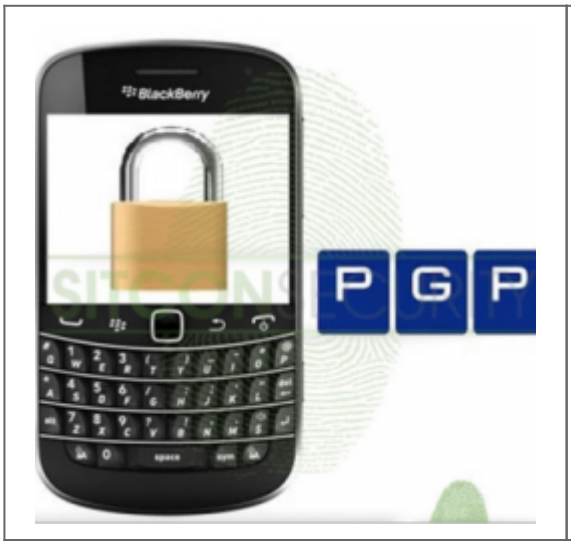
En dépit des admonestations répétées de l'ONU et de la Cour internationale de justice , les autorités nippones ont en effet repris la chasse à la baleine dans l'océan Antarctique en novembre dernier . Tokyo avait été contraint de renoncer à la saison 2014-2015 de prises de cétacés dans la zone australe après une décision en mars 2014 de la CIJ qui, saisie par l'Australie, avait jugé que le Japon détournait à des fins commerciales une activité présentée comme étant destinée à la recherche animale. A savoir : le programme de recherche scientifique baptisé «Jarpa», aux contours pour le moins flous.

Depuis, le pays a soumis un nouveau programme à la Commission baleinière internationale (CBI), lequel prévoit de capturer 3.996 petits rorquals (ou baleines de Minke) en Antarctique dans les douze prochaines années, soit 333 par saison contre environ 900 dans le cadre du précédent programme condamné.

Réagissez à cet article

Source : *Nissan victime collatérale de la cause des baleines – Industrie – Services*

Les Blackberry PGP déchiffrés par la Police hollandaise



Les Blackberry PGP déchiffrés par la Police hollandaise

Commercialisés par de nombreux vendeurs en ligne, les smartphones Blackberry embarquant en surcouche le standard de chiffrement de messagerie PGP seraient loin d'assurer un échange confidentiel des données. Tout du moins pour la Police hollandaise qui a confirmé être en mesure de les déchiffrer.

Les oreilles des défenseurs de la vie privée vont encore siffler. Des enquêteurs de la Police hollandaise ont en effet confirmé à Motherboard être en mesure d'accéder aux messages chiffrés envoyés depuis un terminal Blackberry sur lesquel le standard de chiffrement PGP est intégré en surcouche. « Nous sommes capables d'obtenir des données chiffrées depuis les terminaux Blackberry PGP », a fait savoir Tuscha Essed, responsable presse du Netherlands Forensic Institute (NFI), qui assiste la Police dans la recherche de preuves pour ses enquêtes en Hollande. L'information était parue initialement en décembre sur le blog misdaadnieuws.com où plusieurs documents sourcés NFI ont été publiés.

Le fait que les emails chiffrés puissent être lus et les messages effacés retrouvés, ne semble en tout cas pas perturber outre mesure les fournisseurs de Blackberry PGP. « Nous n'avons pas été affecté. Nos services sont complètement sécurisés et nous n'avons jamais été compromis », a indiqué un porte-parole de GhostPGP dans un mail à Motherboard. « Nous utilisons le dernier chiffrement PGP du moment qui est aussi impossible à déchiffrer. Nos clients sont très satisfaits du niveau de sécurité fourni », a quant à lui indiqué un représentant de TopPGP.com.

Réagissez à cet article

Source : *Les Blackberry PGP déchiffrés par la Police hollandaise – Le Monde Informatique*

Utiliser Internet à des fins personnelles peut être un motif de licenciement

Utiliser Internet à des fins personnelles peut être un motif de licenciement

La justice européenne confirme à nouveau que dans un cercle professionnel, la direction a un droit de regard sur les échanges électroniques des salariés. Les e-mails ou autres services de communication en ligne peuvent être surveillés.

La Cour européenne des droits de l'homme (CEDH) vient de débouter un plaignant dont le licenciement avait été motivé par une utilisation indue de ressources professionnelles. Ce dernier avait utilisé à des fins personnelles, et pendant les heures de travail, des outils professionnels mais également la connexion de l'entreprise, entre autres services en ligne.
Le plaignant, un ingénieur roumain en charge des ventes, utilisait en particulier Yahoo Messenger pour converser avec des clients mais surtout avec des connaissances personnelles. La décision de la Cour met ainsi en avant le fait que l'employé échangeait très régulièrement des messages « avec son frère et sa fiancée et portant sur des questions personnelles telles que sa santé et sa vie sexuelle ».
La société a mis fin au contrat de son collaborateur au motif que son règlement intérieur interdisait l'usage de ces mêmes ressources à des fins personnelles. Cet argument a été soutenu par la justice d'autant qu'elle ne qualifie pas d'abusif le fait qu'un employeur souhaite vérifier que ses employés accomplissent leurs tâches professionnelles pendant les heures de travail.

Stress travail e-mail email

La CEDH estime donc que la surveillance des communications du salarié était légitime dans la mesure où elle est considérée comme raisonnable. Cela signifie que l'employeur a cherché à préserver la productivité de ses salariés sans pour autant instaurer de politique rigide de surveillance des communications. La Cour précise que cette attention portée à l'encontre du collaborateur était organisée dans le cadre d'une procédure disciplinaire.
En France, le régime est très similaire. La justice valide régulièrement des licenciements lorsque des salariés utilisent trop souvent leurs outils informatiques pour des motifs personnels. Il est en général question de navigations régulières et conséquentes pour des tâches qui ne sont en rien en rapport avec le travail.

Réagissez à cet article

Source : *Utiliser Internet à des fins personnelles peut être un motif de licenciement*

Wikipédia bloque pour un an le ministère de l'Intérieur pour « foutage de gueule »

Ministère de l'Intérieur (France)

48° 52′ 19″ N 2° 19′ 01″ E carte

Pour les articles homonymes, voir Ministère de l'Intérieur.

Le **ministère de l'Intérieur**[2] est le département ministériel du gouvernement français chargé traditionnellement de la sécurité intérieure, de l'administration du territoire et des libertés publiques.

Depuis deux siècles, le ministère de l'Intérieur est au cœur de l'administration française : il assure sur tout le territoire le maintien et la cohésion des institutions du pays. Son organisation, ses moyens humains et matériels constituent l'outil privilégié de l'État pour garantir aux citoyens l'exercice des droits, devoirs et libertés réaffirmés par la Constitution de la Ve République.

Installé à l'hôtel de Beauvau, dans le 8e arrondissement de Paris, à quelques pas du palais de l'Élysée, il est surnommé, par métonymie, « la Place Beauvau ».

L'actuel ministre de l'Intérieur est Bernard Cazeneuve, depuis le 2 avril 2014.

Sommaire [masquer]

1 Historique

Ministère de l'Intérieur

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DE L'INTÉRIEUR

Wikipédia bloqué pour un an : le ministère de l'Intérieur pour « foutage de gueule »

Le ministère de l'Intérieur a visiblement eu la main un peu lourde quant au nombre de modifications apportées sur sa page Wikipédia, mais est également accusé de différents dérapages. Résultat : un an de blocage.

Ministère de l'Intérieur (France)

48° 52′ 19″ N 2° 19′ 01″ E carte

Pour les articles homonymes, voir Ministère de l'Intérieur.

Le **ministère de l'Intérieur**[2] est le département ministériel du gouvernement français chargé traditionnellement de la sécurité intérieure, de l'administration du territoire et des libertés publiques.

Depuis deux siècles, le ministère de l'Intérieur est au cœur de l'administration française : il assure sur tout le territoire le maintien et la cohésion des institutions du pays. Son organisation, ses moyens humains et matériels constituent l'outil privilégié de l'État pour garantir aux citoyens l'exercice des droits, devoirs et libertés réaffirmés par la Constitution de la Ve République.

Installé à l'hôtel de Beauvau, dans le 8e arrondissement de Paris, à quelques pas du palais de l'Élysée, il est surnommé, par métonymie, « la Place Beauvau ».

L'actuel ministre de l'Intérieur est Bernard Cazeneuve, depuis le 2 avril 2014.

Sommaire [masquer]

1 Historique

Ministère de l'Intérieur

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DE L'INTÉRIEUR

Création 1790

Une interdiction de contribuer délivrée pour cause de « foutage de gueule ». Cela prêterait à sourire si le blocage en question ne concernait pas le ministère de l'Intérieur. D'après le Canard enchaîné, l'encyclopédie en ligne a en effet bloqué l'adresse IP de la place Beauvau pour « attitude non collaborative », « passage en force » et « foutage de gueule ».

En plus de modifications trop nombreuses à son goût, Wikipédia accuse également les fonctionnaires de vandalisme répété. Le 21 août dernier, Wikipédia a remarqué un changement sur sa page de présentation, avec la sympathique mention « Sale batar » (avec la faute). La modification émanait de l'adresse IP du ministère.

Début décembre, l'encyclopédie en ligne avait adressé un « dernier avertissement » à l'encontre du compte du ministère : visiblement, cela n'a pas suffi.

Wikipedia Beauvau

Après un premier blocage temporaire en 2013 (la fiche du préfet de police de l'époque, Bernard Boucault, avait subi six modifications en 30 minutes afin d'effacer la trace de ses démêlés avec les opposants au mariage pour tous), le compte du ministère de l'Intérieur se retrouve désormais bloqué pour un an. Difficile de comprendre comment, au sein d'un ministère, de tels agissements peuvent se répéter.

Toujours est-il qu'il y a fort à parier que ce dernier trouvera tout de même les moyens de contrôler ce qui se passe sur sa page de référence.

Réagissez à cet article

Source : *Wikipédia bloque pour un an le ministère de l'Intérieur pour « foutage de gueule »*

Amnesty critique la nouvelle loi sur la cybercriminalité au Koweït

Amnesty critique la nouvelle loi sur la cybercriminalité au Koweït

---

Amnesty International a vivement critiqué mardi une nouvelle loi sur la cybercriminalité au Koweït qui, selon cette organisation, va restreindre davantage la liberté d'expression et doit être révisée.

Le texte, qui entre en vigueur mardi, « va s'ajouter à l'éventail de lois sur le web qui restreignent déjà le droit des Koweïtiens à la liberté d'expression et doit être révisé d'urgence », écrit l'organisation de défense des droits de l'Homme dans un communiqué.
La nouvelle législation prévoit la criminalisation d'une série d'expressions en ligne comportant notamment des critiques envers le gouvernement, des dignitaires religieux ou des dirigeants étrangers, relève Amnesty.
« Cette loi répressive » fait partie d'un éventail de législations destinées à « étouffer la liberté d'expression », a commenté Saïd Boumedouha, directeur adjoint d'Amnesty International pour le Moyen-Orient et l'Afrique du nord.
Des dizaines de personnes au Koweït ont été arrêtées et poursuivies en justice, certaines servant déjà des peines de prison, en vertu d'une autre législation pour des commentaires sur les réseaux sociaux.
Votée en juin, la nouvelle loi prévoit des peines de 10 ans de prison et des amendes allant jusqu'à 165.000 dollars pour des crimes en ligne, notamment ceux liés au terrorisme.
Pour le gouvernement, cette loi est nécessaire pour combler un vide juridique et réglementer l'utilisation des services en ligne tels que Twitter.
La peine minimale en vertu de la loi consiste en six mois de prison et 6.600 dollars d'amende pour celui qui ose, illégalement, « infiltrer un ordinateur ou un réseau électronique ».
« Les autorités koweïtiennes ne doivent pas appliquer cette loi jusqu'à ce qu'elle soit révisée pour se conformer aux obligations internationales du Koweït en matière de droits de l'Homme », a dit M. Boumedouha.
« Cette loi n'appartient pas au XXIe siècle », a-t-il ajouté, soulignant que « les Koweïtiens méritent mieux » qu'une telle législation.

Réagissez à cet article

Source : *Koweït: Amnesty critique la nouvelle loi sur la cybercriminalité – Internet – Notre Temps*

Fin du support de Windows 8 – Et maintenant ?

Fin du support de Windows 8 – Et maintenant ?

Les utilisateurs de Windows 8 qui veulent continuer à bénéficier des correctifs de sécurité sur leur système d'exploitation doivent maintenant passer à la version 8.1, considérée comme le dernier service pack en date de Windows 8. Par ailleurs, comme prévu, après ce 12 janvier, Microsoft cesse également de supporter de nombreuses versions de son navigateur Internet Explorer.

A peine plus de trois ans après sa sortie en octobre 2012, le mal-aimé Windows 8 ne sera plus supporté par Microsoft au-delà ce 12 janvier 2016, date de la première mise à jour de sécurité mensuelle de l'année (le fameux Patch Tuesday, désormais appelé Update Tuesday).

Pour accéder aux prochains correctifs de sécurité apportés à l'OS – et ne pas prêter le flanc aux attaques exploitant les failles qui pourraient y être découvertes à l'avenir – les utilisateurs devront passer à Windows 8.1. Ce dernier est en fait considéré comme un « service pack » de la version 8. Or, Microsoft laisse habituellement deux ans à ses clients pour installer les services packs de ses systèmes d'exploitation et la version finale de Windows 8.1 a été livrée en octobre 2013.

Une fois passé à Windows 8.1, les utilisateurs disposeront du support standard jusqu'au 9 janvier 2018. Ils pourront ensuite accéder au support étendu jusqu'au 10 janvier 2023.

Sur son site, Microsoft décrit clairement la situation : https://support.microsoft.com/en-us/lifecycle##gp/LifeWinFAQ

Autre option, passer à Windows 10

Pour les utilisateurs de Windows 8, l'autre option est de migrer directement vers Windows 10, lancée le 29 juillet dernier. Par ailleurs, ainsi que cela avait été annoncé de longue date, le 12 janvier 2016 marque également la livraison des dernières mises à jour pour plusieurs versions du navigateur web Internet Explorer, la plupart antérieures à IE 11. Microsoft en a fourni le détail depuis longtemps dans un tableau détaillant les versions d'IE supportées pour son OS desktop, pour Windows Server et pour l'OS embarqué (Windows Embedded). On voit ainsi qu'IE 9 est toujours supporté pour Windows Vista SP2, Windows Server 2008 SP2 et IA64. Les utilisateurs de Windows 7 SP1 devront utiliser IE 11. En revanche, IE 11 ne sera plus supporté pour Windows 8 et ses utilisateurs devront passer à 8.1 Update ou 10.

Beginning January 12, 2016, only the most current version of Internet Explorer available for a supported operating system will receive technical support and security updates, as shown in the table below:

Windows Desktop Operating Systems	Internet Explorer Version
Windows Vista SP2	Internet Explorer 9
Windows 7 SP1	Internet Explorer 11
Windows 8.1 Update	Internet Explorer 11

Windows Server Operating Systems	Internet Explorer Version
Windows Server 2008 SP2	Internet Explorer 9
Windows Server 2008 IA64 (Itanium)	Internet Explorer 9
Windows Server 2008 R2 SP1	Internet Explorer 11
Windows Server 2008 R2 IA64 (Itanium)	Internet Explorer 11
Windows Server 2012	Internet Explorer 10
Windows Server 2012 R2	Internet Explorer 11

Windows Embedded Operating Systems	Internet Explorer Version
Windows Embedded for Point of Service (WEPOS)	Internet Explorer 7
Windows Embedded Standard 2009 (WES09)	Internet Explorer 8
Windows Embedded POSReady 2009	Internet Explorer 8
Windows Embedded Standard 7	Internet Explorer 11
Windows Embedded POSReady 7	Internet Explorer 11
Windows Thin PC	Internet Explorer 8
Windows Embedded 8 Standard	Internet Explorer 10
Windows 8.1 Industry Update	Internet Explorer 11

For customers running on an older version of Internet Explorer, such as Internet Explorer 8 on Windows 7 Service Pack 1 (SP1), Microsoft recommends customers plan to migrate to one of the above supported operating systems and browser combinations by January 12, 2016.

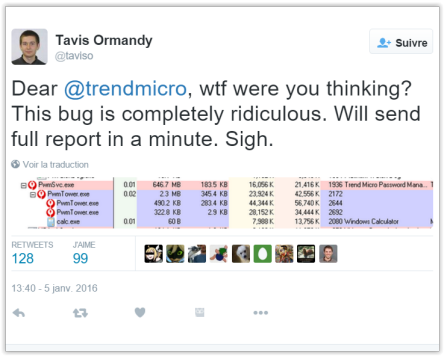
Réagissez à cet article

Le coffre-fort à mots de passe de Trend Micro pas si fort

Le coffre-fort à mots de passe de Trend Micro pas si fort

L'éditeur de solutions de sécurité Trend Micro a lancé un correctif pour patcher une faille dans son logiciel Password Manager permettant à un attaquant distant de voler les mots de passe utilisateur.

Un chercheur en sécurité de Google, Tavis Ormandy, a tiré la sonnette d'alarme après avoir trouvé plusieurs failles dans le gestionnaire de mots de passe de Trend Micro, Password Manager. Ces dernières peuvent permettre à un personne malintentionnée d'exécuter du code à distance et de voler les mots de passe des utilisateurs stockés dans ce logiciel. L'éditeur japonais a confirmé ces problèmes et propose une mise à jour automatique pour les résoudre.



Ce n'est pas la première fois que Tavis Ormandy alerte l'éditeur sur l'existence de telles failles de sécurité. Se sentant frustré par un temps de réaction trop long de Trend Micro, le chercheur de Google a d'ailleurs pris la décision de poster les derniers échanges qu'il a eus avec la société. « Alors cela signifie que n'importe quel internaute peut voler tous les mots de passe en silence, autant qu'exécuter du code arbitraire sans aucune interaction utilisateur », s'est indigné Tavis Ormandy. « J'espère vraiment que vous prenez conscience de la gravité de la situation car je suis très étonné de tout cela. »

Des mots de passe utilisateurs trouvés en 30 secondes

Les utilisateurs des solutions antivirus de Trend Micro peuvent choisir d'utiliser le gestionnaire de mots de passe Password Manager afin pour exporter dedans l'ensemble de leurs mots de passe et de n'avoir plus qu'un mot de passe maître à retenir et utiliser. Les concurrents Dashlane ou LastPass proposent des services similaires. Ce gestionnaire est écrit en Javascript avec node.js et ouvre de multiples ports HTTP RPC pour des requêtes API, a précisé Tavis Ormandy. En 30 secondes, le chercheur indique avoir trouvé une requête API permettant d'accepter du code distant et également qu'une autre lui a permis d'accéder aux mots de passe stockés dans le gestionnaire. Cerise sur le gâteau, M. Ormandy a trouvé plus de 70 API de Trend Micro étaient exposées et a recommandé – non sans humour – à l'éditeur de recruter un constant externe pour auditer son code.

Les logiciels antivirus tournent avec un haut niveau de privilège sur les systèmes d'exploitation, ce qui signifie que l'exploitation d'une vulnérabilité peut donner à un attaquant un accès profond à un ordinateur. Des dizaines de sévères vulnérabilités ont été trouvé sur les 7 derniers mois dans les logiciels antivirus incluant ceux de Kaspersky Lab, Eset, Avast, AVG Technologies, Intel Security et Malwarebytes.

Réagissez à cet article

Source : *Le coffre-fort à mots de passe de Trend Micro transformé en passoire – Le Monde Informatique*