Des règles désormais plus strictes pour la protection des données privées

Des règles désormais plus strictes pour la protection des données privées

La réforme décidée par le Parlement, la Commission et le Conseil européen aura de profondes implications. De plus le texte s'étendra aux pays associés à l'Union : Liechtenstein, Norvège et Islande. La Suisse s'en s'inspirera-t-elle ?

Après 3 ans, Parlement, Commission et Conseil Européen, le « trilogue » bruxellois, sont d'accord sur la réforme de la protection de la vie privée. La directive de 1995 et ses mises à jour étaient obsolètes et furent transposés sans harmonie dans les Etats, d'où l'idée d'un règlement qui s'appliquera tout de suite.

Ce règlement s'applique aux données privées traitées, pas celle qui sont stockées en vrac. Ce sont les résultats qu'on tire de l'exploitation de ces données qui sont dangereuses. Le règlement ne s'appliquera pas aux traitements des données dans un cadre privé (ouf !). Les autorités judiciaires ne seront pas soumises au contrôle des commissions de vie privée

Celui qui gère et traite vos données (le data controller) devra bien être identifié et réel. Celui qui héberge ses données (data processor) tombe aussi sous le règlement : s'il n'est pas établi dans l'Union, le règlement s'applique à lui quand même , surtout s'il s'agit de profiler le comportement en ligne des citoyens européens. Le pays superviseur sera celui du pays du siège principal du data controller et non pas là où les data centers ont été (dé)localisés. C'est à ce prix qu'un Amazon ou Google n'aura plus à dépendre de 28 commissions de vie privée différentes. Si l'entité n'est pas présente dans l'Union, elle doit mandater un représentant.
Le règlement évoque la pseudonymisation, une contraction d'anonymisation et pseudonyme : l'usage de pseudonymes n'exempte pas les sites d'appliquer le règlement, car on peut souvent remonter à qui est derrière. Par contre, le règlement ne s'applique plus après un décès !

Consentement
Le consentement de l'individu au traitement de ses données, qui existe depuis 1995, sera explicite et non tacite). Le data controller doit en garder la preuve: elle sera non valable si l'utilisateur final a subi un petit chantage (par ex. un service dégradé sans ces données privées). Pour la recherche scientifique, on admet qu'il n'est pas facile de demander à l'avance ce consentement, car on ne sait pas toujours ce qui va en sortir.
Si le data controller détecte des crimes ou des menaces à l'ordre public, il doit les communiquer aux autorités. Idem en cas de cybermenace.
Si le traitement des données vise un but humanitaire, de santé publique (épidémies), ou un cas d'urgence pour l'utilisateur final, leur traitement va de soi, consentement ou pas!
Les données sur l'emploi, la protection sociale et les revenus devraient aussi pouvoir être exploitées si le but est, pour l'État, d'augmenter le bien-être public et une politique ad hoc.
Le traitement de données personnelles doit être proportionnel : si on peut l'éviter à service équivalent, c'est mieux. De même, si la société qui a des données de vous ne sait pas vous identifier, elle ne doit pas chercher à le savoir pour… avoir votre consentement.

Les données sensibles : race, religion, opinion politique
Les données liées à l'exercice de droits et de choix fondamentaux, comme la religion, l'appartenance politique ou la race bénéficient d'une protection renforcée. Leur traitement devrait être une exception et soumis, avant leur exécution, à une analyse d'impact du risque encouru d'un tel profilage. Par contre, les photographies ne seront pas protégées saut à contenir des données biométriques.

Accès et rectification de données chez les tiers
Le droit à la rectification doit être aisé à exercer, en ligne par exemple si les données ont été collectées ainsi. Une réponse, oui ou non, sera fournie dans le mois.
À charge pour le data controller de vérifier que celui qui adresse sa demande d'accès est la bonne personne. Le droit à l'oubli à la «Google» devient… un droit à l'effacement si les données collectées ne sont plus nécessaires ou ne sont plus traitées. Ce droit à l'effacement s'opérera en cascade : les entités qui auraient rendu les données publiques seront obligées d'informer les autres qui les exploiteraient ou les auraient copiés.
À une demande d'une copie de ses données personnelles (droit d'accès), c'est un format lisible par un humain qui est exigé, pas du binaire ! D'ailleurs, dit le règlement, ne faudrait-il pas un format de donnes interopérables pour permettre, enfin, la portabilité des données entre sociétés. Il n'est pas précisé si c'est applicable au cloud (car c'est du stockage, pas du traitement). Le règlement évoque les algorithmes qui prennent des décisions sur base des données personnelles ainsi que le profilage.

Fuites et vol des données
Les fuites de données devront être notifiées aux autorités et aux personnes impactées dans les 72 heures à moins que leur chiffrage ne les rendent inviolables. À noter tout de même un relâchement de l'obligation de notifier à la commission de vie privée tous les traitements des données personnelles, uniquement les cas risqués d'atteintes aux droits et libertés fondamentales.

Échanges internationaux
Les données peuvent être échangées avec des pays tiers en dehors de l'Union : c'est à la Commission de statuer si le pays répond ou non aux exigences minimales de sécurité. La Commission peut aussi retirer son agrément.
Le data controller peut toutefois continuer à opérer avec un pays « peu sûr » s'il compense avec des mesures de sécurité supplémentaires. Les sociétés peuvent mettre en place entre leurs filiales des règles internes pour atteindre un même niveau de sécurité que le règlement. Attention aux échanges avec des pays tiers (ex : les USA à la demande d'une cour) et donc à l'application extraterritoriale de ses lois à des citoyens européens : ils sont autorisés s'ils sont couverts par un traité d'assistance mutuel.
Le texte s'étendra aux pays associés à l'Union : Liechtenstein, Norvège et Islande. La Suisse s'en s'inspirera-t-elle ?

Réagissez à cet article

Source : *Serrage de vis européen sur la protection des données privées – Le Temps*

Apprentissage :

l’intelligence artificielle, une élève de plus en plus douée

	**Apprentissage : l’ #intelligence artificielle, une élève de plus en plus douée**

Un programme informatique est-il capable, à #la manière d'un enfant, d'apprendre de son environnement ? S'il reste encore du chemin à parcourir, le machine learning, ou « apprentissage automatique », a connu des avancées significatives ces dernières années, poussé notamment par de grandes entreprises aux moyens inédits. Avec comme icône médiatique le Google Brain, qui a réussi la prouesse, en 2012, de découvrir le concept de chat en analysant des millions d'images issues du Web.

NOURRIR LE PROGRAMME : UN TRAVAIL FASTIDIEUX

La technique la plus courante de machine learning est l'apprentissage supervisé : pour qu'un programme apprenne à reconnaître une voiture, par exemple, on le nourrit de dizaines de milliers d'images de voitures, étiquetées comme telles. Un entraînement qui nécessite des heures, voire des jours, avant que le programme puisse en repérer sur de nouvelles images.

Cette technique est relativement ancienne, mais elle a fait un bond avec les récentes avancées technologiques. La masse de données désormais disponibles ainsi que la puissance de calcul à disposition des ingénieurs multiplient l'efficacité des algorithmes.

Cette nouvelle génération d'apprentissage supervisé fait déjà partie de notre quotidien : les outils de traduction automatique en sont le parfait exemple. En analysant des immenses bases de données associant des textes et leur traduction, le programme relève des régularités statistiques, sur lesquelles il se fonde pour trouver la traduction la plus probable non seulement d'un mot, mais aussi d'une formule, voire d'une phrase.

Efficace, cette méthode atteint vite ses limites. « Ces machines sont bêtes, souligne Pierre-Yves Oudeyer, directeur de recherche en robotique et sciences cognitives à l'Institut national de recherche en informatique et en automatique. Elles ne comprennent rien aux phrases qu'elles traduisent, elles ont juste vu que telle phrase était souvent traduite de telle manière. » Qui plus est, elles nécessitent un travail fastidieux de la part des ingénieurs, chargés de concevoir les gigantesques bases de données pour nourrir leur apprentissage.

QUAND UNE IA INVENTE LE CONCEPT DE CHAT

Les chercheurs en intelligence artificielle s'emploient à dépasser ces limites, pour se rapprocher de l'apprentissage humain, comme l'explique Andrew Ng :

« Si vous réfléchissez à la façon dont les enfants apprennent à reconnaître les voitures, il n'existe aucun parent, aussi attentionné et patient soit-il, qui pointera du doigt 50 000 voitures. La plupart des neuroscientifiques pensent que pour apprendre les animaux et les enfants vont dans le monde et l'expérimentent par eux-mêmes. »

C'est sur cette idée que repose le projet de deep learning Google Brain, un réseau de neurones artificiels créé en connectant pas moins de 16 000 processeurs. En 2012, soit un an après son lancement, c'est ce programme qui avait réussi à découvrir le concept de chat. Concrètement, la machine a analysé, pendant trois jours, dix millions de captures d'écran de YouTube, choisies aléatoirement et non étiquetées. A l'issue de cet entraînement, le programme avait appris à détecter des têtes de chats et des corps humains – des formes récurrentes dans les images analysées.

Lire nos explications : Comment le « deep learning » révolutionne l'intelligence artificielle

LE CAS COMPLEXE DES ROBOTS

Apprendre en expérimentant le monde : c'est la problématique à laquelle sont confrontés les chercheurs en robotique développementale et cognitive. « On tente de voir comment les robots peuvent apprendre le sens d'un mot, à travers l'expérience sensorielle et motrice, explique Pierre-Yves Oudeyer. Une chaise, par exemple, il va falloir qu'il l'expérimente, qu'il se rende compte qu'il peut s'y asseoir. »

Comme tout programme d'apprentissage, cela passe par la recherche de régularités :

« Cela peut être par exemple : "Quand je bouge mon bras de telle manière, il se passe ça." Ils pourront alors prédire les conséquences d'actions qui ne seront pas exactement les mêmes que celles déjà effectuées, dans un contexte qu'ils n'ont pas encore rencontré. »

Un sacré défi, car, contrairement au Google Brain, le robot doit collecter lui-même les expériences d'apprentissage. Impossible alors de s'entraîner sur des millions de possibilités, car cela prendrait trop de temps. Qui plus est, un robot doit être réactif à son environnement, et ne peut donc pas prendre plusieurs heures pour digérer les connaissances acquises lors de son expérience afin de préparer une réponse, qui sera entre-temps devenue obsolète.

Des expériences consistent par exemple à faire en sorte qu'un robot apprenne par lui-même à se déplacer. La machine doit expérimenter des mouvements puis enregistrer les conséquences sur son centre de gravité et son emplacement dans l'espace, puis en tirer des conclusions. Et recommencer, jusqu'à trouver la technique de déplacement la plus efficace.

Ces expérimentations peuvent être totalement aléatoires. Mais les scientifiques ont développé des algorithmes d'apprentissage actifs, « l'équivalent de la curiosité », précise Pierre-Yves Oudeyer, grâce auxquels les robots mesurent les expérimentations les plus intéressantes à effectuer pour progresser plus rapidement dans leur apprentissage. « On peut être surpris par le type de solution que le robot va trouver pour avancer. C'est parfois une solution qu'on n'avait pas imaginée, mais qui pourtant est efficace. »

« ON EST LOIN DE LA FLEXIBILITÉ D'UN ENFANT DE 5 OU 6 MOIS »

Malgré les résultats parfois impressionnants du machine learning, « le spectre de ce qu'une intelligence artificielle peut apprendre est très limité, nuance le chercheur. Le mécanisme de l'apprentissage chez l'enfant fait partie des grands mystères scientifiques, on balbutie donc dans la construction de machines dotées de capacités d'apprentissage similaires. » Pour les robots, « on est loin de la flexibilité d'un enfant de 5 ou 6 mois », prévient-il.

Et surtout, comment faire en sorte qu'un programme puisse apprendre sans l'intervention d'un ingénieur pour chaque tâche ? C'est une des grandes difficultés rencontrées dans l'apprentissage automatique :

« Aujourd'hui, on travaille sur des familles de tâches : faire qu'un robot apprenne à marcher, qu'il apprenne à attraper tel type d'objet, qu'il construise une carte d'un environnement… On développe un système ad hoc à chaque fois. Mais on ne sait pas comment une machine peut construire des représentations nouvelles pour des tâches nouvelles, comme apprendre à courir quand on sait marcher… On n'en a aucune idée. »

EN BREF :

Ce dont l'intelligence artificielle est aujourd'hui capable :

- faire évoluer ses connaissances en analysant des données ;
- découvrir des concepts en repérant seule des régularités statistiques.

Ce qu'elle ne sait pas faire :

- comprendre les concepts appris ;
- apprendre comme un enfant.

Les progrès qu'il reste à faire :

- apprendre de nouvelles tâches par elle-même ;
- développer sa curiosité.

Réagissez à cet article

Source : *Apprentissage : l'intelligence artificielle, une élève de plus en plus douée*

Quelles sont les modalités de blocage des sites Internet ?

	Quelles sont les modalités de #blocage des sites Internet ?

M. Lionel Tardy interroge M. le ministre de l'intérieur sur le décret n° 2015-125 du 5 février 2015 relatif au blocage des sites provoquant à des actes de terrorisme ou en faisant l'apologie et des sites diffusant des images et représentations de mineurs à caractère pornographiques.
Ce décret précise les modalités d'applications de l'article 6-1 de la loi pour la confiance dans l'économie numérique (LCEN). En complément, il souhaite savoir si, une fois la procédure appliquée, l'OCLCTIC sera également destinataire de données statistiques relatives aux tentatives de connexions aux sites bloqués, et le cas échéant, les modalités de ce recueil.

Texte de la réponse
La loi du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme a doté la France de nouveaux moyens face à la menace constante et croissante à laquelle elle est confrontée. Elle permet, notamment, de mieux combattre la propagande terroriste sur internet. Ses textes réglementaires d'application ont été rapidement publiés et toutes ses dispositions sont donc aujourd'hui applicables. Il en est ainsi des dispositions visant, suivant un dispositif gradué et équilibré garantissant le respect des libertés publiques, à renforcer les capacités de blocage des sites internet faisant l'apologie du terrorisme ou y provoquant. Le décret d'application a été publié dès le 5 février 2015 (décret no 2015-125 relatif au blocage des sites provoquant à des actes de terrorisme ou en faisant l'apologie et des sites diffusant des images et représentations de mineurs à caractère pornographique). S'agissant du nombre de connexions à un site dont l'accès est bloqué, il fait l'objet d'une comptabilisation assurée par la sous-direction de lutte contre la cybercriminalité de la direction centrale de la police judiciaire. Cette comptabilisation s'inscrit dans une démarche d'évaluation du dispositif mais vise aussi à mieux appréhender l'évolution du comportement des internautes. Lorsqu'un internaute tente de se connecter à un site dont l'accès est bloqué, il est immédiatement renvoyé sur une page d'information du ministère de l'intérieur, lui expliquant la nature du blocage et l'informant sur les voies de recours. L'adresse IP est enregistrée. Les adresses IP ainsi collectées ne sont pas exploitées mais permettent une comptabilisation précise du nombre de connexions à chacune des pages bloquées. Les premiers chiffres enregistrés depuis la mise en place du dispositif font apparaître plus de 30 000 connexions par semaine concernant les sites de pédo-pornographie, et 250 connexions en moyenne par semaine concernant les sites à caractère terroriste. Différents éléments peuvent expliquer cet écart. Dans la liste des sites dont l'accès est bloqué, ceux concernant la pédo-pornographie sont plus nombreux que ceux provoquant à des actes terroristes ou en faisant l'apologie (rapport de 3 pour 1). Par ailleurs, les connexions aux sites pédo-pornographiques ne sont pas toujours volontaires (liens publicitaires sur sites pornographiques légaux, « pourriels », etc.). Au-delà de ces dispositions nationales, le ministère de l'intérieur a engagé plusieurs actions à l'échelle européenne et internationale. En témoignent, notamment, les récentes rencontres du ministre de l'intérieur avec les grands acteurs américains de l'internet pour les amener à davantage participer à la régulation des contenus appelant à la commission d'actes terroristes ou en faisant l'apologie. Ces travaux ont notamment permis de décider la création d'une plate-forme de bonnes pratiques dans la lutte contre la propagande terroriste sur internet.

Réagissez à cet article

Source : *Question n°74166 – Assemblée nationale*

Le jour de la Cybersécurité maritime

Le jour de la Cybersécurité maritime

Alors qu'était publié le 25 décembre 2011 mon premier article consacré à (l'absence de) la cybersécurité dans le secteur maritime, jamais je n'aurais imaginé y revenir avec une telle régularité chaque 25 décembre depuis [1].

De là à imaginer que ce jour pourrait devenir LE jour de l'année où l'on y penserait, il n'y a qu'un pas que j'ai eu envie de franchir ! J'appelle donc solennellement de mes vœux, et en toute simplicité, qu'une autorité nationale, européenne voire internationale décrète que chaque 25 décembre soit la journée de la cybersécurité du secteur maritime.
Si mon souhait se perd dans l'immensité intersidérale du cyberespace, vous pouvez compter sur moi pour cette amicale « piqûre de rappel » aussi longtemps qu'elle sera nécessaire. En souhaitant simplement que je cesse ce rappel avant 2020 sinon cela signifiera que le niveau d'inquiétude et, surtout, de risque aura grimpé en flèche. Mais puisque c'est actuellement la trêve des confiseurs et parce que l'année 2015 aura été particulièrement difficile en France [2], essayons de rêver quelques instants.
Saluons tout d'abord la tenue des « premières rencontres parlementaires cybersécurité et milieu maritime » le 12 février 2015 à Paris, brillamment organisées par le « Cybercercle » qu'il convient ici de saluer pour son rôle et son activisme passionné. A la suite de cette journée, une lettre autour de ces rencontres, que je recommande, a été publiée [3].
Fin octobre, le colloque Safer Seas [4] a réuni à Brest l'ensemble des acteurs du secteur. Une part modeste mais somme toute bien visible [5] a été laissée à la cybersécurité notamment sous l'angle de la cybercriminalité [6].
Si, sans doute, trop nombreux sont encore les décideurs du secteur maritime à découvrir que des ports aux navires en passant par la supply chain tout ce qui embarque de l'informatique doit être soumis à interrogation, ne boudons cependant pas notre plaisir. Oui la prise de conscience a lieu et, oui, enfin, tout le monde est en train de (ou va prochainement) se mettre autour de la table pour en discuter.
La prochaine étape va donc consister à passer de la prise de conscience aux paroles, que l'on espère fortes, puis à leur concrétisation : évaluation globale des risques informatiques, audits [7], développement et insertion de services et de produits qualifiés [8], processus d'homologation [9], éducation via de la sensibilisation à l'ensemble des salariés de la filière, bonnes pratiques, etc. L'ampleur de la tâche étant si vaste [10], il faut simplement souhaiter et agir rapidement pour que les prochaines étapes ne s'effectuent pas au rythme d'une annexe à rame mais bien plus sur celui d'un hydroglisseur commandé par un capitaine expérimenté et volontaire, entouré d'un équipage adroit et tenace y compris – et surtout – au cœur des tempêtes qui s'annoncent.

[1] ou presque : 2013 puis 2014
[2] tant par les attentats de janvier et de novembre que par l'inexorable montée du chômage et la paupérisation continue d'une part croissante de nos concitoyens
[3] http://fr.calameo.com/read/004370735c23949b43ff3
[4] http://www.saferseas-brest.org/
[5] http://presse.rivacom.fr/fr/newsletter/1494/la-cybersecurite-un-enjeu-majeur-pour-le-monde-maritime
[6] http://www.letelegramme.fr/bretagne/mer/cybercriminalite-bateaux-et-ports-pour-cibles-28-10-2015-10829564.php
[7] http://si-vis.blogspot.fr/2015/02/tester-son-niveau-de-cybersecurite.html
[8] http://www.ssi.gouv.fr/entreprise/qualifications/
[9] http://www.ssi.gouv.fr/actualite/pour-homologuer-votre-systeme-dinformation-suivez-le-guide/
[1 0]
http://arstechnica.com/information-technology/2015/12/hacked-at-sea-researchers-find-ships-data-recorders-vulnerable-to-attack/

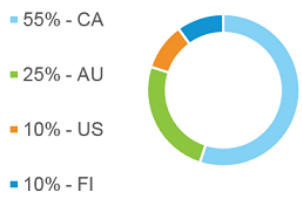
Réagissez à cet article

Source : *Si vis pacem para bellum: Cybersécurité maritime 2015*

Le cheval de Troie Ramnit refait surface

Le cheval de Troie Ramnit refait surface

Ramnit refait surface moins d'un an après l'offensive d'Europol contre ses serveurs de contrôle Une première pour un botnet bancaire selon IBM



En février dernier, suite à une opération menée par plusieurs États ainsi que des acteurs privés (parmi lesquels Microsoft, Symantec et AnubisNetworks) qui a été coordonnée par le centre de lutte contre la cybercriminalité d'Europol, un réseau de serveurs de contrôle du botnet Ramnit a été démantelé. Trois cents domaines internet exploités par les pirates ont également été redirigés.
Détecté pour la première fois en 2010, le cheval de Troie Ramnit permettrait de gagner un accès distant aux ordinateurs Windows infectés et de subtiliser par la suite des données sensibles, comme des informations bancaires. Wil van Gemert, le directeur des opérations d'Europol, a salué le succès de l'opération : « cette opération réussie illustre l'importance pour les forces de l'ordre internationales de travailler de concert avec l'industrie privée afin de lutter contre la menace globale du cybercrime ».
Seulement, les chercheurs d'IBM ont mis la main sur une variante du cheval de Troie qui se base sur une infrastructure C&C différente de son prédécesseur et emploie un fichier de configuration plus court ainsi qu'un schéma d'injection web différent pour infecter les victimes. Plus de la moitié des infections a été observée au Canada. En seconde position sur la liste des pays les plus affectés viennent l'Australie qui compte à elle seule une infection sur quatre, puis les États-Unis.
Selon les chercheurs de la X-Force d'IBM, il semblerait que ce soit la première fois qu'un botnet de fraude bancaire refasse surface, ce qui a aiguisé leur curiosité puisque, jusqu'à présent, c'étaient plutôt les botnets de spams qui étaient souvent ramenés en circulation, les cybercriminels derrière les botnets de fraude bancaire préférant se contenter de l'argent déjà collecté et du fait qu'ils n'aient pas été arrêtés.
Les experts expliquent que « le cheval de Troie arborait un fichier de configuration lourd avec des déclencheurs d'URL qui lui indiquaient vers quelle banque, quelle transaction et quels sites de réseau social se tourner pour collecter des informations d'identification ». La configuration de Ramnit est orientée pour tenir les victimes éloignées d'une liste exhaustive d'outils de scans en ligne, de sites web d'antivirus, des sites d'information sur le cybercrime, mais également des blogs de sécurité. « Dans son ancienne configuration, la seule utilisation des mots « cybercriminalité » ou « police » de la part des victimes suffisait à déclencher un effet de redirection ».
Une autre trace laissée par les anciennes configurations est la liste relativement importante de sites de recrutements récoltant les informations d'identification, afin de viser ceux qui sont à la recherche d'un emploi et de les recruter. « Pour les victimes, cela pouvait être une lame à double tranchant étant donné que les opérateurs Ramnit pouvaient également obtenir toutes les informations qu'elles ont mises sur leur CV professionnel ».
La X-Force Threat Intelligence d'IBM n'a pas eu vent du fait que le code source de Ramnit ait été vendu ouvertement, partagé avec d'autres groupes de cybercriminels ou sur les forums dans le marché noir. Aussi, ils pensent qu'il y a de fortes chances qu'il s'agisse là du même groupe d'individus qui a remis cette nouvelle version en activité.

Réagissez à cet article

Source : *Ramnit refait surface moins d'un an après l'offensive d'Europol contre ses serveurs de contrôle, une première pour un botnet bancaire selon IBM*

La cybercriminalité en nette hausse en fin d’année

La cybercriminalité en nette hausse en fin d’année

« La cybercriminalité en nette hausse au cours du 3e trimestre 2015 » , titre le site www.developpez.com qui ajoute que « ces problématiques de sécurité constituent un prélude à des événements majeurs dont l’impact sera, selon Trend Micro, particulièrement fort en 2016 ».

Le site s’appuie sur une étude de Trend Micro intitulé « Hazards Ahead : Current Vulnerabilities Prelude Impending Attacks », qui revient longuement sur le bilan en forte progression des faits de délinquance informatique au 3e trimestre 2015, avant d’esquisser une perspective pour l’année 2016 qui sera aussi riche, selon l’étude, du fait notamment du développement des technologies mobiles et de l’internet des objets.
Pour un responsable de chez Trend Micro, interrogé par les auteurs de l’enquête de terrain, il est clair que « l’évolution des piratages commence à grever la rentabilité des entreprises et le quotidien de tout un chacun ».
L’intérêt de cette étude est qu’elle donne un aperçu sur les « dégâts » occasionnés par la délinquance informatique sur la vie privée de citoyens qui en sont victimes.
« Des cas de suicides ont d’ailleurs été recensés du fait des conséquences de cette attaque sur la vie privée des utilisateurs du site », relève le site qui évoque, en effet, une attaque massive, avec vol de données de quelque 30 millions d’utilisateurs contre Ashley Madison. Il s’agit, nous apprend l’encyclopédie en ligne Wikipedia d’un « site de rencontres en ligne et un réseau social canadien.
Le public visé est celui des internautes mariés, ou du moins vivant en couple, et souhaitant avoir une relation extraconjugale ».

Réagissez à cet article

Source : *« La cybercriminalité en nette hausse au cours… – Horizons*

Cyber attaque arabe contre Israël

Cyber attaque arabe contre Israël

Un groupe de hackers arabes surnommé Kadmoun a annoncé qu'il avait entamé une série d'attaque massive contre 1 600 sites israéliens en ligne. Une semaine après la liquidation du terroriste Samir Kountar à Damas, attribuée à Israël, cette attaque n'a pas encore été repérée en Israël.

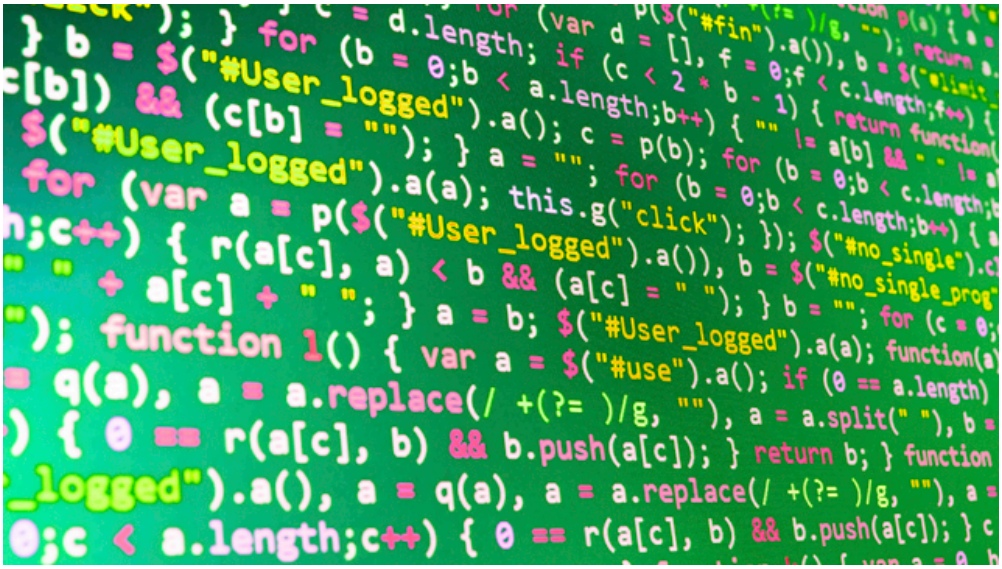
Réagissez à cet article

Source : *Cyber attaque arabe contre Israël | Coolamnews*

Code Erreur 451 en cas de site bloqué ou censuré par un organisme gouvernemental

Code Erreur 451 en cas de site bloqué ou censuré par un organisme gouvernemental

Les sites Web censurés sont désormais indiqués par un code « Error : 451 » de l'Internet Engineering Task Force.



L'Internet Engineering Task Force – IETF – vient d'officialiser un nouveau code d'erreur pour indiquer qu'un site est bloqué ou censuré par un organisme gouvernemental. Suite à ce vote, les internautes du monde entier vont désormais savoir quand un gouvernement veut leur interdire d'accéder à un site Internet. Le code en question – Error 451 (en anglais) – devient synonyme de censure sur Internet. Le code HTTP Erreur 404 est bien connu des internautes, tout comme le code Erreur 500 dans une moindre mesure – qui indique un problème de serveur. Ne doutons pas que l'**Erreur 451** va rapidement devenir l'un des codes d'erreur stars de la toile.

L'organisme de standardisation du Web a décidé d'indiquer dans un souci de transparence qu'un site Internet est interdit, bloqué ou censuré dès qu'un utilisateur tente de s'y connecter. L'IETF prévoit notamment que le gouvernement à l'origine de cette censure pourra accompagner le message d'erreur d'une explication sur les causes du blocage d'accès. L'origine du nombre « 451 » est une référence dans la plus pure tradition des geeks, puisque l'erreur 451 renvoie à l'ouvrage de science-fiction de Ray Bradbury « **Fahrenheit 451** » publié en 1953 et dont le thème central est la dénonciation de la censure et de toute forme de propagande. Le message universel de libre accès l'information sur Internet existe encore.

Réagissez à cet article

Source : *Le code Erreur 451 synonyme de censure*

Le site de la BBC victime d’une cyber-attaque

Le site de la BBC victime d’une cyber-attaque

Ce jeudi matin, tous les sites de la BBC étaient inaccessibles à cause d'une attaque par déni de service…

Une cyber-attaque de grande ampleur. Le fonctionnement du site Internet de la BBC a été perturbé jeudi matin par une attaque par déni de services, rendant la consultation des informations impossible, selon un article du groupe britannique d'audiovisuel public.

« Une attaque par déni de service »

« Tous les sites Internet de la BBC étaient inaccessibles jeudi matin en raison d'une importante cyber-attaque », a indiqué la chaîne dans un article publié dans la section technologie de son site Internet attaqué qui était consultable par intermittence dans la matinée.
« Des sources au sein de la BBC ont indiqué que les sites étaient inaccessibles à cause d'une attaque par déni de service », ajoute l'article qui précise que l'attaque a porté sur le site et des services associés comme le service iPlayer pour revoir les émissions et l'application iPlayer Radio.

La situation est revenue à la normale

« Le site de la BBC est maintenant de retour et fonctionne normalement. Nous nous excusons pour le désagrément », a indiqué peu après 12h GMT une porte-parole de la chaîne dans un communiqué.
Ce type d'attaques a pour but de rendre un service indisponible en inondant un réseau ou en perturbant les connexions à un serveur.

La BBC déjà victime d'une cyber-attaque

En juillet 2014, une précédente attaque avait paralysé le service iPlayer de la BBC pendant un week-end entier, précise le groupe britannique d'audiovisuel public.
En septembre dernier, c'était le site Internet de l'Agence britannique de lutte contre le crime (NCA) qui avait été perturbé en raison d'une attaque équivalente, dans ce qui s'apparentait à une riposte d'un groupe de pirates après une série d'arrestations.
Selon la police, quelque 30 % des entreprises britanniques ont signalé avoir subi des attaques par déni de service en 2014.

Réagissez à cet article

Source : *Le site de la BBC victime d'une cyber-attaque*

Plus de 34 000 utilisateurs de Steam concernés par le piratage de données personnelles

Plus de 34 000 utilisateurs de Steam concernés par le piratage de données personnelles

Selon Valve, l'éditeur du service cloud de jeux vidéo Steam, c'est la combinaison d'une attaque par déni de service visant le Steam Store et d'un problème de cache qui est à l'origine de l'exposition des données personnelles de 34 000 clients.
Valve s'est finalement expliqué plus en détails sur ce qui s'est passé le jour de Noël sur sa plateforme Steam. Rappelons que des utilisateurs du service de distribution de jeux vidéo ont remarqué avoir accès depuis leurs comptes à des données personnelles d'autres utilisateurs, comme leurs adresses mail, leurs historiques d'achats, ou encore leurs numéros (incomplets) de cartes de crédit.

Dans un communiqué diffusé hier, Valve explique que ce bug est le résultat de deux facteurs : une attaque par déni de service qui a touché son magasin en ligne, le Steam Store, et une erreur dans le système de cache qui fut déployé pour la contrer. "Au cours de la deuxième vague de cette attaque, la seconde configuration de cache déployée a mal géré le trafic web en cache pour les utilisateurs authentifiés. Cette erreur de configuration s'est traduite pour certains utilisateurs capables de voir des réponses du Steam Store qui étaient générées pour d'autres usagers."

Valve a indiqué que les données personnelles de 34 000 clients ont ainsi été exposées. L'entreprise dit travailler avec son partenaire gérant la mise en cache afin d'identifier chaque client affecté pour pouvoir le contacter directement. (Eureka Presse)

Réagissez à cet article

Source : *Steam : plus de 30 000 utilisateurs concernés par le*

piratage de données