Contrôles de la CNIL en 2015 – Demandez le programme… | Le Net Expert Informatique

Contrôles de la CNIL en 2015 – Demandez le programme…

En 2015, la CNIL contrôlera des technologies ou des traitements récemment mis en œuvre et faisant partie du quotidien des Français.

En 2015, un objectif d'environ 550 contrôles est prévu (421 contrôles réalisés en 2014), se décomposant de la façon suivante :
• environ 350 vérifications sur place, sur audition ou sur pièces. Un quart des contrôles sur place portera sur les dispositifs de vidéoprotection / vidéosurveillance
• 200 contrôles en ligne.

Les thématiques prioritaires des contrôles 2015
Comme chaque année, la CNIL prévoit de dédier une part significative de son activité de contrôle à des thèmes choisis du fait de leur impact sur les libertés et du nombre important de personnes concernées.

Le paiement sans contact : le large développement de ces dispositifs en fait une thématique de première importance, eu égard notamment au nombre de personnes concernées. Outre les questions de sécurité, la prise en compte du droit d'opposition sera notamment vérifiée.

Le traitement de données personnelles dans le cadre de la gestion des risques psycho-sociaux (RPS) en entreprise : dans le prolongement de l'accord national interprofessionnel de 2008 relatif à l'amélioration des conditions de travail, de plus en plus d'entreprises diligentent des enquêtes sur les risques psychosociaux auprès de leur salariés afin d'évaluer et de mieux lutter contre le stress au travail. Ces enquêtes soulèvent des questions pratiques qui ont conduit de nombreux salariés à saisir la CNIL. Les contrôles s'opèreront auprès de prestataires et d'entreprises (publiques et privées) ayant mené une enquête RPS ces dernières années.

Le Fichier National des Permis de Conduire mis en œuvre par le ministère de l'Intérieur : ce fichier répertorie l'ensemble des permis de conduire enregistrés en France (environ 40 millions). Le solde des points restants sur le permis est consultable en ligne depuis le site telepoints.info. Le FNPC comporte également toutes les décisions relatives au permis de conduire, et notamment, les décisions administratives (retrait, suspension, annulation, restriction du droit d'en faire usage) et judiciaires (y compris les compositions pénales, amendes ainsi que les procès-verbaux des infractions constatées). Les vérifications porteront en particulier sur la fiabilité et la mise à jour des données, leurs modalités d'accès et leur sécurisation.

Les objets connectés « bien-être et santé » : un écosystème s'est développé autour d'une offre bien-être et santé comprenant des objets connectés et des services en ligne, permettant le suivi individuel et le partage de données relatives par exemple à l'activité physique ou l'évolution de la corpulence du détenteur. Ces dispositifs suscitent de nombreuses interrogations quant à l'information et au consentement des utilisateurs.

Les outils de mesure de fréquentation des lieux publics : ces nouveaux dispositifs déployés dans l'espace public (centres commerciaux, quartiers ou villes entières) permettent via les connexions aux bornes mobiles et wifi une mesure fine du trafic de données personnelles. Ces mesures permettent entre autres objectifs de monétiser l'espace publicitaire. Des contrôles sur ces thèmes permettront de renforcer la doctrine naissante.

Les « Binding Corporate Rules » (BCR) : à ce jour, 68 sociétés ont adopté des BCR. Ces dispositifs n'ont fait pour l'heure l'objet d'aucun contrôle ex-post. La réalisation de contrôles de quelques entreprises ayant adopté des BCR fournira un éclairage sur l'impact du dispositif au regard de la protection des données personnelles et du respect de la vie privée au sein des groupes concernés.

Enfin, l'année 2015 sera l'occasion pour la CNIL de continuer le travail de coopération internationale entre autorités de protection des données. Cette coopération s'effectuera notamment au travers du troisième volet du « Sweep Day » coordonnée par le GPEN (« Global Privacy Enforcement Network » – réseau international d'autorités en charge de la protection de la vie privée) qui concernera le thème de « la vie privée de la jeunesse » (« Youth Privacy »).

Concrètement, l'audit conjoint qui sera réalisé en mai portera sur les services en ligne proposés aux mineurs (sites visant particulièrement les utilisateurs de moins de 12 ans et/ou les adolescents). Les autorités se concentreront notamment sur l'information, et le contrôle de l'âge.

En outre, des contrôles seront menés dans le cadre de la coopération européenne en matière de police (Europol, Schengen, etc.).

Source : http://www.cnil.fr/linstitution/actualite/article/article/programme-des-controles-2015/

Android : vos données personnelles impossibles à effacer ? | Le Net Expert Informatique

Des chercheurs ont mis en lumière les problèmes de sécurité du système d'exploitation mobile de Google.
Grâce à un seul petit bouton « Restaurer les paramètres d'usine », Google promet à ses utilisateurs de supprimer tous les contenus de leur smartphone Android. La mémoire du smartphone serait ainsi totalement effacée. Mais à en croire une étude menée par deux chercheurs de l'université de Cambridge, il n'en est rien : cette fonction de suppression serait inefficace sur plus de 500 millions de smartphones Android. Explications.

Quelles données ont été récupérées ?
Les chercheurs ont examiné 21 smartphones de 5 grandes marques et sous différentes versions d'Android : Samsung Galaxy S2 et S3, LG Optimus L7, Nexus 7, HTC Desire C, Motorola Razr I, etc. Cet échantillon représenterait près de 500 millions de smartphones actuellement en circulation. Sur la totalité des smartphones étudiés, les données personnelles ont pu être récupérées après avoir été effacées. Les deux chercheurs ont ainsi pu mettre la main sur les identifiants Google des utilisateurs sur tous les modèles. Puis, ils ont pu accéder aux informations des services Google associés à ces comptes : Gmail, Calendrier, Drive, etc. Enfin, les chercheurs ont pu récupérer des données de communications (SMS, e-mails, appels, etc.) et des fichiers multimédias (photos et vidéos).

Comment c'est possible ?
Comme l'explique le résultat des recherches, lorsqu'un utilisateur appuie sur le bouton pour effacer ses données, le smartphone supprime en réalité l'accès à ces données et non les informations elles-mêmes. « C'est comme pour un ordinateur : un formatage du disque dur ne suffit pas à effacer les données », explique à Europe 1 Jean-François Beuze, expert en sécurité informatique.

Comment être sûr que toutes les données sont effacées ?
« Il faut chiffrer ses données », conseille le spécialiste en sécurité. C'est à dire ajouter une étape de protection supplémentaire à ces informations personnelles. Pour cela, il faut se rendre dans les réglages du smartphone, puis dans le menu Sécurité et enfin cocher la case « chiffrer les données sur le smartphone ». Si une carte mémoire est utilisée pour étendre le stockage de l'appareil, l'utilisateur devra également chiffrer celle-ci. Pour les données les plus sensibles, « il existe des appareils émettant un champ électromagnétique pour effacer toute donnée sur le smartphone », ajoute Jean-François Beuze. Mais ces appareils restent réservés aux professionnels en raison de leur coût élevé.

Source : http://www.europe1.fr/technologies/android-les-donnees-personnelles-impossibles-a-effacer-970842

Attaque à grande échelle de routeurs | Le Net Expert Informatique

Une attaque à grande échelle utilise les browsers pour détourner les routeurs

Des chercheurs ont découvert un outil d'attaque web qui permet à des pirates de détourner les serveurs DNS des routeurs et de les remplacer par des serveurs voyous.

Des cybercriminels ont développé un outil d'attaque web à grande échelle qui leur permet d'exploiter les vulnérabilités des routeurs et de détourner leurs paramètres DNS quand les utilisateurs visitent des sites web compromis ou sont dirigés vers des publicités malveillantes depuis leurs navigateurs. L'objectif de ces attaques est de remplacer les serveurs DNS configurés sur les routeurs par des serveurs voyous contrôlés par des attaquants. Ainsi, les pirates peuvent intercepter le trafic, le rediriger vers des sites frauduleux, détourner les requêtes de recherche, injecter des publicités malveillantes sur les pages web et plus encore.

L'adresse DNS, qui est comparable à un annuaire de l'Internet, a un rôle essentiel. Elle traduit les noms de domaine, plus faciles à mémoriser, en adresses IP indispensables pour faire communiquer les ordinateurs entre eux. La gestion des adresses DNS se fait en cascade. Quand un utilisateur tape le nom d'un site Web dans un navigateur, la requête est d'abord transmise au système d'exploitation. Et, pour diriger le navigateur vers l'adresse IP demandée, le système d'exploitation doit passer par le routeur local qui est lui-même chargé d'interroger les serveurs DNS généralement configurés et gérés par le fournisseur d'accès internet. La chaîne de commandes se poursuit jusqu'à ce que la demande parvienne au serveur ayant autorité pour le nom de domaine recherché ou jusqu'à ce qu'un serveur fournisse les informations de son cache. Or, si des attaquants d'immiscent dans une des étapes du processus, ils peuvent répondre à la requête en renvoyant une adresse IP frauduleuse. Ils peuvent ainsi tromper le navigateur et l'orienter vers le site d'un serveur différent. Typiquement, ce site pourrait, par exemple, héberger la réplique d'un site réel qui servirait aux pirates à dérober des informations de connexion d'un utilisateur.

Détecter le routeur pour adapter l'attaque

Un chercheur en sécurité indépendant, connu en ligne sous le nom de Kafeine, a récemment observé des attaques dites « drive-by » lancées à partir de sites web compromis qui redirigeaient les utilisateurs vers un kit d'exploits inhabituel basé sur le web, spécifiquement conçu pour compromettre les routeurs. En général, les kits d'exploits vendus sur les forums illégaux et utilisés par les cybercriminels cherchent à exploiter des vulnérabilités dans les plug-ins pour navigateurs comme Flash Player, Java, Adobe Reader ou Silverlight. Leur but est d'installer des logiciels malveillants sur les ordinateurs qui n'auraient pas téléchargé les dernières versions de ces modules populaires. Le plus souvent la stratégie de ces attaques consiste à injecter un code malveillant dans des sites compromis ou de l'inclure dans des publicités malveillantes, code qui redirige automatiquement les navigateurs vers un serveur d'attaque chargé de déterminer l'OS, l'adresse IP, la localisation géographique, le type de navigateur utilisé, les plug-ins installés et d'autres détails techniques. En fonction de ces informations, le serveur d'attaque sélectionne dans son arsenal d'exploits ceux qui ont le plus de change de réussir.
Mais, les attaques observées par Kafeine fonctionnent différemment : cette fois, les utilisateurs de Google Chrome ont bien été redirigés vers un serveur malveillant, mais celui-ci a chargé un code destiné à déterminer le modèle de routeur utilisé afin de remplacer les serveurs DNS configurés sur l'appareil. « Beaucoup d'utilisateurs pensent que si leurs routeurs ne sont pas configurés pour la gestion à distance, les pirates ne peuvent pas exploiter les vulnérabilités de leurs interfaces d'administration web à partir d'Internet, parce que ces interfaces ne sont accessibles qu'à partir des réseaux locaux. Mais, cela est faux », a déclaré le chercheur. De telles attaques sont possibles grâce à une technique appelée Cross-Site Request Forgery (CSRF), laquelle permet à un site web malveillant de forcer le navigateur à exécuter des actions malveillantes sur un site Internet différent. Et le site cible peut justement être l'interface d'administration d'un routeur uniquement accessible via le réseau local. De nombreux sites web ont mis en place des défenses pour se protéger contre ces attaques CSRF, mais les routeurs ne bénéficient généralement pas de ce type de protection.

Les principaux routeurs vulnérables

Le nouveau kit d'exploits drive-by identifié par Kafeine a utilisé la technique du Cross-Site Request Forgery pour détecter plus de 40 modèles de routeur de divers fournisseurs dont Asustek Computer, Belkin, D-Link, Edimax Technology, Linksys, Medialink, Microsoft, Netgear, Shenzhen Tenda Technology, TP-Link Technologies, Netis Systems, Trendnet, ZyXEL Communications et HooToo. Selon le modèle, l'outil essaie de changer les paramètres DNS du routeur en exploitant des vulnérabilités connues par injection de commande ou en utilisant des identifiants d'administration courants. Dans ce cas aussi, il utilise la technique CSRF. Et en cas de succès de l'attaque, le serveur DNS primaire du routeur passe sous contrôle des attaquants et le serveur secondaire, utilisé comme relais en cas de panne, est paramétré en tant que serveur DNS public de Google. De sorte que, si le serveur malveillant est temporairement hors service, le routeur disposera toujours d'un serveur DNS parfaitement fonctionnel pour résoudre les requêtes, et le propriétaire ne pourra pas soupçonner une défaillance, ni être tenté de reconfigurer l'appareil.

Selon Kafeine, l'une des vulnérabilités exploitées par l'attaque affecte les routeurs de divers fournisseurs, et a été rendue publique en février. « Certains fournisseurs ont effectué des mises à jour de firmware sur leurs routeurs, mais le nombre de matériels mis à jour au cours des derniers mois reste probablement très faible », a déclaré le chercheur. Car la plupart des routeurs doivent être mis à jour manuellement et l'opération exige certaines compétences techniques. Voilà pourquoi un grand nombre de routeurs ne sont pas mis à jour. Et les attaquants le savent. En fait, d'autres vulnérabilités sont ciblées par ce kit d'exploits, dont l'une a été identifiée en 2008 et l'autre en 2013.

1 million de tentatives le 9 mai

Toujours selon le chercheur indépendant, il semble que l'attaque a été menée à grande échelle : au cours de la première semaine du mois de mai, le serveur d'attaque a comptabilisé environ 250 000 visites uniques par jour, avec un pic de près de 1 million de visites le 9 mai. Les pays les plus touchés étaient les États-Unis, la Russie, l'Australie, le Brésil et l'Inde, mais la répartition du trafic a été plus ou moins globale. Pour se protéger, les utilisateurs doivent vérifier régulièrement si de nouvelles mises à jour de firmware pour leurs routeurs sont disponibles sur les sites Web des fabricants et ils doivent les installer, surtout si ces mises à jour concernent des correctifs de sécurité. Si le routeur le permet, les utilisateurs devraient également limiter l'accès à l'interface d'administration à une adresse IP à laquelle aucun terminal n'a normalement accès, mais qu'ils peuvent affecter manuellement à leur ordinateur en cas de besoin de façon à pouvoir modifier les paramètres de leur routeur.

Source : http://www.lemondeinformatique.fr/actualites/lire-une-attaque-a-grande-echelle-utilise-les-browsers-pour-detourner-les-routeurs-61265.html
Par Jean Elyan

« Vol » de documents via Google, la condamnation de Bluetouff confirmée | Le Net Expert Informatique

	« Vol » de documents via Google, la condamnation de Bluetouff confirmée

Olivier Laurelli, relaxé en première instance, avait accédé sans piratage à un extranet accessible par le moteur de recherche. Condamné en appel, son pourvoi en cassation a été rejeté.

Trop fouiller dans Google peut être cause de sanction judiciaire. Olivier Lorelli, alias Bluetouff, blogueur reconnu dans le domaine de la sécurité informatique, cofondateur du site Reflets.info, en fait l'amère expérience. Le spécialiste voit en effet sa condamnation pour « maintien frauduleux » dans le système et « vol » de documents confirmée par la Cour de cassation, révèle Le Parisien.
Rappel des faits. En 2012 Bluetouff avait trouvé par hasard « le serveur extranet de l'Agence nationale de sécurité sanitaire de l'alimentation, de l'environnement et du travail (Anses), utilisé par les chercheurs pour stocker et échanger leurs documents de travail. Au lieu d'être protégées par un identifiant et un mot de passe, comme elles auraient dû l'être, ces données, indexées sur Google, étaient accessibles sans le moindre piratage. »
Le blogueur télécharge alors 8.000 de ces documents internes, sur des données de santé publique. Il publie plus tard un article sur les nanoparticules qui utilise une infime partie de ces documents, ce qui alerte l'Anses, laquelle lance la police sur l'affaire. La DCRI identifie le blogueur, et s'ensuivent une perquisition à son domicile, la saisie de son matériel informatique et une garde à vue de 30 heures. Rien que ça.

« Gogleu ? Lojin ? »
Olivier Laurelli est presque logiquement relaxé en première instance. En avril 2013, les juges considèrent qu'il n'y a pas eu de piratage pour accéder aux documents (récit par l'intéressé) : « Il n'est pas contesté par l'Anses qu'une défaillance technique existait dans le système et que Monsieur Olivier Laurelli a pu récupérer l'ensemble des documents sans aucun procédé de type « hacking » », écrivaient-ils.
L'Anses ne fait d'ailleurs pas appel, contrairement au Parquet qui ne digère pas cette relaxe. Mauvaise pioche pour Bluetouff, le second procès, en décembre dernier, a opposé le pseudo-pirate à des juges visiblement très loin de maîtriser le sujet.
Un journaliste de Médiapart rapporte que « la magistrate chargée de rappeler les faits semblait même ne pas connaître Google, prononcé à la française « gogleu », ni savoir ce que signifie un « login », prononcé « lojin ». Difficile, dans ces conditions, d'expliquer qu'il est effectivement possible de tomber sur des documents de travail par une simple recherche… […] « Vous ne vous souciez pas de savoir si vous alliez tuer toute la planète? » s'indigne ainsi une magistrate alors que l'accusé vient de lui expliquer que ces documents n'étaient, visiblement, pas confidentiels. »
Si les juges relaxent le blogueur du chef d'« accès frauduleux », il le condamne néanmoins à une amende de 3.000 euros pour « maintien frauduleux dans un système de traitement automatisé de données » et « vol » de documents. De plus, cette peine sera inscrite à son casier judiciaire.
Olivier Laurelli et son avocat, Olivier Iteanu, décident alors de se pourvoir en cassation, pourvoi donc rejeté : la condamnation est donc confirmée. Dénonçant un « vrai scandale », l'avocat du blogueur, a annoncé à nos confrères son intention de saisir la Cour européenne des droits de l'Homme. Selon lui, on « fait payer » à son client des écrits « mettant en cause des entreprises et des services français ».
Le fait qu'aucun piratage n'ait été effectué n'a pas ému la cour qui rappelons-le ne juge que la forme, pas le fond de la procédure. Reste que cette condamnation confirmée constitue une très mauvaise nouvelle pour les lanceurs d'alerte.

Source : http://www.zdnet.fr/actualites/vol-de-documents-via-google-la-condamnation-de-bluetouff-confirmee-39819710.htm

Renseignement : le Sénat apporte sa touche au texte | Le Net Expert Informatique

	Renseignement : le Sénat apporte sa touche au texte

Après un vote solennel à l'Assemblée, la commission des lois du Sénat s'est penchée sur le texte du projet de loi Renseignement. Les sénateurs se sont attachés à renforcer les contrôles et limiter certains points du texte.

Si à l'Assemblée, le texte de loi Renseignement était passé comme une lettre à la poste malgré les efforts de rares opposants, il semble que le Sénat ait choisi une approche plus prudente à l'égard de ce projet de loi qui suscite de nombreuses controverses, malgré un apparent consensus dans la majorité et l'opposition.

La commission des lois du Sénat a ainsi adopté pas moins de 145 amendements lors de l'examen du texte, qui avait lieu mercredi et jeudi. Ceux-ci concernent différents aspects du texte et visent, pour la plupart, à renforcer les contrôles et les garanties, sans pour autant changer en profondeur la portée du texte.

Ainsi, les amendements viennent remanier l'article concernant les fameuses boîtes noires, censées être déployées chez les opérateurs afin de procéder à une surveillance automatisée et anonyme du trafic, anonymat qui sera levé sur autorisation du Premier ministre afin d'identifier des individus suspectés de préparer des actes terroristes.

Le délai « d'autorisation des techniques particulières portant sur les données de connexion a été abaissé à deux mois » renouvelables sur autorisation du Premier ministre, contre quatre mois dans la précédente version.

Le Sénat balise le texte

Le Sénat s'est également attaché à limiter l'ampleur de la collecte mise en place grâce à cette technique, en la limitant aux seules métadonnées ainsi qu'en supprimant l'application de la procédure d'urgence. Le gouvernement jugeait le recours à cette procédure « indispensable » mais le Sénat ne semble pas convaincu et recommande donc de s'en tenir au circuit normal, qui comprend l'autorisation par le Premier ministre et un avis de la CNCTR avant le déploiement de ces mesures.

Le Sénat a également renforcé les options de contrôle de la CNCTR : les sénateurs ont clarifié les règles de nomination et de fonctionnement de cette nouvelle commission de contrôle, facilité la possibilité de saisir le Conseil d'État ainsi que les recours à la disposition de la commission lorsque celle-ci découvre la mise en œuvre d'une technique de renseignement qui lui aurait été dissimulé.

Une version remaniée du texte donc, qui apporte de nouvelles garanties à l'égard des mesures détaillées dans ce texte de loi. Le projet doit encore recevoir l'approbation du Senat en séance plénière, à partir du 4 juin. Après cette date, la commission mixte paritaire sera chargée de trouver un texte conciliant les deux versions. Puis interviendra la saisine du Conseil Constitutionnel avant la promulgation du texte par le président de la République.

Source : http://www.zdnet.fr/actualites/renseignement-le-senat-apporte-sa-touche-au-texte-39819704.htm
Par Louis Adam

Alerte : Des millions de routeurs domestiques peuvent être attaqués à distance | Le Net Expert Informatique

Une faille dans le driver NetUSB permet à un pirate de prendre le contrôle total de l'équipement et d'y installer, par exemple, des malwares. Pour l'instant, seul TP-Link a fourni un correctif.

Netgear, TP-Link, Trendnet, Zyxel… Si vous possédez un routeur domestique de l'une de ces marques, il est probable que vous ayez un problème de sécurité. La plupart de ces routeurs disposent en effet d'une fonctionnalité théoriquement assez pratique, à savoir le partage en réseau d'une connexion USB. Concrètement, vous connectez un équipement en USB sur votre routeur – un disque dur par exemple – et celui-ci devient alors accessible à distance au travers du réseau. Beaucoup de ces routeurs s'appuient pour cela sur un module logiciel nommé « NetUSB », développé par le fournisseur taiwanais KCodes.
Le problème, c'est qu'il existe dans ce module une faille qui permet à une personne mal intentionnée de faire crasher le routeur ou d'y exécuter n'importe quel code. Et donc d'en prendre possession pour, par exemple, y installer des malwares. Cette vulnérabilité a été découverte par les chercheurs en sécurité de la société autrichienne SEC Consult. Elle repose sur une erreur de codage : quand le nom de l'ordinateur qui souhaite se connecter à distance est supérieur à 64 caractères, le module NetUSB génère un dépassement de mémoire tampon et le fait planter. Pire : comme ce module est exécuté au niveau du noyau Linux du routeur, cette faille permet d'accéder au plus haut niveau de privilège. Plutôt pratique pour un pirate.

Exemple de routeur vulnérable.

Attaque par Internet
Certains d'entre vous se diront que ce n'est pas si grave que cela, car il faut déjà pouvoir rentrer dans le réseau domestique pour réaliser cette attaque. Mais cela n'est pas toujours vrai. Les chercheurs de SEC Consult ont trouvé que pour un certain nombre de routeurs, les connexions NetUSB étaient accessibles par Internet, peut-être en raison d'une mauvaise configuration. Par ailleurs, il s'avère que la procédure d'authentification utilisée pour initier une connexion avec NetUSB est totalement inutile : « les clés AES sont statiques et peuvent être trouvées dans le driver », expliquent les chercheurs. En d'autres termes, lorsque le routeur expose sa fonctionnalité NetUSB sur le web, un pirate pourra s'y introduire sans problème.
Une rapide recherche a montré qu'au moins 26 fabricants de routeurs utilisent le logiciel de KCodes dans au moins 92 produits. Ce qui représente certainement plusieurs millions de clients dans le monde. Contacté par les SEC Consult, KCodes n'a fait aucun commentaire. Que faut-il faire pour se protéger ? Seul TP-Link a développé, à ce jour, un correctif qu'il diffusera progressivement dans ses différents modèles. Dans certains équipements, il est possible, par ailleurs, de désactiver le partage de connexion USB. Les clients de Netgear, en revanche, ne pourront rien faire. Le fabricant a indiqué d'emblée ne pas pouvoir produire de patch, et qu'il était impossible de désactiver la fonction de partage. Il ne reste alors qu'une seule solution : la prière.

Source : http://www.01net.com/editorial/655187/des-millions-de-routeurs-domestiques-peuvent-etre-attaques-a-distance/

Hycopter : Le Supercopter des drones ? | Le Net Expert Informatique

	Hycopter : Le Supercopter des drones ?

Actuellement, les meilleurs drones multirotor ont une autonomie qui ne dépasse pas la demi-heure. Si cela n'est pas vraiment gênant pour les modèles grand public destinés aux loisirs, cette limite est un vrai handicap pour les applications professionnelles. Les opérateurs qui filment avec des drones doivent passer plus de temps sur le terrain pour accomplir leur mission et investir dans des jeux de batteries pour pouvoir décoller à nouveau sans délai.
Augmenter l'autonomie de ces engins est un casse-tête car la puissance des batteries est corrélée à leur taille et à leur poids. Mais Horizon Energy Systems (HES), une entreprise basée à Singapour spécialisée dans les piles à combustible et les systèmes d'alimentation hybrides, pense avoir trouvé la solution.

Elle a développé un drone quadricoptère nommé Hycopter qui pourrait voler jusqu'à quatre heures d'affilée grâce à une pile à combustible. L'originalité du concept est qu'HES est parvenu à intégrer sa technologie dans le châssis du drone. « Nous nous sommes rendu compte que la structure de ces drones était creuse et avons pu utiliser cet espace vide en le remplissant avec un gaz d'hydrogène », explique un des ingénieurs en charge du projet. Ainsi, le châssis tubulaire de l'Hycopter est rempli avec 120 grammes de gaz hydrogène pressurisé à 350 bars. Le gaz est transformé en électricité via une pile à combustible hybride lithium polymère. Le drone complet pèse 5 kilogrammes. Il peut emporter une charge supplémentaire d'un kilogramme, mais alors son autonomie passerait de quatre à un peu moins de deux heures.
Horizon Energy Systems a eu l'idée d'exploiter la structure du drone pour y intégrer son système d'alimentation. Ainsi, les deux parties tubulaires centrales du châssis sont remplies d'un gaz d'hydrogène pressurisé qui est converti en électricité par la pile à combustible lithium polymère (Ultra-light HES Fuel Cell, sur le schéma). Le drone peut emporter une charge d'un kilogramme qui peut être déplacée le long du châssis pour répartir le poids (Flexible positioning of payload). © Horizon Energy Systems

Le premier vol d'essai prévu cette année
Sur la maquette de démonstration présentée à la presse, les tubes du châssis destinés au stockage du gaz d'hydrogène sont en acrylique transparent mais, sur le prototype fonctionnel, ils seront en carbone de 5 millimètres d'épaisseur. Horizon Energy Systems dit être en train de finaliser la conception de son appareil et compte mener les premiers vols d'essai dans le courant de l'année. La viabilité du concept n'est donc pas encore démontrée. Mais l'entreprise, visiblement sûr d'elle, accepte les précommandes, sans toutefois communiquer sur le prix de l'Hycopter. L'engin est destiné à un usage professionnel : cartographie à grande échelle, surveillance des frontières ou d'infrastructures critiques, inspections de bâtiments…
L'autre application citée par HES concerne les futurs drones livreurs qui, grâce à une telle autonomie, pourraient bénéficier d'un rayon d'action beaucoup plus important. Une innovation qui pourrait bien intéresser Amazon, qui compte se servir de drones pour livrer certaines commandes peu volumineuses. Le géant du e-commerce a récemment obtenu un brevet pour un système de guidage grâce auquel le drone pourrait livrer le client là où il se trouve en temps réel, en le suivant grâce à son smartphone.


Ce drone quadricoptère nommé Hycopter est alimenté par une pile à combustible qui lui confère une autonomie de vol théorique de quatre heures. Le prototype est en cours de développement. Un premier vol d'essai est prévu cette année. © Horizon Energy Systems

---

Source :
http://www.futura-sciences.com/magazines/high-tech/infos/actu/d/drone-hycopter-drone-hydrogene-devrait-battre-record-autonomie-58320/
Par Marc Zaffagni, Futura-Sciences

Denis JACOPINI questionné par un journaliste de l’Express | Le Net Expert Informatique

	Denis JACOPINI questionné par un journaliste de l’Express

Le site d'actualité de jeux vidéo Nintendojo.fr a faussement annoncé mercredi 1er avril avoir été bloqué par le ministère de l'Intérieur. Une blague douteuse qui, par l'absurde, révèle néanmoins certains écueils de la loi Cazeneuve. Explications.

Voici l'écran qui s'affiche ce mercredi lorsque l'on tente de se connecter au site Nintendojo.fr

Ministère de l'Intérieur

Enfin, les détracteurs de la loi Cazeneuve tiennent leur martyr! Jugez donc: Nintendojo.fr, un simple site consacré à l'actualité des jeux Nintendo, est inaccessible ce mercredi. Il renvoie vers une page du ministère de l'Intérieur qui explique que le contenu a été bloqué. Une mesure qui est autorisée depuis le vote de la loi Cazeneuve fin 2014, avec de premiers cas en mars dernier, mais en principe réservée aux sites terroristes ou pédophiles.

Rassurez-vous tout de suite. « Il s'agit d'une blague de mauvais goût et ça nous a bien fait rigoler », explique à L'Express Mortal, l'administrateur du site. Il ne faut donc pas voir la main du ministère de l'Intérieur derrière ce faux blocage, mais un poisson d'avril qui aura trompé des dizaines d'internautes et quelques sites d'information.

Pourquoi ce gag?

« Ce n'est pas un geste politique, mais nous estimons quand même que la loi qui permet le blocage de certains sites internet est mauvaise, justifie Mortal, qui se revendique de la Quadrature du Net, association de défense des libertés sur internet hostile au dispositif. On avait envie de piquer les gens pour que ça éveille un peu les consciences sur le sujet. Cela pourrait arriver pour de vrai à d'autres demain, c'est ça le problème », tranche-t-il.

De la difficulté de distinguer « vrai » et « faux » blocage

Qu'on le juge drôle ou pas, le poisson d'avril de Nintendojo.fr pose de sérieuses questions sur le principe même de bloquer certains sites Internet. Est-il possible pour un internaute face à une page qui affiche le fameux message du ministère de l'Intérieur de savoir avec certitude que le site a été bloqué? « La réponse est simple: c'est non », estime **Denis Jacopini**, consultant en cybersécurité. Point de vue partagé par plusieurs observateurs interrogés ce mercredi.

« **Rien est impossible, poursuit l'analyste. Cela peut être un vrai message, bien sûr. Mais cela peut aussi être une blague de l'administrateur du site, ou l'oeuvre d'un hacker qui a modifié le site**« , avance-t-il.

Qu'en pense l'Intérieur? Contactés par L'Express, les services du ministère n'ont pas donné suite à nos sollicitations. A ce jour, les services de la Place Beauvau n'ont pas mis en place de dispositif pour informer sur de telles situations. Il ne serait pas étonnant, dans ce contexte, de voir fleurir les farces voire de réelles arnaques du même tonneau dans les semaines qui viennent.

Attention, arnaques à prévoir…

Dans le cas de Nintendojo.fr, l'artifice était plutôt élaboré. Le message affiché sur la page d'accueil du site reprenait, aussi bien graphiquement qu'au niveau du contenu, celui affiché en cas de blocage. Ce n'est pas tout. Un utilisateur de Twitter a comparé le code HTML de la page vers laquelle redirigeait Nintendojo.fr avec celui d'une page affichée via un site réellement bloqué par l'Intérieur, et ils étaient bien identiques.

Mais Nintendojo.fr est allé encore plus loin. « Nous avons vraiment procédé à un blocage DNS » (domain name system, nom de domaine) explique Mortal. Ce qui a pu donner l'illusion a certains que le site avait bel et bien été « bloqué ». « Techniquement, le dispositif de censure fait appel à un résolveur DNS menteur, c'est-à-dire qu'il ne renvoie pas le résultat correct, mais un mensonge tel que demandé par le gouvernement », explique nextinpact.com.

Concrètement, le gouvernement n'efface pas les sites bloqués: l'internaute qui essaye de s'y connecter est simplement redirigé vers la fameuse page ministérielle. Un mécanisme que Nintendojo.fr a plutôt bien singé ce mercredi.

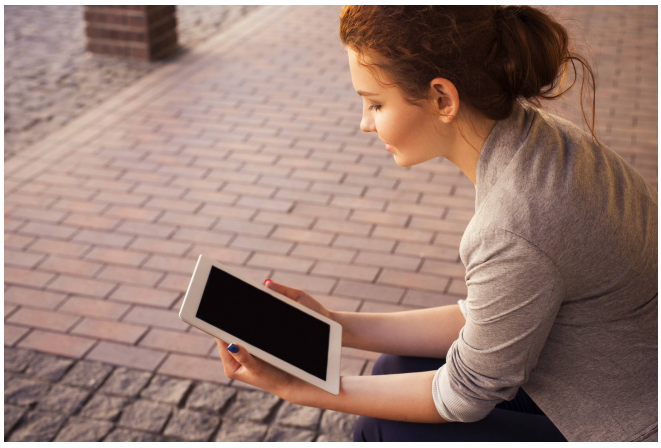
« On aurait pu faire encore plus sophistiqué »

Les bons connaisseurs, eux, ont néanmoins pu déjouer la supercherie en testant d'autres DNS. Ils ont alors observé que tous renvoyaient vers la page du ministère de l'Intérieur, ce qui n'aurait pas été le cas pour un « vrai » blocage gouvernemental. En situation réelle, les fournisseurs d'accès à Internet (FAI) bloquent le site concerné au fur et à mesure, ce qui prend du temps. De plus, il existe des DNS publics, gérés par d'autres acteurs du Web (par exemple, Google), qui peuvent ne pas faire l'objet de blocage. Changer de résolveur DNS est d'ailleurs précisément l'une des solutions pour ceux qui souhaitent contourner la censure.

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

Source : http://lexpansion.lexpress.fr/high-tech/les-vraies-questions-que-pose-le-faux-blocage-de-nintendojo-par-le-gouvernement_1667195.html

Mouchards sur les ebooks : Big brother is reading you ! | Le Net Expert Informatique

	Mouchards sur les ebooks : Big brother is reading you !

Grâce aux « mouchards numériques », il est désormais possible de savoir si un livre a été lu jusqu'au bout. Amazon, Apple, Google et Kobo en savent beaucoup plus sur vos habitudes de lecture que vous ne le pensiez…

Eric Zemmour a vendu plus de 400 000 exemplaires de son essai « Le suicide français ». Mais seulement 7,3 % des lecteurs l'ont lu jusqu'à la fin ! L'économiste Thomas Piketty fait un peu mieux : 9,7 % des lecteurs ont terminé son pavé de près de 1 000 pages (Le capital au XXI ème siècle). Encore mieux, le dernier roman de Patrick Modiano, Prix Nobel 2014 (Pour que tu ne te perdes pas dans le quartier) affiche un honorable taux de 44 %. Quant à Valérie Trierweiller (Merci pour ce moment), son score d'achèvement est, de loin, le meilleur : environ 66 % des lecteurs sont allés au terme des mésaventures sentimentales de l'ex compagne de François Hollande.
Comment connaît-on ces taux de lecture avec une telle précision ? Tout simplement grâce aux « mouchards » numériques installés sur nos liseuses et nos tablettes. Ces instruments dédiés à la traçabilité permettent en effet de collecter une série de données sur le comportement des e-lecteurs : nombre de pages lues, vitesse de lecture, temps passé sur une page, heures de lecture, surlignage…
Ces chiffres proviennent des statistiques collectées par Kobo (partenaire de la Fnac) l'un des leaders de la lecture numérique dans le monde. Autant dire qu'ils ne sont pas passés inaperçus, notamment auprès des lecteurs les plus attentifs aux questions de confidentialité des données. Mais il faut reconnaître à Kobo une qualité : il dit ce qu'il fait. L'un de ses responsables, Nathan Maharaj, a publiquement présenté ce dispositif de mesure de « l'engagement du lecteur » lors du salon du Livre de Francfort qui s'est tenu au mois d'octobre dernier. Selon Kobo, ces données ne seraient exploitées qu'à des fins statistiques ; surtout, elles seraient anonymisées et non rattachées à un compte lecteur. En revanche, elles sont revendues aux éditeurs qui peuvent ainsi accéder à des données inédites sur le comportement réel des lecteurs.
Lire la suite….

Source : http://www.archimag.com/bibliotheque-edition/2015/05/22/mouchards-ebooks-big-brother-reading-you

L’impression 3D de la peau humaine est presque une réalité | Le Net Expert Informatique

	L’impression 3D de la peau humaine est presque une réalité

L'Oréal, géant de la cosmétique, s'associe avec Organovo, une entreprise de bio-impression 3D cotée en bourse. Cette nouvelle technologie allie l'impression 3D et des tissus vivants dans le but d'imprimer de la peau humaine.
Dans son annonce de ce projet de collaboration, L'Oréal a utilisé un terme propre à la Silicon Valley en le présentant comme une technologie dite "de rupture". Aujourd'hui, toutes les grandes sociétés sont des incubateurs d'entreprises technologiques.

(Source)
Guive Balooch, directeur de l'Incubateur de la beauté connectée à L'Oréal, a déclaré : "Nous avons développé notre incubateur de technologie pour dévoiler des innovations de rupture à travers les industries ayant le potentiel de transformer le marché de la beauté". L'Oréal ajoute :
Notre partenariat ne va pas seulement créer de nouvelles méthodes de pointe in vitro pour évaluer la sécurité et la performance du produit. Le potentiel de ce nouveau secteur de technologie et de recherche est sans limites.

Des "tissus humains vivants" au service de la beauté
Comme l'a souligné L'Oréal, les méthodes de bio-impression 3D d'Organovo permettent l'automatisation et la reproductibilité de la "création" de "tissus humains vivants" qui pourraient "imiter la forme et la fonction des tissus originels du corps."

Dans la vidéo ci-dessous, Organovo explique (en anglais) comment cette peau est produite :

Keith Murphy, le PDG d'Organovo, décrit "ce partenariat [comme] une nouvelle étape considérable pour l'extension des fonctions des technologies de ."
En parlant de "modélisation de la peau", L'Oréal tente de créer un nouveau marché. L'avenir nous dira si cette technologie s'appliquera au niveau de la chirurgie réparatrice, et éventuellement soigner les grands brûlés.

Une innovation pour la santé et la recherche
Bien que L'Oréal investisse dans cette nouvelle technologie, son utilisation première est pharmaceutique. Dans un article paru dans Le Monde, Fabien Guillemot, chercheur à l'Inserm, énumère les usages possibles de ces tissus humains créés par bio-impression : "Ce procédé permet de reproduire la physiologie de tissus humains afin de tester de manière plus prédictive des molécules, ingrédients et candidats médicaments." De quoi réduire considérablement l'expérimentation animale.
Ainsi, la bio-impression pourrait également permettre le développement de la médecine individualisée, de produire des greffons et d'en finir avec les problèmes de rejet car la peau en question est réalisée à partir des cellules mêmes du patient. La bio-impression permettrait aussi d'accélérer la recherche contre le cancer.

Un marché en expansion
Ces nouvelles technologies représentent des enjeux socio-économiques majeurs qui affolent les investisseurs. Selon une étude du MedMarket Diligence relayée par Le Monde, le marché de l'ingénierie tissulaire était évalué à 15 milliards de dollars en 2014 et devrait doubler d'ici 2018. Ses utilisations multiples et limitations jusqu'à présent indéfinies suscitent de grandes attentes.
En janvier 2014, Organovo avait déjà imprimé un bout de foie produisant de l'albumine et capable de synthétiser le cholestérol. Cependant, l'impression totale d'organes, leur commercialisation et leur utilisation n'est pas prête de devenir monnaie courante dans les hôpitaux. De plus, la création et la commercialisation de tissus humains reste un marché éthiquement discutable.

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : http://www.konbini.com/fr/tendances-2/impression-3d-peau-humaine/
Article co-écrit et traduit par Marie Fabre