The European Data Governance Forum – CNIL

European Data Governance Forum – CNIL

Le G29 et la CNIL organisaient le 8 décembre une conférence internationale qui se tenait à l'UNESCO. La conférence avait pour thème : Protection des données, innovation et surveillance : quel cadre éthique pour l'Europe ?

2015 est une année charnière pour la protection de la vie privée, avec l'adoption du règlement de l'Union Européenne sur la protection des données, la poursuite des négociations commerciales internationales et les décisions finales à prendre sur la gouvernance de l'internet. Cette période est cruciale pour l'Europe qui, dans le nouvel environnement numérique, doit promouvoir haut et fort les valeurs sociétales qui sont les siennes et définir des actions prioritaires pour le futur.
Une réponse d'ensemble à ces défis internationaux ne saurait être élaborée par des acteurs agissant en ordre dispersé. La complexité des problèmes posés demande une réflexion collective de la part de l'ensemble des parties prenantes.
La conférence du 8 décembre organisée par le G29 (groupe des autorités européennes de protection des données) et la CNIL était placée sous le patronage de l'UNESCO et de la Délégation permanente française auprès de l'UNESCO. Elle réunssait des représentants et experts d'horizons divers – institutions nationales, européennes et internationales, industrie, ONG et société civile – qui ont présenté leur point de vue sur les défis actuels de la surveillance numérique et sur la manière d'y répondre de manière adéquate dans une société démocratique.
La conférence s'est achevée par la présentation d'une Déclaration adoptée par le G29 qui était endossable par les parties prenantes qui le souhaitaient. Cette Déclaration soulignait la responsabilité collective de toutes les parties prenantes dans la définition et le respect d'un cadre éthique pour la collecte et l'utilisation de données personnelles dans l'économie numérique. Elle a défini les principes essentiels à inclure dans un tel cadre ainsi que les actions clés à entreprendre par toutes les parties prenantes, des secteurs public et privé, pour garantir le respect des règles.

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

Source : http://www.newspress.fr/Communique_FR_284395_1332.aspx

ESET s’engage auprès de Facebook pour protéger les utilisateurs des cyber-menaces

	ESET s’engage auprès de Facebook pour protéger les utilisateurs des cyber-menaces

ESET protège tous les utilisateurs Facebook contre le piratage.
ESET rejoint l'initiative Anti-malware lancé par Facebook et offre « ESET Online Scanner » à tous les utilisateurs de Facebook. Cette solution permet d'identifier les posts provenant non pas des utilisateurs mais de logiciels malveillants. Ces posts sont alors retirés en toute sécurité. ESET Online Scanner pour Facebook est disponible depuis le 03 décembre 2014 et pour tous les utilisateurs de Facebook.

« Notre but est d'offrir à nos utilisateurs la meilleure technologie afin d'améliorer l'utilisation de nos services et de protéger au mieux leurs appareils connectés. ESET Online Scanner va de manière significative diminuer le nombre de clics sur des liens malicieux, effectués des milliards de fois chaque jour sur Facebook » explique Chetan Gowda, Web developer chez Facebook.

La version dédiée d'ESET Online Scanner pour Facebook, a été conçue pour détecter et nettoyer les ordinateurs infectés des utilisateurs de Facebook. « ESET est heureux d'offrir ses services aux utilisateurs de Facebook du monde entier. ESET est reconnu pour sa légèreté et sa qualité de détection, ces deux atouts se retrouvent dans cette version pour Facebook, gratuitement.», annonce Ignacio Sbampato, Directeur Commercial et Marketing chez ESET HQ.

Votre ordinateur a besoin d'être nettoyéSuppression des logiciels malveillants Un fonctionnement simple et ciblé
Lorsqu'un utilisateur se connecte à son compte, Facebook cherche des comportements malicieux – comme l'envoi de spams ou de liens infectés provenant d'amis Facebook. Si ce type d'activité est détecté, Facebook invite l'utilisateur à utiliser ESET Online Scanner. L'analyse s'effectue directement sur Facebook, gratuitement et en tâche de fond.

L'utilisation du scanner est sans impact sur le système de l'utilisateur, de sorte qu'il peut continuer à utiliser son appareil sans gêne. Une fois l'analyse terminée, l'utilisateur reçoit une notification de la part de Facebook; un compte rendu du scan est aussi disponible. Le nettoyage commence une fois l'analyse terminée si des malwares ont été détectés.

Ce service pour Facebook est basé sur une solution gratuite ESET Online Scanner protégeant des millions d'internautes. Sur plus de 44 millions de scans, ESET Online Scanner a détecté avec succès des malwares dans presque la moitié des analyses.

ESET est un outil de protection et de désinfection que je conseille personnellement.
Vous avez envie de découvrir et de tester gratuitement ce logiciel de protection (ESET NOD32 ou ESET SMART SECURITY, je peux vous communiquer une licence sur simple demande.
Denis JACOPINI

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

Source : https://mail.google.com/mail/u/0/?hl=fr&shva=1#inbox/14a2e1044c5865c4

La justice européenne va encadrer la vidéosurveillance depuis le domicile – Next INpact

La justice européenne va encadrer la vidéosurveillance depuis le domicile – Next INpact

Jeudi, la Cour de Justice de l'Union dira si une caméra située dans une propriété privée qui surveille également une partie de l'espace public échappe ou non aux règles de protection en matière de traitement des données à caractère personnel.

Le déploiement des solutions de vidéosurveillance personnelles se démocratisant, une affaire tranchée demain par la Cour de Justice de l'Union européenne méritera une certaine attention. Le cas examiné est né en Tchécoslovaquie.

Un certain M. Ryneš, agacé que les vitres de sa maison soient brisées à maintes reprises avait installé un système de vidéosurveillance. Les flux étaient enregistrés sur disque dur à partir de caméras captant l'entrée de sa maison, celle de la maison d'en face, mais également une partie de la voie publique.

Une amende infligée par la CNIL tchèque

Dans la nuit du 6 au 7 octobre 2007, nouveau vandalisme à l'aide d'une fronde. Les enregistrements sont remis à la police qui parvient à identifier des suspects. Problème, l'un d'eux conteste la légalité des procédures auprès de l'Office tchèque pour la protection des données à caractère personnel. Et pour cause : ces enregistrements ont été effectués sans son consentement alors qu'il était sur la voie publique.
La CNIL locale lui donne raison et inflige une amende à M. Ryneš. Ce dernier attaque cependant cette décision devant la Cour suprême administrative tchèque, laquelle, prise d'un doute, a saisi la Cour de justice pour savoir si ces enregistrements constituaient ou non un traitement de données couvert par la directive 95/46 sur les données personnelles. Celle-ci en effet, ne s'applique pas quand le traitement est effectué par une personne physique pour l'exercice d'activités exclusivement personnelles ou domestiques.

L'analyse de l'avocat général

Pour l'heure, l'avocat général a déjà conclu que le traitement de données à caractère personnel effectué par ce Tchèque ne relevait pas de la notion d' « exercice d'activités exclusivement personnelles ou domestiques », une des exceptions à la directive en question. Du coup, a contrario, ce système de vidéosurveillance devrait entrer dans le plein champ de ce texte européen.
Si la Cour suit cette analyse, cela ne signifiera pas nécessairement que l'amende infligée au responsable du traitement sera légitimée. Il faudra en effet déterminer si d'autres articles de cette directive ne peuvent être appelés en renfort pour légitimer cette installation effectuée sans le consentement des personnes filmées (article 7 f) de la directive).

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

Source : http://www.nextinpact.com/news/91283-la-justice-europeenne-va-encadrer-videosurveillance-depuis-domicile.htm

---

Fête des lumières 2014 de Lyon : les coulisses high-tech de la Place des Terreaux

!

Fête des lumières 2014 de Lyon : les coulisses high-tech de la Place des Terreaux !

Chaque année, la fête des Lumières revient illuminer la ville de Lyon. L'installation de la place des Terreaux est assurément l'une des plus impressionnantes de ce cru 2014. Dans la pratique, des vidéos haute résolution sont projetées sur les façades de la mairie de Lyon ainsi que sur le musée des beaux-arts (les deux bâtiments sont situés autour de la place des Terreaux).

‘

La couverture de la mairie est assurée par 5 projecteurs professionnels Barco de 26 000 lumens d'une résolution de 1920 x 1200 pixels. Pour le musée, les techniciens ont dû utiliser 6 projecteurs du même type. Dans cette configuration, chaque projecteur recouvre une surface d'environ 35 m².
L'alimentation des projecteurs en image est assurée par des serveurs média de type Modulo Pi. Ces derniers sont taillés sur mesure pour délivrer des contenus audio et vidéo HD ou 4K sans le moindre accroc. Côté hardware, ils sont équipés d'un processeur de type Core i7 épaulé par 16 Go de RAM, et d'une carte graphique de type AMD Fire Pro W7000. Les fichiers vidéo sont stockés dans 8 SSD en Raid. Le serveur tourne sous Windows Embedded Standard 7, et exécute le programme serveur de modulo Pi. Une seule machine est capable de distribuer 4 flux vidéo non compressés (progressifs, sans codecs, suite d'images TGA) en 1920 x 1200 pixels, ou un seul flux 4K 120 hertz non compressé.
Les serveurs Modulo Pi sont tous mis en réseau de manière à assurer une diffusion audio / vidéo parfaitement synchronisée. Ils sont également capables de piloter les projecteurs, et corrigent la déformation lorsque l'image n'est pas projetée sur une surface plane. Détail intéressant : si les serveurs Modulo Pi sont pilotables depuis un ordinateur sous Windows ou Mac OSX, une nouvelle application Android (encore en version bêta) fait désormais son apparition.

En clair, il est possible de piloter l'ensemble de ces projections gigantesques depuis un « simple » téléphone portable !

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

Source :
http://www.clubic.com/video/reportages/video-fete-des-lumieres-2014-de-lyon-les-coulisses-high-tech-de-la-place-des-terreaux-458881.html

---

La protection des données personnelles, « atout pour la France », selon Manuel Valls

La protection des données personnelles, « atout pour la France », selon Manuel Valls

« Je mesure l'audace d'inviter un ancien ministre de l'intérieur parler de protection des données, cela peut paraître risqué » : surprise, c'est le premier ministre, Manuel Valls, qui a prononcé le discours d'ouverture de l'« European data governance forum », organisé lundi 8 décembre à Paris.

Cette journée de conférence au siège de l'Unesco a été mise en place par le G29, qui rassemble les autorités européennes de protection des données, afin de réfléchir à un « cadre éthique et juridique » sur la question des données personnelles.

Le chef du gouvernement a souligné à plusieurs reprises le rôle que doivent jouer, selon lui, les autorités européennes et les Etats : « Il serait erroné de penser que toute régulation tue l'innovation. La régulation, c'est le rôle des Etats. Les valeurs de la démocratie doivent peser sur le monde numérique, la loi doit s'y appliquer. »

Projet de loi sur le numérique

« En 2015 et 2016, la loi réaffirmera de manière solennelle le droit à la vie privée et à la protection des données personnelles, ainsi que le contrôle des actes des services de renseignement », a expliqué le premier ministre. Sans préciser si cette question sera abordée dans le cadre du projet de loi numérique, en 2015, ou s'il fera l'objet d'un texte distinct.

Manuel Valls et Mme Falque-Pierrotin, la présidente de la CNIL, ont également rappelé que 2015 serait l'année du règlement sur les données personnelles, adopté au printemps par le parlement européen et qui doit désormais faire l'objet d'un accord entre les Etats membres. Sur ce sujet, le premier ministre a souligné « le soutien de la France à la réflexion sur le règlement sur les données », tandis que Mme Falque-Pierrotin a estimé qu'il y avait « urgence à nous doter de cet instrument juridique unique pour toute l'Union ».

Sur la question très sensible de l'inclusion – ou non – de la lucrative question des données personnelles dans les négociations sur les traités de libre-échange actuellement en négociation notamment entre l'UE et les Etats-Unis, M. Valls s'est voulu rassurant : « La France veillera, dans les négociations sur les traités de libre-échange, à ce que le standard européen soit préservé. »

« DÉFICIT DE CONFIANCE »

Le gouvernement français en est convaincu, a martelé Manuel Valls : la protection des données est un atout économique. « L'Europe doit faire de la protection des données personnelles un argument d'attractivité et de compétitivité. L'utilisateur doit pouvoir faire ses choix sur ses propres données en toute connaissance. Cela a un potentiel économique énorme. »

Un avis partagé par Mme Falque-Pierrotin : « Il ne faut pas que le déficit de confiance se transforme en méfiance » générale au sein de l'écosystème numérique. « Le monde a changé. Certains voudraient faire croire que la vieille histoire de la protection des données est dépassée », a conclu Manuel Valls. « Chaque époque a son combat : le droit des femmes, l'abolition de la peine de mort… La France y a tenu sa place. C'est parce que la France est le pays des droits de l'homme qu'elle doit faire de la protection des données un grand combat pour les droits humains. »

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

Source : http://www.lemonde.fr/pixels/article/2014/12/08/la-protection-des-donnees-personnelles-atout-pour-la-france-selon-manuel-valls_4536408_4408996.html par Martin Untersinger

---

L'intelligence artificielle, notre futur Terminator?

L’intelligence artificielle, notre futur Terminator?

L’intelligence artificielle pourrait menacer à terme l’Humanité: il ne s’agit pas d’un film de science-fiction mais de la prédiction du célèbre physicien Stephen Hawking, qui relance le débat sur le risque de voir l’homme dépassé par les technologies qu’il a lui-même créées.

Interrogés par l’AFP, anthropologue, futurologues et experts en intelligence artificielle se montrent partagés sur les craintes d’Hawking.
Les craintes d’un homme apprenti sorcier sont anciennes et elles ont nourri nombre de romans et des films comme « 2001: Odyssée de l’espace » avec son ordinateur meurtrier Hal 9000 et plus récemment « Terminator », le robot exterminateur.
Mais aujourd’hui, c’est un astrophysicien très respecté, le Britannique Stephen Hawking, qui lance un pavé dans la mare. Atteint d’une dystrophie neuromusculaire, il s’exprime grâce à un ordinateur.
« Les formes primitives d’intelligence artificielle que nous avons déjà se sont montrées très utiles », reconnaît-il. « Mais je pense que le développement d’une intelligence artificielle complète pourrait mettre fin à la race humaine », a-t-il déclaré cette semaine à la BBC.
Déjà, le milliardaire Elon Musk avait expliqué avoir investi dans des sociétés d’intelligence artificielle pour « garder un oeil » sur ce qui se passe dans ce domaine. « Nous devons nous assurer que les conséquences sont bonnes et non mauvaises », selon lui.
« Cela me fait plaisir qu’un scientifique des +Sciences dures+ dise cela. Je le dis depuis des années », déclare Daniela Cerqui, anthropologue à l’université de Lausanne.
« Nous déléguons à ces machines de plus en plus de prérogatives de l’humain, afin qu’elles soient plus performantes que nous. On va finir par devenir leur esclave », selon elle.
A l’inverse, Jean-Gabriel Ganascia, philosophe et expert en intelligence artificielle, juge « excessif » le « cri d’alarme » de Hawking.
« Le danger, c’est davantage l’homme qui se servirait de ces technologies pour asservir » d’autres humains, considère ce professeur à l’Université Pierre-et-Marie-Curie à Paris.
– Développer une intelligence artificielle « amicale »-
Nick Bostrom, futurologue à l’Université d’Oxford, pense que « la machine intelligente parviendra à dépasser l’intelligence biologique. Il y aura alors des risques existentiels associés à cette transition ».
« Les machines sont déjà plus fortes que nous. Je pense qu’elles finiront aussi par devenir plus intelligentes, même si ce n’est pas le cas actuellement », ajoute-t-il.
Au cours de ces dernières années, d’énormes progrès ont été réalisés dans le domaine de l’intelligence artificielle, en tant que capacité à traiter, à analyser des données et à répondre à des questions.
Mais on est « encore loin » de l’intelligence artificielle générale « complète », qui inquiète Stephen Hawking, souligne Anthony Cohn, professeur à l’université de Leeds (centre du Royaume-Uni). « Il faudra encore plusieurs décennies. »
Mathieu Lafourcade, spécialiste en intelligence artificielle et en traitement du langage à l’Université de Montpellier (sud de la France), juge « alarmiste » l’avertissement du physicien.
Mais il pense que « dans un futur hypothétique », il faudra peut être « s’en remettre » dans certains domaines aux machines car leurs capacités intellectuelles auront dépassé les nôtres. « La machine nous proposera une solution que nous ne serons pas à même de comprendre mais il faudra lui faire confiance », par exemple si elle nous recommande des mesures contre le réchauffement climatique, considère-t-il.
« Toutefois, si la machine débloque, il faudra se réserver la possibilité de la débrancher », souligne-t-il.
Stuart Armstrong, futurologue à l’université d’Oxford, relève que « les incertitudes sur le développement de l’intelligence artificielle sont extrêmes ».
« Le problème, c’est qu’il est extrêmement difficile de programmer des objectifs compatibles avec la dignité voire la survie de l’Humanité », dit-il.
« Il faudrait programmer presque toutes les valeurs humaines parfaitement dans l’ordinateur afin d’éviter que l’Intelligence artificielle n’interprète +éradique la maladie+ comme +tue tout le monde+ ou bien +garde les humains sains et saufs et contents+ comme +enterre tout le monde dans des bunkers avec de l’héroïne+ ».
« Il faut que les ingénieurs prennent ces problèmes au sérieux et trouvent des solutions pour développer une intelligence artificielle +amicale+, pleinement compatible avec les valeurs humaines », considère-t-il.

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

Source :
http://www.leparisien.fr/sciences/l-intelligence-artificielle-notre-futur-terminator-08-12-2014-4355179.php#xtref=https%3A%2F%2Fwww.google.fr%2F

Le PSN inaccessible suite à une attaque de Lizard Squad

Le PSN inaccessible suite à une attaque de Lizard Squad

Depuis quelques heures, le PlayStation Network de Sony est inaccessible pour de nombreux utilisateurs. Il s'agirait visiblement d'une nouvelle attaque DDOS, revendiquée par le groupe Lizard Squad.

Les problèmes touchent principalement l'Amérique du Nord, mais d'autres joueurs dans le monde ont remarqué quelques soucis depuis le milieu de la nuit.
PlayStation a rapidement tenu informé ses joueurs via Twitter, sans toutefois donner trop d'informations.
On ne sait donc pas vraiment quand seront réglés ces soucis, mais on sait au moins que les équipes de Sony travaillent à régler le problème, et c'est déjà une bonne nouvelle.
Le groupe Lizard Squad a revendiqué cette attaque, et c'est donc visiblement le serveur d'authentification de Sony qui est visé (comme l'indique ce tweet https://twitter.com/LizardPatrol/status/541751366297743360), perturbant ainsi grandement le PSN.
Espérons que tout rentrera dans l'ordre rapidement, puisque ces problèmes répétés risquent fortement d'agacer les joueurs.

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

Source : http://www.gameblog.fr/news/47390-le-psn-inaccessible-suite-a-une-attaque-de-lizard-squad

HTTPS : la sécurité pour tous, mais à quel prix ?

	**HTTPS : la sécurité pour tous, mais à quel prix ?**

Réseaux : Plusieurs chercheurs ont présenté lors des conférences ACM CoNext à Sidney le résultat de leurs recherches sur le coût et les implications du déploiement de HTTPS. Un gain de sécurité pour l'utilisateur mais un choix qui implique d'envisager les conséquences.

Face aux écoutes de la NSA, les principaux constructeurs et acteurs du numérique semblent au moins tous d'accord sur un point : il faut tout chiffrer. Non pas que cela vous sauvera immédiatement des grandes oreilles de la NSA, qui est peut être déjà arrivé à bout des algorithmes de chiffrement les plus pointus, mais cela aura au moins un mérite : celui d'augmenter le « coût de la surveillance » pour les importuns, compliquer la tache des Five Eyes afin de décourager l'espionnage à grande échelle de nos communication.

Quel est le prix du S dans HTTPS ?

Chacun y va donc de son petit chiffrement mais pour le web, en attendant un http/2 qui se fait désirer, la plupart des principaux sites web ont progressivement basculé au déploiement de HTTPS, une couche de chiffrement sécurisant les connexions web. Mais quel est le coût réel de cette sécurité ? C'est la question que se sont posée plusieurs chercheurs de l'université de Carnegie Mellon, de Telefonica ou de l'école polytechnique de Turin.

Déployer le HTTPS suppose tout d'abord des coûts financiers non négligeables à travers l'achat et le maintien de certificats : l'étude se base sur les tarifs de Symantec mais les offres dans le domaine sont extrêmement variables en fonction du prestataire et des services associés. Mais plus que la question financière, c'est celle des performances qui intéresse les chercheurs.

L'utilisation de HTTPS présente plusieurs désavantages : tout d'abord une augmentation, minime mais sensible, de la latence et du temps nécessaire au chargement d'une page. Si celle-ci varie beaucoup en fonction de nombreux facteurs, les chercheurs constatent néanmoins une augmentation du temps de réponse, parfois de plus de 300ms. Un cout de performance « pas si négligeable que cela », rappellent les auteurs de l'étude, qui rappellent que chaque seconde compte pour les internautes.

Un réseau opaque

Si l'impact sur la batterie est jugé mineur, le déploiement du HTTPS pourrait en revanche se retourner contre les opérateurs en compliquant l'utilisation de solutions reposant sur le Deep Packet Inspection. Certes, c'est plus ou moins le but initial puisque le Deep Packet Inspection est utilisée par des applications de surveillance, mais cette technologie permet également à un opérateur de lutter contre le spam ou les attaques ddos.

Le DPI a mauvaise presse et cela se comprend, mais si le déploiement du HTTPS se poursuit, comme le supposent les auteurs de l'étude, alors les opérateurs vont devoir envisager de nouvelles solutions pour lutter contre ces problèmes. Moins polémique mais peut être plus problématique encore : le HTTPS empêche par exemple les opérateurs et fournisseurs d'accès d'avoir recours à du caching pour épargner leur bande passante.

Pourtant, malgré les problèmes relevés par l'étude, les chercheurs restent confiant et s'attendent à voir HTTPS de plus en plus présent au cours des années à venir : « le S est là pour rester » concluent ils, et ce malgré les désavantages liés au chiffrement sur les connexions web. Reste donc à trouver un moyen de minimiser l'impact, peut être grâce à http/2, dont les premières spécifications sont attendues cette année.

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

Source : http://www.zdnet.fr/actualites/https-la-securite-pour-tous-mais-a-quel-prix-39810969.htm
Par Louis Adam

Que deviennent les données stockées sur nos objets connectés ?

Que deviennent les données stockées sur nos objets connectés ?

Une équipe de France 2 a enquêté sur ces objets connectés qui ont envahi notre quotidien et conservent nos données personnelles.

Chaque jour, 5 millions de Français prennent le pouls de leur santé à l'aide de leurs objets connectés qui engloutissent des informations sur leurs utilisateurs. Ces données sont envoyées via Internet sur un serveur stocké dans un lieu ultra-sécurisé, le data-center, constitué de millier d'ordinateurs. La protection de ces données dépend de la législation du pays où elles sont conservées. « Si vous avez de la chance, vos données atterriront en France dans un data-center comme celui-là, dans la réglementation française qui est très protectrice. Si vous n'avez pas de chances, elles atterriront aux États-Unis ou ailleurs », commente Arnaud de Bermingham, directeur des services d'hébergement Online.

Les internautes exposés à la publicité ciblée

Aux États-Unis, l'administration peut librement accéder à vos données personnelles sous couvert de sécurité nationale. En France, les fabricants d'objets connectés doivent obtenir le consentement des utilisateurs et garantir leur sécurité contre le piratage. Subsiste toutefois le risque de voir ses données vendues à des fins mercantiles. La loi interdit toutefois l'utilisation de ces données par la sécurité sociale ou les assurances.

La vidéo de FranceTV Info pour mieux comprendre le phénomène

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

Source : http://www.francetvinfo.fr/economie/medias/video-que-deviennent-les-donnees-stockees-sur-nos-objets-connectes_757247.html
Par France 2

SONY : Connexion impossible au PSN

SONY : Connexion impossible au PSN

Déjà responsable de la paralysie des serveurs du Xbox Live sur Xbox One et Xbox 360 dernièrement, le groupe de hacker Lizard Squad semble de nouveau être en train de complètement faire disjoncter le PSN, causant des messages de connexion impossible sur PS4, PS3 et PS Vita en ce lundi 8 décembre 2014. En effet, les joueurs se plaignent un peu partout de ne plus pouvoir jouer en ligne sur leur console PlayStation, et de ne plus avoir accès au PSN.

Il y a peu de temps, Lizard Squad avait annoncé une campagne visant à complètement mettre à terre les services online de Microsoft et Sony le jour de Noël 2014, et est déjà responsable de plusieurs épisodes de paralysie du PSN et du Xbox Live ces dernières semaines. Prendre en otage le PSN aujourd'hui même, alors que Sony est en pleine PlayStation Experience est-il un message d'avertissement aux deux constructeurs ? Difficile à dire, d'autant que rien n'est jamais demandé en retour. C'est alors les joueurs qui se retrouvent pénalisés avec des connexions impossible au PSN et Xbox Live. Cependant, dans l'ombre, Anonymous souhaite ne pas en rester là, et menace à son tour Lizard Squad dans une vidéo postée sur internet il y a deux jours, disponible ci-dessous.
Bien entendu, il est toujours assez délicat d'accorder de la légitimité aux nouvelles vidéos d'Anonymous, tant ce groupe est volatile, et peut être représenté par n'importe qui. Vont-ils essayer de voler dans les plumes d'un Lizard Squad qui multiplie les actions pour mettre à terre les services online de la PS4 et de la Xbox One régulièrement ? De son côté, Sony avoue être en ce moment même au travail pour rétablir les connexions à son PSN. Nous vous tiendrons bien entendu au courant de la situation, dans notre colonne d'actualité jeux vidéo, comme toujours.

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

Source : http://playerone.tv/news/v/6234/connexion-impossible-au-psn-lizard-squad-ddos-encore-les-services-playstation.html