Une nouvelle norme Wi-Fi destinée aux objets connectés

	**Une nouvelle norme Wi-Fi destinée aux objets connectés**

La Wi-Fi Alliance a présenté un nouveau standard baptisé Wifi Halow (ou IEEE 802.11ah pour les intimes.) Celui-ci est spécialement pensé pour le marché des objets connectés et promet une consommation énergétique moindre ainsi qu'une meilleure portée.

La Wi-Fi Alliance n'entend pas rester sur la touche sur le marché des objets connectés : l'organisme, qui rassemble les principaux acteurs et industriels spécialisés ayant recours aux technologies Wi-Fi, a annoncé l'arrivée d'un nouveau standard baptisé Halow. Celui-ci misera principalement sur deux aspects pour s'imposer sur les objets connectés : d'une part, la Wi-Fi Alliance met en avant une consommation énergétique réduite pour les machines ayant recours à Halow,. Basé sur la norme IEEE 802.11ah, Halow est encore en attente de validation.

Halow, it's me

Ce protocole fonctionne sur la bande de fréquence 900 Mhz et promet une portée maximale doublée par rapport aux protocoles actuellement utilisés. A titre de comparaison, la portée de la norme 802.11ac, déployée en 2011, est évaluée à environ 35m. Le Wi-Fi Halow promet également une meilleure robustesse du signal, afin d'assurer une meilleure connectivité au sein des environnements urbains ou domestiques. En revanche, celui-ci offrira un débit moindre, ce qui n'est pas forcement un défaut dans le secteur des objets connectés, qui cherchent plutôt à transmettre de petites quantités de données à intervalles fréquents.

Celui-ci sera également compatible avec les principaux protocoles Wi-Fi actuellement utilisés par les différents constructeurs et sera évidemment conçu pour prendre en charge nativement les connexions IP. Un processus de certification des objets exploitant ce nouveau protocole sera lancé d'ici 2018, mais les premiers produits ayant recours à Halow devraient être disponibles dès 2016.

Le marché des objets connectés reste pour l'instant chaotique, mais de nombreux compétiteurs tentent de mettre en avant leurs propres protocoles afin de prendre les devants sur la concurrence. L'objectif est de devenir un standard dans un secteur qui, plus que beaucoup d'autres, à un grave besoin d'interopérabilité. On a ainsi vu Sigfox présenter sa propre technologie, rapidement suivi par LoRa tandis qu'Archos ou d'autres développent eux aussi leurs propres alternatives.

Réagissez à cet article

Source : *Wi-Fi Halow : Une nouvelle norme destinée aux objets connectés*

Un malware soupçonné d’être à l’origine d’une coupure de courant en Ukraine

Un malware soupçonné d’être à l’origine d’une coupure de courant en Ukraine

Le 23 décembre, les habitants de la ville ukrainienne d'Ivano-Frankivsk ont subi une importante panne de courant. Celle-ci a été provoquée par une défaillance provenant de la centrale électrique régionale et a affecté plusieurs milliers de foyers de la région. Mais cette soudaine panne n'était pas un accident : en effet, la société chargée de l'exploitation de la centrale a précisé que celle-ci avait été causée par des « interférences » sur leurs systèmes.

Mais pour plusieurs médias locaux, la piste d'une cyberattaque visant les infrastructures énergétiques du pays est à privilégier. La société de cybersécurité ESET a d'ailleurs publié plusieurs informations en ce sens : la société explique avoir récupéré des samples de malware ayant affecté plusieurs centrales ukrainiennes, et explique que ceux-ci ont pu être utilisés dans le cadre d'une cyberattaque à l'encontre des équipements ukrainiens.

Des nouvelles du cyberfront

ESET se dit en mesure d'affirmer que plusieurs entreprises Ukrainiennes du secteur de l'énergie sont victimes de cyberattaques. Les attaquants ont notamment recours à une famille de malware baptisées BlackEnergy, dont les traces ont été détectées à plusieurs reprises en 2015 dans des entreprises ukrainiennes liées au secteur de l'énergie.
BlackEnergy est un malware connu, qui a déjà été repéré plusieurs fois par le passé. Celui-ci se présente sous la forme d'un malware modulaire : une fois la cible infectée, les attaquants peuvent exploiter la porte dérobée ainsi créée afin de télécharger des modules différents permettant au malware d'accomplir diverses actions sur la machine cible.
Parmi les modules identifiés de ce malware, l'un d'entre eux permet notamment de s'attaquer aux systèmes SCADA, des postes utilisés pour le contrôle et la surveillance des installations industrielles. BlackEnergy permet également le téléchargement d'un autre malware, baptisé cette fois killdisk, et dont l'objectif est la destruction de données. Un arsenal qui laisse ESET penser que ces outils ont pu être mis en œuvre dans l'attaque dont semble avoir été victime la centrale électrique d'Ivano-Franivsk.
Les services de sécurité ukrainiens accusent la Russie d'être à l'origine de l'attaque selon Reuters, mais ces derniers n'ont émis aucun commentaire venant confirmer ou infirmer cette théorie. Une enquête a été ouverte par les autorités nationales pour déterminer les circonstances exactes de cette coupure de courant.

Réagissez à cet article

Source : *Ukraine : un malware soupconné d'être à l'origine d'une coupure de courant*

Les 5 dangers pour vos ordinateurs, smartphones et données en 2016

Les 5 dangers pour vos ordinateurs, smartphones et données en 2016

Les 5 tendances qui motiveront leurs actions envers votre ordinateur, votre smartphone, vos données…

Ecartelée entre la démocratisation de l'Internet des objets (thermostat intelligent, balance connectée…), la prise de pouvoir du stockage dans le « cloud » et l'émergence des nouveaux smartphones vedettes, la sphère des nouvelles technologies subira en 2016 les assauts des virus virulents, des arnaques en ligne, des cybercriminels.
Comme un caméléon virtuel, la cybercriminalité s'adaptera plus que jamais à l'air du temps pour exploiter les nouveaux territoires en friche.
Entre prudence et clairvoyance, voici les 5 tendances cybercriminelles qui se développeront ces 12 prochains mois, selon les experts de l'éditeur de solution de sécurité BullGuard.

1. La montée en puissance du « ransomware »
Impitoyable méthode d'extorsion, le « ransomware » bloque votre ordinateur, crypte vos fichiers personnels et vous réclame un paiement en ligne pour les libérer.
La menace brandie en cas de refus de payer la rançon : l'extermination de vos données (photos, vidéos, documents…).
Alors que les virus à l'ancienne et les chevaux de Troie accusent une certaine perte de vitesse, le « ransomware » est appelé à les dribbler.
Ces logiciels malveillants s'attrapent en visitant un site préalablement « hacké » (piraté) ou un obscur site volontairement malveillant, en téléchargeant des fichiers vérolés, notamment sur les plateformes d'échange de fichiers illégaux…

2. Le smartphone, cette cible indiscrète
Connecté à Internet 7 jours sur 7, 24 heures sur 24 dans le scénario le plus extrême, le smartphone concentre une myriade de données personnelles, des adresses email de vos contacts au numéro de votre carte de crédit.
Le téléphone est par conséquent une cible de choix pour les cybercriminels, qui rivalisent d'ingéniosité pour contourner les nouvelles barrières de sécurité régulièrement déployées par Apple pour ses iPhone et Google pour son système d'exploitation mobile Google Play.
Après avoir concentré leurs efforts sur la Chine et l'Extrême-Orient, les cybercriminels devraient viser tout particulièrement l'Europe en 2016.
Certes, nos smartphones étaient déjà menacés par le virus et les logiciels malveillants. Hélas, le niveau d'alerte devrait grimper de quelques degrés.

3. L'Eldorado inquiétant de l'Internet des objets
Nouvelle marotte des constructeurs, l'Internet des objets entend envahir notre quotidien pour évaluer et prédire nos besoins, mesurer notre activité, adapter l'éclairage et le chauffage de notre habitation en fonction de nos usages…
Qu'il s'agisse d'un pèse-personne connecté ou d'un thermostat intelligent, ces appareils vulnérables de par leur connexion constante à Internet récoltent au kilo les données personnelles.
Imaginons le cas d'une caméra de sécurité connectée. Elle pourrait simplement être détournée par un cybercriminel pour détecter les moments où vous quittez votre maison.
Toujours en quête d'un standard, notamment pour la sécurité, la galaxie de l'Internet des objets, tout juste née de son Big Bang historique, ne manquera pas de révéler en 2016 ses failles et ses vulnérabilités.

4. Des nuages dans le ciel du « cloud »
Inexorable lame de fond qui modifiera à jamais le monde du stockage, le « cloud » éparpille données et fichiers dans un nuage de serveurs (ordinateurs) répartis dans d'immenses « data center » aux quatre coins du monde.
Ces « fermes » informatiques dédiées au stockage et au traitement des données présentent un double intérêt pour les cybercriminels.
Leur puissance peut être détournée à d'autres fins, tandis que les données stockées constituent un sérieux trésor de guerre au cœur duquel il est tentant de piocher.
Objet de toutes les attentions des esprits mal intentionnés, la vulnérabilité du « cloud » risque d'être régulièrement soulignée ces prochains mois.

5. Les gangs sous les projecteurs
Les cybercriminels se structurent en gangs d'une efficacité redoutable, souligne BullGuard.
« Ils passent des semaines, voire des mois, à effectuer des missions de reconnaissance avant d'attaquer des organisations », témoignent les experts de l'éditeur. « Ces entreprises ont été conçues dès le départ pour se spécialiser dans les crimes informatiques et ont des hiérarchies cloisonnées qui incorporent des programmeurs spécialisés dans le piratage, de vendeurs de données et des gestionnaires, tous supervisés par un cadre supérieur. Ces équipes de cybercriminels occuperont le devant de la scène en 2016. »

Réagissez à cet article

Source : *Virus, arnaques en ligne, cybercriminalité : les 5 dangers de l'année 2016 – L'Avenir Mobile*

Google corrige 5 failles critiques d’Android

Google corrige 5 failles critiques d’Android

Pratiquement tous les terminaux tournant sous une version récente d'Android sont affectés par au moins une des cinq failles critiques corrigées par Google dans l'OS mobile.

Google a remédié à une douzaine de vulnérabilités d'Android, dont cinq sont qualifiées de « critiques ».
Parmi les failles critiques identifiées et corrigées dans cette nouvelle série de correctifs, la firme de Mountain View signale qu'une des vulnérabilités pourrait permettre à un attaquant d'exécuter du code distant – comme un malware – en exploitant la manière dont Android traite certains fichiers médias.

Nexus, puis smartphones Samsung, LG et BlackBerry

Google précise par ailleurs qu'Android 5.0 et les versions ultérieures – dont « Marshmallow » 6.0 – sont affectées par ces différentes vulnérabilités.
Et si la nature de ces failles vous évoque quelque chose, ce n'est pas une coïncidence. Mois après mois, le service « mediaserver » reste le composant le plus problématique d'Android. Au point que Google a copié-collé le même message dans ses bulletins de sécurité à chaque fois que le composant a été affecté.
La vulnérabilité critique porte sur une partie centrale du logiciel Android et qui dispose de permissions auxquelles les applications tierces n'ont normalement pas accès. D'autres failles se situent elles dans la gestion du Bluetooth et du Wi-Fi, ou encore au niveau du kernel.
Les terminaux Nexus sont les premiers appareils Android à recevoir les correctifs de sécurité. D'autres fabricants, parmi lesquels Samsung, LG et BlackBerry, déploieront des mises à jour dans les prochains jours.

Réagissez à cet article

Source : *Google corrige 5 failles critiques d'Android*

2/3 des Français ont peur de l’intelligence des machines

2/3 des Français ont peur de l’intelligence des machines

Une étude réalisée par l'Ifop révèle qu'une grande majorité des Français appréhendent la montée en puissance de l'intelligence artificielle liée au Big Data. Une crainte paradoxale et un peu irrationnelle.

L'intelligence artificielle est-elle un danger pour l'humanité? De grands noms du monde scientifique ou de la high-tech semblent craindre en tout cas l'émergence d'une intelligence autonome des machines. Comme Elon Musk, le fondateur de Tesla, qui incitait en 2014 des étudiants à la prudence. « L'intelligence artificielle est plus dangereuse que le nucléaire », affirmait-il ainsi lors d'un **symposium**. Une crainte partagée par Bill Gates ou encore Stephen Hawking. Le grand physicien britannique affirmait même il y a un an à la BBC que « le développement d'une pleine intelligence artificielle pourrait signifier la fin de la race humaine. » Rien que ça.

Et les messages de ces personnalités semblent porter auprès de la population française. Selon une étude réalisée par l'Ifop pour l'Observatoire B2V des Mémoires, près des 2/3 de nos concitoyens (65%) seraient inquiets de la montée en puissance des machines autonomes. Les romans et films d'anticipation comme Terminator qui dépeignent un monde dominé par les machines intelligentes n'y sont sans doute pas pour rien.

L'intelligence c'est bien, à condition de garder le contrôle

Pourtant, et c'est paradoxal, les Français sont plutôt confiants quant à l'essor du Big Data qui serait à l'origine du développement de l'intelligence artificielle (I.A.) des machines. Ainsi, 69% d'entre eux pensent cette I.A. va croître avec le développement exponentiel de la production de données (Big Data). Et surtout que ce Big Data présente des avantages à court terme pour la santé et le bien-être (meilleure prévention des maladies, découvertes scientifiques…). 67% des Français sont plutôt enthousiastes quant aux promesses du Big Data.

« Pour les personnes sondées, le Big Data présente des avantages: il est considéré comme un facteur de progrès, notamment pour la recherche scientifique, la prévention et le traitement des maladies, analyse Francis Eustache, neuropsychologue et président du Conseil scientifique de l'Observatoire B2V des Mémoires. En même temps, l'intelligence artificielle inquiète, en particulier avec l'autonomie croissante des machines. » En d'autres termes, l'intelligence des machines c'est bien, mais à condition de ne pas les laisser agir seules, de garder le contrôle.

Des peurs un peu irrationnelles

Car derrière cette crainte de l'intelligence artificielle, il y a en fait deux peurs bien distinctes. Celle de machines trop intelligentes dotées d'une conscience, qui décideraient de se passer de l'humanité. Scénario très peu crédible à en croire de nombreux scientifiques comme le chercheur Jean-Gabriel Ganascia, spécialiste de ces questions. Une autre peur, plus crédible celle-là, est liée à **l'autonomie croissante de machines** (automobiles, drones, logiciels de trading…) trop peu fiables. Mais là aussi, les craintes sont sans doute exagérées tant les pouvoirs publics encadrent de plus en plus ce type de technologies.

Réagissez à cet article

Source : *2/3 des Français ont peur de l'intelligence des machines*

La CNIL sanctionne une société marketing

La CNIL sanctionne une société marketing

La Commission Nationale Informatique et Libertés vient de lancer un « avertissement public » à l'encontre de la société marketing Profils Seniors, pour « collecte déloyale » de données personnelles.

Profils Seniors est une petite société basée dans l'Essonne et « a pour activité la constitution d'une base de données de seniors qu'elle loue à des tiers effectuant de la prospection commerciale électronique », rappelle la CNIL dans son communiqué.
Or, les personnes interrogées par téléphone ne sont pas informées clairement de cette finalité, ce qui amène « à considérer cette collecte comme déloyale », estime l'organisme, chargé de veiller au respect des données personnelles faisant l'objet d'un traitement informatique.
Ainsi, selon les contrôles réalisés sur place par la CNIL en 2015, « les personnes appelées pensent participer à une enquête sur la consommation des ménages français, alors que l'appel vise également à constituer une base de données de seniors qui feront l'objet de prospection commerciale électronique par des tiers ».

Du non-consentement préalable à la non-protection des données personnelles
Par ailleurs, « la société ne recueillait pas le consentement préalable des personnes à recevoir de la prospection commerciale par voie électronique, tel qu'exigé par les textes » et « n'assurait pas la sécurité et la confidentialité des données personnelles qu'elle traitait », ajoute la CNIL.
De plus, Profils Seniors n'assurait pas « la sécurité et la confidentialité des données personnelles qu'elle traitait et qu'il n'existait pas de contrat ou de clauses spécifiques avec ses sous-traitants permettant de leur imposer des conditions de sécurité et de confidentialité des données » et n'avait pas « déposé une demande d'autorisation pour le transfert des données vers des sous-traitants situés dans des pays en dehors de l'Union européenne », souligne la commission.
Les sanctions que peut prononcer la CNIL vont de l'avertissement au retrait d'autorisation, en passant par la sanction pécuniaire (150.000 euros maximum) et l'injonction de cesser le traitement de données concernées.
L'organisme, qui plaide lui-même régulièrement pour un renforcement de ses pouvoirs, souligne par ailleurs que l'adoption du règlement européen sur les données personnelles lui permettrait, à partir de 2018, d'infliger des sanctions allant jusqu'à 4% du chiffre d'affaires de la société incriminée.

Réagissez à cet article

Source : *Les Echos.fr – Actualité à la Une – Les Echos*

Une célèbre PME de Montmorillon victime de piratage et de chantage

Une célèbre PME de Montmorillon victime de piratage et de chantage

Des pirates informatiques ont volé les données de clients sur le site de l'entreprise montmorillonnaise et tenté de faire chanter ses dirigeants.

Ils ne venaient pas pour les macarons et le chocolat : en début de semaine, des pirates informatiques ont attaqué le site internet de Rannou-Métivier, célèbre PME de Montmorillon. Ils visaient particulièrement la base de données de la clientèle.
« Notre service informatique a immédiatement réagi pour renforcer la sécurité du site. Cependant, des données ont déjà été volées », a fait savoir l'entreprise, mardi après-midi, dans un courrier adressé à tous ses clients disposant d'un compte sur son site.
« Une personne malintentionnée nous a demandé de l'argent en échange de la non-divulgation des données »
Les intrus ont en effet enregistré des adresses de messagerie électronique et postales, ainsi que des mots de passe d'une partie des clients. Une tentative de chantage a suivi : *« Une personne malintentionnée nous a demandé de l'argent en échange de la non-divulgation des données »* nous a précisé l'entreprise hier.

Les dirigeants ont en fait déposé plainte et révélé l'affaire eux-mêmes, informant les clients concernés afin qu'ils prennent leurs précautions.
« Nous vous conseillons de changer le mot de passe de votre messagerie personnelle s'il est identique à celui utilisé pour votre compte Rannou-Métivier, explique l'entreprise*. Si d'autres de vos comptes (Facebook, Ebay, Dropbox…) utilisent à la fois cette même adresse de messagerie et ce même mot de passe, nous vous conseillons d'en changer le mot de passe dans les plus brefs délais. Nous vous présentons toutes nos excuses pour la gêne occasionnée. »*

Pas de données bancaires piratées
Rannou-Métivier assure qu'aucune donnée bancaire n'est tombée entre les mauvaises mains : *« Elles n'ont jamais été stockées sur nos serveurs, elles sont utilisées uniquement le temps du paiement sur le site de la banque. Il n'y a aucun risque de perte d'argent pour nos clients. ».* La faille du site exploitée par le pirate a été identifiée mardi et la sécurité renforcée, tandis que le cryptage des données est en cours.

Rannou-Métivier emploie une soixantaine de personnes, la moitié dans ses laboratoires de production récemment agrandis à Montmorillon, le reste de l'effectif se partageant entre les boutiques de Montmorillon, Poitiers, Châtellerault et Tours.

Réagissez à cet article

Source : *Rannou-Métivier victime de piratage et de chantage – 31/12/2015 – La Nouvelle République Vienne*

Big Data Paris 2016

Big Data Paris 2016

Le congrès Big Data Paris 2016 se tiendra à Paris (Palais des Congrès de la Porte Maillot) le 7 et 8 mars 2016. Organisé par Corp Agency.

Le Congrès Big Data Paris vous invite, pour cette 5e année, à plonger dans l'univers passionnant du prédictif ! Sommet du Big Data en France, le congrès a réuni plus de 6 500 participants en 2015, animés par un seul et unique but : participer à la construction et au développement d'une filière française d'excellence !

Véritable laboratoire d'innovation et de disruption, le Congrès Big Data Paris 2016 valorisera les acteurs les plus avant-gardistes de la scène internationale : retours d'expériences, conférences stratégiques et prospectives, parcours immersif …

Plus d'informations sur le site de l'événement : http://www.bigdataparis.com

---

Réagissez à cet article

Source : *BIG DATA PARIS*

The Current State of Ransomware

	The Current State of Ransomware

---

In the past year or two, one of our most popular technical topics, for all the wrong reasons, has been ransomware.
Ransomware, as we're sure you know, is the punch-in-the-face malware that scrambles your files, sends the only copy of the decryption key to the crooks, and then offers to sell the key back to you.
Even Linux has ransomware these days, although fortunately we've only seen one serious attempt at Linux-based extortion so far, presuambly because cybercriminals haven't yet figured out how to make money in that part of the IT ecosystem.
Let's hope it stays that way for Linux sysadmins, because the crooks are still attacking Windows users heavily, and are still raking in lots of ill-gotten gains.

THE CRYPTOLOCKER YEARS
Two years ago, one strain of ransomware known as CryptoLocker dominated the demanding-money-with-menaces malware scene.
The US Department of Justice (DoJ) suggested that the crew behind CryptoLocker raked in $27,000,000 in September and October 2013 alone, in the first two months that the malware was widely reported.
And a 2014 survey by the University of Kent in England estimated that 1 in 30 British computer users had been hit by CryptoLocker, and that 40% of those coughed up, paying hundreds of dollars each in blackmail money to recover their data.
But in mid-2014, the DoJ co-ordinated a multi-country takedown of a notorious botnet called Gameover Zeus that targeted victims while they were doing online banking.
And, would you believe it: while the cops were raiding the Gameover servers, they came across the CryptoLocker infrastructure as well, and took down those servers at the same time, pulling off a neat double play.
CryptoLocker doesn't start its data scrambling until after it has called home for an encryption key, so killing its servers pretty much neutralised the warhead of the malware: it would get right to the very brink of detonation and then freeze, waiting for data that never came.
But any celebration about the damage done to the ransomware scene as a whole was short-lived.

RANSOMWARE REDUX
Cybercrime, if you will tolerate a clumsy metaphor, abhors a vacuum, and new ransomware soon appeared to fill the multi-million-dollar void left by the demise of CryptoLocker.
CryptoWall, and its close derivative CryptoDefense, were early pretenders to CryptoLocker's throne, but many others have appeared, too.
Threats like TorrentLocker, CTB-Locker and TeslaCrypt are big names these days, joined by other intriguing threats such as VirLock, ThreatFinder (an ironic name, considering that it is itself the threat) and CrypVault.

WHAT TO DO?
When it comes to malware of this sort, the dictum "know your enemy" is worth remembering.
With this in mind, James Wyke and Anand Ajjan, who are Senior Threat Researchers in SophosLabs, have recently published a thorough and well-written paper entitled The Current State of Ransomware.
This paper is a highly-recommended read – and it's a free download, no registration required.
https://www.sophos.com/en-us/medialibrary/PDFs/technical%20papers/sophos-current-state-of-ransomware.pdf?la=en

You'll learn about the history of ransomware, the latest threats, how they work, and what you can do to defend yourself.
Great stuff from SophosLabs!

Réagissez à cet article

Source : *The Current State of Ransomware – a new paper from SophosLabs |*

Filtrage des spams par les FAI. Possible ?

Filtrage des spams par les FAI. Possible ?

Par une ordonnance de référé concernant un litige entre Buzzee et Free, le Tribunal de commerce de Paris interdit aux FAI de bloquer les spammeurs.

Par une ordonnance de référé concernant un litige entre Buzzee et Free, le Tribunal de commerce de Paris interdit aux FAI de bloquer les spammeurs.
Voilà une jurisprudence qui peut à la fois effrayer et rassurer. Dans un litige opposant la firme Buzzee et Free en tant que Fournisseur d'Accès à Internet (FAI) et fournisseur d'un service de messagerie, le Tribunal de commerce de Paris a statué en référé pour interdire tout filtrage a priori par adresse IP des messages du premier par le second.
Certes, c'est une ordonnance de référé (statuant en urgence sur une évidence), qui plus est dans une justice spécialisée et de premier niveau. Nous sommes donc loin d'une décision de Cassation en chambre plénière. Mais les principes retenus dans cette jurisprudence portent loin puisqu'ils interdisent de fait à un FAI de filtrer les spams.

Bienvenue aux spammeurs au nom de la liberté d'expression

Buzzee est spécialisée dans l'envoi massif d'e-mails. Pour Free, c'est donc un spammeur et il a bloqué à l'entrée de ses serveurs mails tous les courriels provenant de cette entreprise en les filtrant par blocage d'adresses IP des serveurs SMTP de Buzzee. Cette dernière a donc attaqué en justice Free pour obtenir un déblocage. Et le tribunal lui a donné raison sur l'essentiel, limitant simplement ses prétentions financières exorbitantes et non-justifiées.
En effet, pour le tribunal suivant en cela l'argumentaire de Buzzee, ce n'est pas au FAI de décider qui respecte ou non la réglementation en matière de prospection commerciale, même si ses utilisateurs sont en majorité des particuliers qui doivent consentir préalablement à recevoir un message publicitaire.
Le code des postes et communications électroniques impose même une stricte neutralité aux FAI. Juridiquement, que Buzzee soit ou non un spammeur n'est pas le sujet et il n'a d'ailleurs pas été débattu. Par cette argumentation, c'est bien tout filtrage total a priori du spam qui est condamné. Au minimum, le destinataire des messages devrait donner mandat explicite à son opérateur pour filtrer selon des critères précis (comme à un opérateur de type MailInBlack par exemple). D'un autre côté, le rappel des règles de libre circulation du courrier électronique ne peut pas faire de mal. Car si un opérateur filtre le spam de sa propre initiative, on pourrait demain filtrer d'autres types de messages avec la même discrétion.

Réagissez à cet article