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*

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*

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*

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*

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

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

---

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

NOURRIR LE PROGRAMME : UN TRAVAIL FASTIDIEUX

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

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

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

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

QUAND UNE IA INVENTE LE CONCEPT DE CHAT

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

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

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

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

LE CAS COMPLEXE DES ROBOTS

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

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

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

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

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

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

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

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

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

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

EN BREF :

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

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

Ce qu'elle ne sait pas faire :

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

Les progrès qu'il reste à faire :

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

Réagissez à cet article

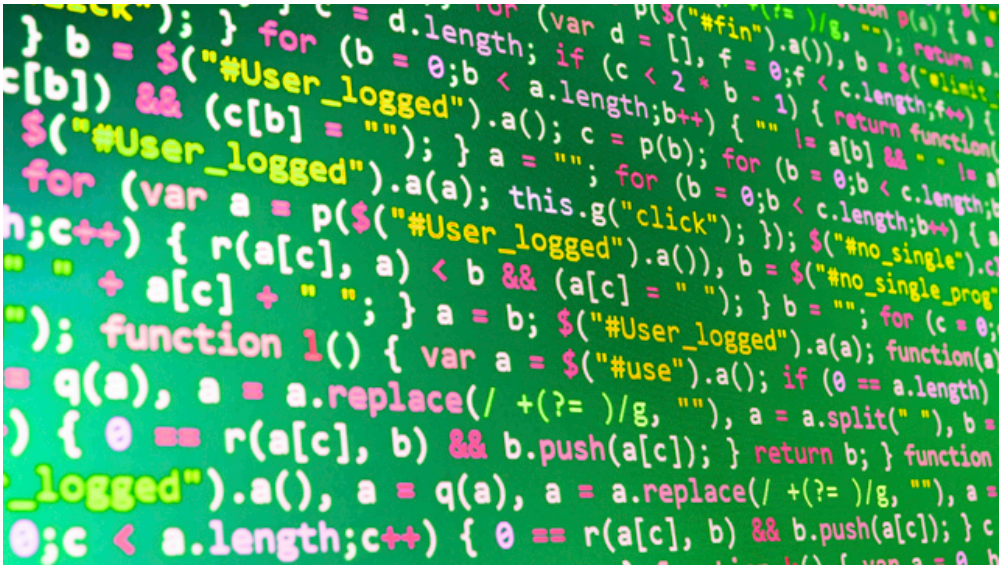
Source : *Apprentissage : l'intelligence artificielle, une élève de plus en plus douée*

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

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

---

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



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

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

Réagissez à cet article

Source : *Le code Erreur 451 synonyme de censure*

Les plus gros piratages de 2015 | Techniques de l’ingénieur

Les plus gros piratages de 2015 | Techniques de l’ingénieur

Année après année, c'est la même constat : quels que soient leur taille et leur secteur d'activité, les entreprises ne protègent pas assez efficacement leurs réseaux et les données personnelles ou sensibles qu'elles hébergent. Dans la majorité des cas, les attaques informatiques ont été facilitées par le non-respect de règles essentielles : mises à jour des logiciels, mots de passe faible, données sensibles pas chiffrées…

Janvier : 20 000 sites français piratés
Des mairies, des universités, des conseils généraux, des églises ou des PME… Après l'attentat contre Charlie Hebdo, de nombreux sites ont été victimes de pirates se réclamant du groupe État islamique. Dans la majorité des cas, ce piratage s'est limité à du « défacement » (modification de la page d'accueil notamment en remplaçant du texte par des revendications et/ou des images). Ce nombre élevé peut surprendre. En réalité, très peu de sites appliquent des règles élémentaires de sécurité.

Février, le « casse » du siècle
Selon l'éditeur russe d'antivirus Kaspersky, une centaine d'établissements bancaires d'une trentaine de pays auraient perdu entre 260 à 800 millions d'euros. Cette attaque massive aurait été organisée par des équipes russes et ukrainiennes.

Avril : mauvais vol chez Ryanair
Environ 4,5 millions d'euros ont été dérobés d'un des comptes de la compagnie aérienne à bas coûts Ryanair. Selon la société irlandaise, des pirates informatiques se seraient emparés de la somme par « un transfert

Juillet : des états civils plus privés
Des informations confidentielles sur la vie et l'état civil de près de 7% des américains ont été volées dans les serveurs de l'Office of Personnel Management, une agence du gouvernement fédéral des États-Unis qui gère notamment les demandes d'emploi dans la fonction publique. 22, 5 millions de personnes sont concernées par ce vol de données personnelles. Ce n'est pas la première fois que des administrations américaines sont victimes d'intrusion.

Juillet : des hackers au volant
Ne plus se plus se véhicules seront connectés d'ici quelques années. Les constructeurs devront renforcer la sécurité de leurs modèles sous peine de sortie de route ! Dans le Missouri, deux hackers ont en effet démontré qu'il était possible de prendre le contrôle à distance d'une Jeep Cherokee commercialisée par le groupe Fiat Chrysler. Situés à une quinzaine de kilomètres du véhicule, Charlie Miller et Chris Valasek (deux experts en sécurité, le premier étant connu notamment pour avoir révélé plusieurs failles dans l'iOS d'Apple) ont coupé le moteur pendant que la voiture roulait sur une autoroute. Ils ont également pris le contrôle des freins et du volant.

Août : des rencontres adultères… publiques
37 millions de comptes utilisateurs (dont des Français avec des adresses du ministère de l'Intérieur, de la Culture ou de plusieurs mairies) d'Ashley Madison ont été récupérés par un pirate. La base de données de cet important site de rencontres adultères comprend des informations très sensibles, comme les préférences sexuelles ou le numéro de téléphone. Pire, aux États-Unis, plus de 15 000 adresses email utilisées pour la création du compte provenaient de l'administration américaine ou de l'armée. De quoi lancer des opérations d'usurpation d'identité ou du chantage. Des sanctions disciplinaires et des peines de prison sont annoncées. Les conséquences sont parfois dramatiques. La police canadienne enquête sur deux suicides potentiellement liés au piratage de ce site géré par Avid Life Media, une société canadienne de Toronto.

Novembre : jouets en panne
Le fabricant de jouets VTech a été victime du piratage d'une de ses bases de données. Des clients français, canadiens, ainsi que des ressortissants d'autres pays étaient enregistrés dans ce fichier d'environ 6 millions de données. Un internaute britannique de 21 ans a été arrêté le 17 décembre. Il ne serait pas le seul pirate à avoir pénétré ce serveur…

0
Réagissez à cet article

Source : *Les plus gros piratages de 2015 | Techniques de l'ingénieur*

AVG dévoile ses prévisions d'attaques informatiques et technologiques pour 2016

AVG dévoile ses prévisions d'attaques informatiques et technologiques pour 2016

L'apparition de voitures autonomes n'est pas le seul élément prouvant que les systèmes logiciels « intelligents » vont améliorer notre sécurité. D'autres indicateurs sont également visibles sur Internet.
Chez AVG, il nous a fallu des années pour concevoir nos récents algorithmes de détection des brèches et de réputation des fichiers. Pour notre tout dernier moteur antivirus, nous avons utilisé des techniques sophistiquées d'apprentissage neuronal et de collecte de données dans le cloud, qui ont été conçues pour intercepter les logiciels malveillants plus en amont, et de manière plus systématique.

En 2016, de nouvelles solutions de sécurité fondées sur l'intelligence artificielle vont faire leur apparition.
On peut donc espérer que la bataille engagée contre les mauvais génies d'Internet va connaître un regain d'énergie très attendu, et que les menaces seront encore plus vite contrées et éliminées. Les progrès de l'intelligence artificielle et des systèmes d'apprentissage profond (ou « deep learning ») sont devenus bien plus accessibles. C'est ce que l'on a pu voir récemment, par exemple, lorsque Google a ouvert le code source de l'outil Tensorflow mis au point au sein de la division chargée de l'intelligence artificielle chez Google.

Autorités de certification : une disparition annoncée
La nécessité de sécuriser tout le trafic HTTPS des sites Web via un mode de chiffrement prend de l'ampleur. En 2016, avec l'apparition de nouvelles normes ouvertes et le fait que les propriétaires de sites pourront plus facilement faire des choix, il se pourrait que cette réalité devienne globale. Certaines autorités de certification, qui par comparaison commencent à paraître un peu dépassées, risquent de connaître des moments difficiles.
Ces dernières années, certains cas d'erreurs de gestion des certificats, des incidents de sécurité et des brèches de données les ont mis sur la sellette et ont fragilisé la puissance de ces géants. La confiance dans les certificats SSL a également été ébranlée, notamment par le fait que des organismes d'état pourraient infiltrer, dans certains cas, nos communications Web prétendument sûres.
Traditionnellement, le rôle d'une autorité de certification est de confirmer l'identité du propriétaire légitime d'un site Web avant d'émettre un certificat SSL signé. Cela reste une bonne idée pour les entreprises qui peuvent se le permettre, et certaines protections et indemnités d'assurance sont également prévues. En revanche, pour un blogueur ou un propriétaire de site professionnel lambda, il est à la fois laborieux et inutile de payer une autorité de certification et se soumettre à ce qui peut sembler un processus laborieux de vérification et de confirmation. Dans ce contexte, les alternatives techniques telles que Let's Encrypt (actuellement en phase bêta) devraient prospérer.
En outre, l'identification des faux certificats SSL va se poursuivre dans le cadre du programme de transparence des certificats de Google, grâce à des systèmes de détection intégrés dans les navigateurs Web modernes. Google continue à demander aux autorités de certification d'assumer leurs responsabilités, afin que nous soyons tous mieux protégés.
Enfin, avec l'annonce d'autres solutions telles que le protocole DANE proposé par Internet Society, qui offre la possibilité à n'importe quel propriétaire de site Web de valider son propre certificat SSL et donc de se passer totalement d'une autorité de certification, l'année 2016 va nous réserver des nouveautés intéressantes !

Malvertising et réseaux publicitaires : réagir ou disparaître
La publicité malveillante ou « malvertising » désigne ce qui se produit lorsque des visiteurs innocents sont la cible d'éléments malveillants, causés par des échanges avec des tiers douteux et une sécurité déficiente sur plusieurs réseaux publicitaires en ligne. En 2016, les réseaux publicitaires vont devoir réagir ou disparaître, avant qu'ils ne détruisent l'économie numérique qu'ils ont contribué à bâtir, et ne ruinent les résultats des sites Web dont la survie dépend des recettes publicitaires.
Ce problème a une cause principale : la « surface d'attaque » des scripts de publicité et de suivi toujours plus nombreux et complexes fournis par les réseaux publicitaires et intégrés par les éditeurs (souvent de façon transparente) sur leurs sites Web.
Sur mobile, plus de la moitié de la bande passante est utilisée pour la diffusion d'annonces publicitaires, beaucoup plus que pour le contenu même de la page !
S'il est associé avec des attaques réseau plus classiques, ce nouveau vecteur peut servir à infecter des milliers de victimes qui visitent des sites pourtant légitimes. Il faut aussi savoir que, même si beaucoup de grands réseaux publicitaires réagissent rapidement et arrêtent le flux de trafic lorsqu'un cas de malvertising se produit, quelques minutes suffisent pour toucher des centaines, voire des milliers de victimes. Toute personne ayant récemment installé un système de blocage publicitaire vous certifiera que ses sites Web préférés se chargent incroyablement plus vite, ce qui paradoxalement n'arrange rien.
Il faut malheureusement reconnaître qu'une grande partie des sites Web riches en contenu, pour qui les recettes publicitaires sont essentielles, se chargent lentement. En fait, une étude menée par le New York Times a montré que, pour la version mobile de nombreux sites d'actualité, plus de la moitié de la bande passante utilisée sert à la diffusion d'annonces publicitaires. Cela représente un volume de données (chargement des annonces, scripts et codes de suivi) supérieur au contenu effectivement affiché sur la page que vous lisez !
Toutefois, les systèmes de blocage de la publicité ne sont pas une solution à long terme à ce qui, finalement, est un problème de mise en œuvre. C'est encore plus vrai si vous convenez que la disparition du principe de monétisation actuellement en vigueur sur Internet pourrait avoir des conséquences économiques désastreuses. De plus, une récente déclaration de l'IAB (Interactive Advertising Bureau) confirme que les annonceurs « tiennent beaucoup moins compte de l'expérience utilisateur » dans leur manière d'élaborer des contenus.
Pour empêcher les systèmes de blocage d'annonces de se répandre, l'IAB a imaginé L.E.A.N. (de l'anglais Light, Encrypted, Ad Choice Supported and Non-Invasive), un programme basé sur des principes intervenant dans la prochaine phase des normes techniques publicitaires destinées à la chaîne d'approvisionnement publicitaire numérique globale. Quelle que soit la solution choisie, une chose est certaine : les réseaux publicitaires doivent réagir et régler les problèmes de sécurité, faute de quoi l'année 2016 pourrait bien être celle où la « vague scélérate » du malvertising aura emporté des millions d'entre nous.

Les mots de passe résistent
Les mots de passe sont un concept, pas une technologie, et la grande majorité d'entre nous va continuer à se servir de cet outil pour de nombreuses ressources, dans la vie privée comme dans la vie professionnelle. Alors certes, les mots de passe seront toujours utilisés en 2016, mais ils ne sont pas la panacée universelle, et vous avez donc intérêt à connaître certaines alternatives.
Cette année, Yahoo a annoncé le lancement d'une solution de sécurité qui utilise des périphériques mobiles plutôt qu'un mot de passe pour contrôler les accès, et nous avons même vu Google intégrer des fonctionnalités de verrouillage intelligent Smart Lock capables de déverrouiller votre smartphone en se servant des appareils présents à proximité.
Il existe des alternatives intéressantes aux mots de passe, même si ces derniers ont encore de beaux jours devant eux grâce à leur gratuité.
En matière de contrôle d'accès, la validation en deux étapes est un système efficace qui a tendance à se répandre et reste très utilisé chez de nombreux fournisseurs basés dans le cloud. Lorsqu'elle est proposée, vous avez tout intérêt à l'utiliser, surtout si vous n'êtes pas un spécialiste des mots de passe. Même s'il est interminable, le code de votre smartphone n'est pas inviolable, et le dispositif de lecture d'empreintes n'est peut-être pas si inutile.
Les mots de passe sont gratuits, et toutes les autres solutions ont généralement un coût, que ce soit sur le plan de la technologie ou de la complexité, ce qui explique que les mots de passe aient de beaux jours devant eux. Il est certain qu'en 2016, les problèmes liés aux mots de passe (réutilisation, stockage mal sécurisé, par exemple) ne risquent pas de disparaître. Espérons toutefois que nous saurons maintenir la vigilance des consommateurs et des entreprises !
L'Internet des objets : le principe de sécurité intégrée atteint le point d'ébullition Cela peut certes être amusant de posséder une de ces toutes nouvelles bouilloires WiFi, que vous pouvez allumer depuis votre smartphone, sans vous lever de votre fauteuil, mais ces objets normalement inoffensifs peuvent aussi révéler votre clé WiFi. Ceci n'est qu'un exemple de plus du problème existant au niveau de l'intégration de la sécurité.
S'ils ne sont pas protégés, chaque appareil périphérique, chaque téléviseur ou système stéréo intelligent, chaque système d'éclairage ou de sécurité domotique, et même ces nouveaux réfrigérateurs à la mode et ces voitures autonomes, bref tout ce qui est connecté à un réseau peut être la cible d'un hacker.
Les cybercriminels testent le matériel, analysent les ondes et recueillent mots de passe et autres données personnelles, quel que soit l'emplacement où ces informations sont conservées. Dans ce nouveau monde d'objets connectés, le danger augmente à mesure que la technologie vieillit.
Nous sommes nombreux à avoir paramétré nos ordinateurs et nos appareils mobiles de manière à ce qu'ils se mettent à jour automatiquement. En même temps, aucun d'entre nous ne pense à gérer la sécurité de ses appareils domestiques et à installer la dernière version logicielle.
Les objets connectés du quotidien peuvent réveler votre clé Wifi, et être la cible d'un hacker…Nous devons revoir notre façon de considérer ces appareils.
Dans certains cas, il est impossible de les mettre à jour. Nous devons considérer ces appareils et ces gadgets comme des ordinateurs déguisés, et les protéger aussi bien que nous le ferions pour notre PC et notre téléphone. Nous allons continuer à voir de nombreuses choses surprenantes connectées à Internet, et si aucun effort n'est fait pour y intégrer la sécurité, le problème risque d'empirer, car certains fabricants ne prennent pas le temps de mesurer les risques que courent les objets connectés au réseau.
Pour revenir un instant à l'analogie avec la bouilloire, rappelons que, dans une entreprise, si un employé achète une bouilloire intelligente, personne ne va s'en inquiéter et personne ne s'attendra à ce que le département informatique ait son mot à dire sur ce genre d'achat. Nous devons donc revoir entièrement notre façon de considérer ces appareils.

Mettre à jour : un élément vital !
Aujourd'hui plus que jamais, il est absolument essentiel que chaque logiciel, appareil, gadget ou équipement soit mis à jour.
Les constructeurs de voitures autonomes tels que Google annoncent déjà qu'ils assumeront la responsabilité des infractions au code de la route, et éventuellement des accidents ou des blessures corporelles dont leurs véhicules seraient responsables. Maigre consolation, avouons-le, si vous êtes victime d'un accident parce que vous avez oublié d'installer la dernière version du logiciel sur votre voiture … À mesure que les systèmes logiciels intelligents s'installent dans nos vies de multiples manières, ces mêmes logiciels pourraient décider de mettre votre vie en danger, il faut en être conscient.
Il va réellement devenir impératif que vous mettiez systématiquement vos logiciels à jour, en même temps que vos autres appareils. Un jour, cela vous sauvera peut-être la vie…

Réagissez à cet article

Source : *Cyber-Sécurité : AVG dévoile ses prévisions pour 2016 – Global Security Mag Online*

Apple contre le projet de loi britannique sur le renseignement !

Apple contre le projet de loi britannique sur le renseignement !

Le monde semble actuellement « en guerre » contre les projets de loi sur le renseignement qui fleurissent un peu partout dans les pays développés. Et nombreux sont ceux qui prennent part à ces actions. Apple, par exemple, a clairement affiché ses objections face au projet de loi britannique.

Le monde semble actuellement « en guerre » contre les projets de loi sur le renseignement qui fleurissent un peu partout dans les pays développés. Et nombreux sont ceux qui prennent part à ces actions. Apple, par exemple, a clairement affiché ses objections face au projet de loi britannique.

Pour la firme de Cupertino, affaiblir les techniques de chiffrement, comme le souhaite le gouvernement britannique, reviendrait à diminuer la sécurité des « données personnelles de millions de citoyens respectueux des lois« . La création d'une porte dérobée présente, elle, un risque majeur : « une clef laissée sous le paillasson ne serait pas là uniquement pour les gentils. Les méchants sauraient la trouver également. » Voici en substance les points qu'Apple a voulu souligner à la commission en charge de ce projet de loi.

Autre point sensible : la modification du fonctionnement de iMessage pour pouvoir être écouté « placerait une entreprise comme Apple, dont la relation avec les clients est en partie construite sur un esprit de confiance quant à la confidentialité des données, dans une position très difficile« .

La commission saura-t-elle prendre en compte ce genre de considérations ? À suivre !

Réagissez à cet article

Source : *Apple contre le projet de loi britannique sur le renseignement !*

Augmentation de la cybercriminalité encore prévu pour 2016

Augmentation de la cybercriminalité encore prévu pour 2016

Le nombre de piratages informatiques a substantiellement augmenté en 2015, une tendance qui devrait encore s'affirmer en 2016. Chefs d'Etat, groupes industriels, médias, banques, petites entreprises ou particuliers, personne n'est à l'abri de la menace.

Si les cyber-attaques (attaques informatiques, ndlr) ont augmenté durant l'année 2015 en France et dans le monde, la tendance ne semble pas près de s'atténuer en 2016. C'est la mise en garde prononcée par de nombreux organismes, dont le Cercle européen de la sécurité et des systèmes d'information. Cet organe, qui fédère les professionnels du secteur de la sécurité informatique, redoute un cyber-sabotage de grande ampleur en 2016.
Difficile cependant de cerner le danger car il vient de partout, emploie des formes diverses et peut toucher tout le monde, directement ou pas. A grande échelle, une attaque déclenchée à distance peut viser des objectifs affectant des bassins entiers de population : réseau électrique, distribution de l'eau, contrôle de la circulation, trafic aérien. Ou encore s'en prendre à des organismes gouvernementaux avec les conséquences que cela implique.

Des attaques en forte hausse

L'Allemagne a eu affaire à ces deux types d'attaques ces douze derniers mois: la mise hors service par deux fois d'un haut-fourneau dans la Sarre et le piratage de l'ordinateur personnel d'Angela Merkel. En France, l'exemple le plus spectaculaire remonte au printemps dernier quand la chaîne francophone TV5Monde (257 millions de foyers à travers le monde) a carrément cessé d'émettre durant plusieurs heures après une attaque perpétrée par Daech.

TV5 Monde avait été ouvertement ciblée par Daech. REUTERS/Benoit Tessier

A moyenne échelle, les malfaiteurs peuvent s'en prendre à une entreprise pour lui voler des données ou gripper son système informatique. Le cabinet PricewaterhouseCoopers révélait en octobre dernier que les cyber-attaques contre les entreprises avaient progressé de 38 % en un an dans le monde et de 51 % en France alors que les pertes financières s'élevaient à 3,7 millions d'euros par entreprise victime d'attaque en moyenne. Il faut noter que plus d'un tiers des sources d'incident provient d'employés de la compagnie attaquée.
A plus petite échelle, les particuliers sont touchés par des escroqueries en tout genre, à la carte de crédit par exemple. Ainsi, un rapport récent de Norton/Symantec révélait qu'un Français sur cinq s'était fait dérober ses données bancaires après un achat en ligne. Le phénomène est tellement répandu que les banques ont peut-être trouvé la parade, du moins provisoirement : le cryptogramme dynamique qui change toutes les 20 minutes, un identifiant qui va commencer à figurer au dos des cartes de crédit en 2016.

De plus en plus sophistiqués

Les hackers, remarquent les professionnels, utilisent des méthodes de plus en plus sophistiquées pour fracturer les systèmes informatiques de leurs cibles. Dans un rapport récent, l'entreprise de sécurité informatique roumaine Bitdefender identifiait des évolutions notables pour 2016. La première touchait aux systèmes de monétisation publicitaires et en particulier les systèmes de blocage de publicité qui pourraient être utilisés par les pirates informatiques pour développer de nouvelles souches de logiciels malveillants.
D'après Bitdefender, le monde de l'entreprise va être encore plus touché en 2016 à travers des attaques ciblées visant essentiellement le vol d'informations. Mais les individus aussi seront plus vulnérables, en partie du fait de la multiplication des objets connectés qui recèlent de nombreuses failles de sécurité exploitables par les cybercriminels. Même des systèmes d'exploitation réputés plus sûrs, comme le Mac OS X d'Apple, ne seraient plus à l'abri d'être percés par les malfaiteurs en ligne, selon Bitdefender.

Réagissez à cet article

Source : *La cybercriminalité devrait encore augmenter en 2016 – France – RFI*