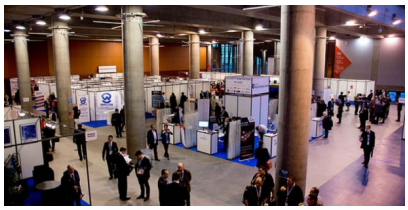
Fic 2016 : La sécurisation des objets connectés préoccupe enfin…

	Fic 2016 : La sécurisation des objets connectés préoccupe enfin…

Le 8e Forum international de la cybersécurité, qui s'est tenu à Lille les 25 et 26 janvier, a permis de découvrir des solutions qui émergent en France en termes de sécurisation des objets de communication et des systèmes d'information auxquels ils sont connectés. Certaines sont encore à construire comme la plateforme Scop, d'autres sont déjà opérationnelles comme le CERT-Ubik et le boitier Hardsploit.

La multiplication des objets communicants, les IoT en anglais pour Internet Of Things, est une excellente opportunité pour la cybercriminalité. Sachant qu'à chacun de ces objets correspond une adresse IP, leur diffusion rend les réseaux très perméables.

« On estime à plus 50 milliards leur nombre d'ici 2020, soit 7 objets connectés par personne sachant qu'il y aura 7,5 milliards d'habitants sur terre. Les hackers vont pouvoir profiter d'une perméabilité des systèmes d'informations jamais atteintes jusqu'à présent. Et si la sécurité était en réalité le principal enjeu de l'Internet des objets ? »

A cette question posée en introduction de son exposé lors du 8e Forum International de la Cybersécurité, Christophe Joly, le directeur sécurité de Cisco France, a bien sûr répondu par l'affirmatif en chiffrant à plus de 375 milliards de dollars le marché annuel du cybercrime qui se profile. Mais comme avec les voitures au début du vingtième siècle et avec Internet plus récemment, le législateur attendra sans doute qu'une catastrophe ait lieu avant de mettre en place des règles. En attendant, rien n'empêche de se protéger.

Sécuriser l'électronique embarquée

Pour Cisco, le leader mondial des technologies informatiques de connectivité, les moyens de le faire passent par une bonne connaissance de son infrastructure informatique et des objets qui s'y connectent. Mais cette approche ne suffit pas toujours, entre autres quand l'objet communique par radiofréquence. De plus, la sécurité des objets connectés ne porte pas uniquement sur les réseaux et les… *Lire la suite…*

Réagissez à cet article

Source : *Cybercriminalité: la sécurisation des objets connectés est en marche au FIC*

D’où vient le danger des Objets connectés ?

D’où vient le danger des Objets connectés ?

Le développement des objets connectés s'accélère de plus en plus tandis que la mise en place de moyens de sécurité reste quant à elle beaucoup plus discrète… Tout le monde connaît le récit mythique du cheval de Troie, alors ne sommes-nous pas en train de danser sur ce qui va causer la perte de notre identité à chacun ? Qu'en est-il des normes de sécurité dans le domaine des objets connectés ? Comment pouvons-nous protéger nos données personnelles ?

Deux étudiants en médecine, ont pointé du doigt les failles que pourraient comporter certains objets connectés, dans des actions spectaculaires : prendre le contrôle d'un Pacemaker à distance ou encore désactiver les freins d'une voiture connectée. Ces actions coups de poing mettent à nu les faiblesses que comportent certains objets connectés face à des hackers malveillants. En effet, c'est précisément là que ce situe le paradoxe des nouvelles technologies qu'utilisent les objets connectés… Car s'ils sont conçus pour nous faciliter le quotidien, ils peuvent au contraire nous faire beaucoup de mal et en particulier à nos données personnelles ! Pour pouvoir se protéger, il faut avant tout comprendre cette technologie et adopter quelques habitudes très utiles.

Tout objet connecté peut être hacké

Pour comprendre comment une balance connectée peut devenir notre ennemi numéro 1, il faut d'abord comprendre comment cheminent des data (c'est-à-dire les données personnelles qui sont recueillies pendant l'utilisation de l'objet connecté) vous concernant, quels en sont les tenants et les aboutissants et où sont stocké ces données.
Il existe trois principaux canaux par lesquels voyagent nos data : les réseaux Wifi, le Bluetooth et les réseaux cellulaires pour objets connectés (Sigfox et Lora sont deux des principaux acteurs de ces réseaux).
Ces données sont ensuite acheminées jusqu'aux serveurs du fabricant ou du développeur de l'application pour ensuite revenir vers vous avant de repartir sur le Cloud… Au milieu de tous ces voyages, il devient très facile de voler ou de prendre le contrôle de vos objets, surtout si vous passez par un réseau public.

Le hackage est une menace très sérieuse à prendre en compte

En 2015, on a constaté une augmentation de 50 % de la cyber-criminalité en France ! Les concepteurs et développeurs d'objets connectés nous parlent sans cesse de nouveautés incroyables et parfaites pourtant comment celles-ci sont-elles sécurisés ? Est-ce que les différents fournisseurs appliquent ou suivent des normes ou une réglementation officielle pour sécuriser le matériel de fabrication ? Il semble qu'il n'y ai pas encore de législation officielle qui soit mise en place, même si la CNIL (Commission Nationale de l'Informatique et des libertés) s'est dernièrement attelé au sujet lors du Forum International de la cyber-sécurité.

Sécurité des objets connectés

C'est lors des voyages des data que celles-ci sont les plus vulnérables.
Mais le problème reste entier tant que les données qui voyagent ne seront pas cryptées… Ces données personnelles récoltés par les objets connectées peuvent avoir un intérêt économique pour certaines sociétés.
Ainsi, votre balance connectée peut en dire long sur vos habitudes alimentaires, votre traqueur de sommeil connecté peut donner, lui aussi, de précieuses informations sur vos habitudes de vie quotidienne. Ces données qui peuvent se monnayer très cher favorisent le profilage ciblé pour les publicités notamment et vous enlever petit à petit la liberté d'acheter ce qui vous plaît et non pas ce que l'on vous a suggéré. Le reste des data qui vous concerne, comme vos données bancaires ne sont, également, pas à l'abri d'un hackeur qui chercherait à vous voler de l'argent sans toucher à votre porte-monnaie !

Optimisez la sécurité de vos objets connectés

Face aux deux risques majeurs de la reprise malveillante de vos données personnelles : l'utilisation commerciale et le piratage des donnés personnelles, vous pouvez adopter quelques gestes simples pour augmenter la sécurité de vos data. Si les objets connectés s'avèrent être dans de nombreux cas, un formidable assistant dans la vie quotidienne pour surveiller votre alimentation, votre sommeil, … Au contraire, s'ils sont mal connus ou utilisés d'une mauvaise manière, ils peuvent devenir très dangereux pour le particulier. Vous ne devez pas oublier qu'il est essentiel de comprendre comment fonctionnent ces technologies pour en profiter au maximum sans crainte.
Dans un premier temps, vous devez lister tous les objets connectés en activité dans votre maison et déterminer pour chacun d'entre-eux à quoi ils sont connectés et par quel biais (Wifi ou Bluetooth ou réseau cellulaire). Par cet inventaire un peu minutieux mais très utile, vous pourrez contrôler le cheminement de vos données personnelles et savoir quel objet connecté communique par des biais peu sécurisés. Pour que votre sécurité soit optimale, vous devez également effectuer régulièrement des mises à jour en ce qui concerne la sécurité et surtout changer régulièrement les mots de passe et vos identifiants. Il ne faut pas oublier que même si vos objets connectés restent dans votre maison, les data qu'ils produisent voyagent eux sur le net et donc dans le monde !

Réagissez à cet article

Source : *IOT et sécurité : ne laissez plus le cheval de Troie entrer chez vous*

La France aurait-elle peur de Intelligence artificielle ?

La France aurait-elle peur de Intelligence artificielle ?

L'intelligence artificielle caractérisée par l'autonomie croissante des machines, ça vous fait peur ? 65% d'un panel de Français répondent oui. Mais pour quelles raisons sont-ils inquiets ? Et aujourd'hui, l'IA, c'est quoi au juste ? Pas sûr qu'une majorité de Français puissent cette fois répondre.

	Plutôt d'accord	Plutôt pas d'accord
· L'intelligence artificielle est amenée à prendre un essor considérable avec le Big Data	69%	31%
· Le Big Data fera l'objet d'une utilisation très importante à long terme par les pouvoirs publics et les entreprises (profilage des individus, surveillance)	68%	32%
· Le Big Data présente des avantages à court terme pour la santé et le bien-être des individus (meilleure prévention des maladies et des risques, traitements plus adaptés, découvertes scientifiques, etc.)	67%	33%
· L'intelligence artificielle caractérisée par l'autonomie croissante des machines (comme les drones armés ou la voiture Google) vous inquiète	65%	35%

Non, ne paniquez pas, vous n'êtes pas pris dans une boucle spatiotemporelle et de retour en février 76, avec sur l'écran, face à vous, Roger Gicquel. Relativisons dès à présent. La France n'a pas peur de l'intelligence artificielle.
Mais une majorité de Français d'un panel de 10004 personnes se déclare plutôt d'accord lorsqu'on lui demande si l'intelligence artificielle « caractérisée par l'autonomie croissante des machines (comme les drones armés ou la voiture Google) » l'inquiète.

Des effets de génération dans les craintes

Et effectivement selon le sondage IFOP commandé par « L'Observatoire B2V des Mémoires », 65% se déclarent inquiets. Ce sentiment ne se diffuse cependant pas de façon uniforme d'un français à un autre.
Ainsi les 25-34 ans sont, en proportion, aussi inquiets (69%) que les 65 ans et plus (70%), bien plus en tout cas que les 18-245 ans (50%). De même, les résultats de l'étude font état de disparité géographique et en fonction du niveau de diplôme sur cette question.
« Il existe donc des effets de génération dans les craintes qui ne tiennent pas simplement à la jeunesse, à l'âge et au niveau d'éducation » commente dans un communiqué Jean-Gabriel Ganascia, professeur à l'Université Pierre et Marie Curie (Paris VI).
Les Français sondés sont donc en majorité inquiets, soit. Mais, et la question n'est pas pédante, combien de ces Français sont au fait des travaux autour de l'IA et de ses usages concrets ? Très certainement une très faible portion, car les notions et savoirs scientifiques associés à ce domaine de recherche s'avèrent d'une très grande complexité.
« Aujourd'hui beaucoup d'entreprises, dont Facebook, partagent cette même vision, à savoir que les problèmes que nous cherchons à résoudre sont infiniment complexes. Et même si nous employons les meilleurs talents, ce n'est pas suffisant pour résoudre ces problèmes comme celui de l'apprentissage non supervisé » expliquait ainsi Florent Perronnin, directeur du laboratoire de recherche parisien de Facebook dédié à l'intelligence artificielle.

« **La peur est dans la population parce qu'elle ne sait pas de quoi on parle** »

Mais celui qui résume le mieux le résultat de cette étude, c'est peut-être Michel Nachez dans une interview à Rue 89 :
« La séduction [à l'égard de l'IA] est du côté de ceux qui sont dans le milieu de l'informatique robotique, et chez les fans de science-fiction. La peur est dans la population parce qu'elle ne sait pas de quoi on parle. Elle est influencée par la littérature, le cinéma, les séries, où la machine finit par tourner mal, se retourne contre l'homme et le détruit. »
Cela ne signifie pas néanmoins que l'intelligence artificielle ne puisse pas être une source légitime d'inquiétude ou de questionnement, mais alors pour des risques bien différents de ceux qui pourraient être imaginés par certains, comme des machines douées de conscience se retournant contre leur créateur.
« Ceux d'entre nous en première ligne dans la fourniture de code sont très excités par l'intelligence artificielle, mais nous ne voyons pas de chemin réaliste permettant à notre logiciel d'acquérir une conscience » déclarait d'ailleurs à ce sujet Andrew Ng, un spécialiste renommé du machine learning (apprentissage automatique).

Et si le risque c'était l'homme et non l'IA ?

Plusieurs personnalités de l'univers des technologies, comme Bill Gates et Elon Musk, ont pourtant argué des dangers représentés par l'IA. Mais pour Jean-Gabriel Ganascia, interrogé par Le Monde, ces « allégations ne reposent sur rien […] Ce n'est même pas que je suis en désaccord sur le plan scientifique, c'est qu'il n'y a rien sur le plan scientifique. »
« Une machine peut être autonome au sens technique du terme : elle peut effectuer une chaîne d'actions (capter des informations, prendre une décision puis agir) sans que l'homme intervienne, à part en amont. Cela n'est pas dangereux en soi, car la machine est soumise au but que l'homme lui a donné » ajoutait-il.
Des dérives découlant de l'utilisation de ces technologies sont possibles. La FTC, le régulateur américain du commerce, souligne ainsi dans un rapport récent les risques potentiels d'exclusion engendrés par l'exploitation d'algorithmes (qui peuvent faire appel à de l'IA) appliqués au Big Data.
Mais la source de ces risques n'est pas alors l'IA elle-même, mais l'auteur ou l'exploitant des algorithmes, par exemple au travers d'un usage tourné essentiellement vers la maximisation du profit, et négligeant l'intérêt des consommateurs, la législation ou portant « atteinte à des valeurs fondamentales d'inclusion et d'équité. »
Et ces risques sont sans doute bien plus plausibles que l'émergence d'une intelligence artificielle malfaisante asservissant la race humaine. « Il pourrait y avoir, dans un futur lointain, une race de robots tueurs, mais je ne travaille pas aujourd'hui à éviter de rendre l'IA malveillante pour la même raison que je ne m'inquiète pas du problème de surpopulation sur la planète Mars » commentait Andrew Ng lors de la conférence GTC 2015.

Réagissez à cet article

Source : *Intelligence artificielle – La France a peur. Mais de quoi au juste ?*

Carte de paiement sans contact – Le client n'est pas toujours roi

Carte de paiement sans contact – Le client n'est pas toujours roi

Refuser les cartes bancaires équipées du paiement sans contact n’est pas toujours simple. Un client du Crédit agricole l’a appris à ses dépens.

En avril 2015, un adhérent de l’UFC-Que Choisir de Senlis saisit l’association locale de ses difficultés avec son agence du Crédit agricole de Rixheim (68). Celle-ci lui a adressé en renouvellement une carte bancaire Visa munie de la fonction paiement sans contact. Ayant lu dans Que Choisir que cette fonction n’était pas sans faille, ce consommateur demande à sa banque le remplacement de sa carte par une même carte Visa mais sans cette nouvelle fonction. Refus de son agence, puis de la direction régionale du Crédit agricole qui affirme que c’est impossible et lui propose en échange soit une carte Visa avec débit différé, soit un autre type de carte bancaire. Pas d’accord, le particulier fait part de ce blocage à l’association locale de l’UFC-Que Choisir de Senlis.

Client à la porte

L’intervention de cette dernière auprès de la banque n’aura pas plus de succès. Face à un tel refus, elle saisit la Cnil (Commission nationale de l’informatique et des libertés) au motif que le Crédit agricole viole une de ses recommandations qui impose aux banques d’offrir à leurs clients la possibilité de refuser la fonction paiement sans contact.

La Cnil rejette la plainte de l’association locale, déclarant ne pas pouvoir imposer aux banques un changement de carte à l’identique mais rappelle que le particulier a la possibilité de faire désactiver la fonction.

Fort de cette réponse, le consommateur demande à son agence cette désactivation.

Pour toute réponse, la banque a mis son client à la porte, le sommant de restituer tous ses moyens de paiement. La Cnil a été avertie d’un tel comportement.

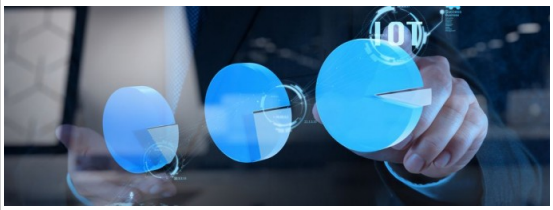
Réagissez à cet article

Source : *Carte de paiement sans contact – Le Crédit agricole a la main leste – UFC Que Choisir*

L’Internet des objets boostera-t-il l’Europe ?

	L’Internet des objets boostera-t-il l’Europe ?

En plein CES de Las Vegas, AT Kearney vient de livrer une version rafraîchie de son étude sectorielle sur la high-tech en Europe avec un focus #IoT.



L'Internet des objets donnera-t-il un nouveau souffle au secteur high-tech en Europe ? AT Kearney a publié un focus dans ce sens qui montre tout le potentiel…s'il est bien exploité.
En pleine effervescence du CES organisé à Las Vegas, le cabinet de consulting d'origine américaine vient de présenter à Paris la troisième version de son étude sur les nouvelles technologies en Europe sous l'angle de l'IoT
C'est une véritable opportunité de croissance sur les 10 prochaines années, estime Hervé Collignon, Partner d'AT Kearney, expert en TMT (télécoms, médias et technologies) et co-auteur du rapport.
Ce potentiel économique est estimé à près de mille milliards d'euros d'ici 2025. Il pourrait correspondre à 7 points de PIB à cet horizon.
Et les start-up comme Sigfox, Netatmo ou Withings et les groupes industriels français ont une carte à jouer. Ils ont pris position sur le marché des objets connectés dans le BtoC et le BtoB (historiquement via le M2M).
Dressons d'abord le tableau des perspectives présumées gigantesques de cet Internet des objets, qui va permettre « l'interconnexion du monde physique en facteur 10 par rapport à l'Internet phase 1 ».
Entre les technologies exponentielles (capteurs, bande passante, hardware, stockage & cloud), la population connectée (3 milliards de personnes en 2015), les effets réseaux (peering, IPv6, plateformes, interopérabilité…) et l'essor du big data, tous les ingrédients sont réunis pour assister à une « nouvelle révolution » qui va toucher tous les secteurs d'activité, estime Hervé Collignon.
A l'horizon 2025, le marché des solutions IoT en Europe (hors fabrication des objects connectés) est évalué à 80 milliards d'euros. Les intégrateurs de systèmes (IBM, Accenture, Atos…) remporteraient la plus grosse part du gâteau : plus d'un quart du business généré (22 milliards d'euros), devant les fournisseurs de services et de plateformes (le club GAFA et les opérateurs télécoms) qui pourraient en tirer un business de 18 milliards d'euros….
On retrouverait les opérateurs dans une autre catégorie : les spécialistes de la connectivité pour l'IoT. Un segment qui pourrait peser 15 milliards d'euros à l'horizon 2025 et qui comporte des pure players comme Sigfox.
Toujours selon le cabinet en stratégie qui a présenté mardi midi les résultats de son étude à Paris, on devrait recenser dans dix ans une base installée de 26 milliards d'objets connectés (correspondant à un marché de 10 milliards d'euros pour les fournisseurs de composants et modules comme Sierra Networks, Telit ou Gemalto).
L'essor de la dimension Internet des objets devraient avoir un impact sur 5 secteurs principalement : le transport et l'hôtellerie (250 milliards d'euros), la santé (235 milliards d'euros), la domotique domestique (160 milliards d'euros), le matériel industriel (pour un montant similaire), et la distribution, commerce (hors commerce électronique) et vente en gros (60 milliards d'euros).
Divers paramètres pourraient modifier cette perspective apportée par AT Kearney : le niveau d'adoption des objets connectés par les consommateurs, la politique industrielle associée à l'IoT en Europe (balbutiante en l'état actuel malgré une certaine prise de conscience par la Commission européenne), la guerre d'influence des plateformes (Google, Apple, Samsung…), la rationalisation des standards IoT sur fond de consortiums puissants (Open Interconnect, Allseen Alliance, Industrial Internet Consortium…), l'avancée de la 5G en Europe, l'impact de l'IoT sur l'emploi et la juste appréciation du traitement des données.
Etude « The Internet of Things : a new path to European Prosperity », ATKearney, janvier 2016, co-auteurs : Thomas Kratzert et Michael Broquist (respectivement Partner et Principal à Stockholm), Hervé Collignon et Julien Vincent (respectivement Partner et Principal à Paris)
En savoir plus sur http://www.itespresso.fr/europe-vraie-puissance-internet-objets-117702.html#2t626JMWackx6u04.99

Réagissez à cet article

Source : *L'Europe, une vraie puissance de l'Internet des objets ? | ITespresso.fr*

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*

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*

Au bout du compte, combien de secondes fait gagner la high-tech ?

Au bout du compte, combien de secondes fait gagner la high-tech ?

Capteurs électroniques, fibre de carbone, combinaisons en polyuréthane, eyetracking… Jusqu'à quel point la technologie permet-elle aux sportifs de dépasser leurs limites… tout en restant humains ?

Quoi ? Vous vous êtes équipé des applications Nike + Running, STT Sport Tracker ou Micoach d'Adidas, et vous n'avez pas encore battu le record du 100 mètres ? C'est normal. Ces applications n'ont pas pour but de vous transformer en Usain Bolt, mais de vous permettre de mieux gérer vos efforts, et de mesurer vos progrès.

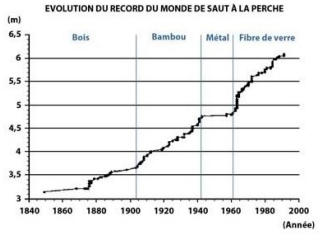
Reste que la technologie a toujours joué un rôle pour améliorer les performances sportives, et faire gagner des centimètres ou des secondes. C'est que la technologie peut améliorer les records grâce à trois facteurs : la mesure de la physiologie, les vêtements de sport et la tenue portée, et les matériaux utilisés.

« L'eyetracking » pour garder l'oeil sur les performances

Pour la mesure des performances corporelles, l'institut des sciences du sport de Berne utilise par exemple l'eyetracking pour étudier « le comportement du regard, ainsi que ses répercussions sur le comportement décisionnel en situations sportives ». Mais la mesure n'a pas de limite : développé par la NASA pour ses astronautes, la « pilule thermomètre » peut être ingérée pour prendre en permanence la température du sportif en plein effort – puis être ensuite restituée par les voies naturelles.

Des « vêtements dopants » ?

Même les vêtements et accessoires peuvent « doper » la performance : ainsi, les combinaisons de nageurs en polyuréthane ont-elles été interdites en 2009, du fait de leur trop grande efficacité. Les scientifiques ont évalué en 2008 que ces tenues permettaient de gagner 1 à 2% sur le chronomètre, et les chercheurs de l'Institut de recherche biomédicale et d'épidémiologie du sport (Irmes) ont estimé que deux tiers des records du monde de natation battus depuis 2000 l'ont été grâce aux combinaisons.



Fibre de carbone, aluminium, graphite…

Quant aux matériaux, ils jouent bien sûr un rôle essentiel dans les gains de performance. La preuve chiffrée en a été apportée de manière éclatante dans la discipline du saut à la perche. Comme le montre le graphique ci-dessous, les perches en bois permettaient à peine de dépasser 3,5 mètres. Avec le bambou, on atteint 4,5 mètres. Le métal permet de tutoyer les 5 mètres et, avec la fibre de carbone, les records explosent, jusqu'à dépasser les 6 mètres.

En 2010, le cycliste Fabian Cancellara a défrayé la chronique parce qu'il utilisait un pédalier optimisé (qui réduit les forces de frottement par un roulement à billes de graphite et huile) qui lui faisait gagner 2 secondes au kilomètre. Toujours dans le cyclisme, l'utilisation d'un cycloergomètre (vélo immobile servant à des mesures scientifiques) a montré que le plateau de type Harmonic permet une augmentation significative de la puissance maximale développée (+ 3%) lors d'un sprint ou d'une montée.

Bien entendu, les prothèses du coureur amputé Oscar Pistorius présentent un cas extrême. Non seulement elles lui permettaient de courir, mais elles furent accusées de lui offrir un avantage face à ses rivaux : une expertise a révélé que l'énergie restituée par les prothèses lors de la poussée était quasiment trois fois plus élevée que celle des chevilles humaines – au point qu'en janvier 2008, l'Association internationale des fédérations d'athlétisme lui a interdit de participer avec les valides aux jeux de Pékin.

La prochaine étape ? Sans doute des capteurs électroniques ou des régulateurs d'hormones greffés en permanence, qui brouilleront les frontières entre les sportifs et les cyborgs…

Réagissez à cet article

Source : *Big Data : La high-tech fait-elle gagner des secondes ?*