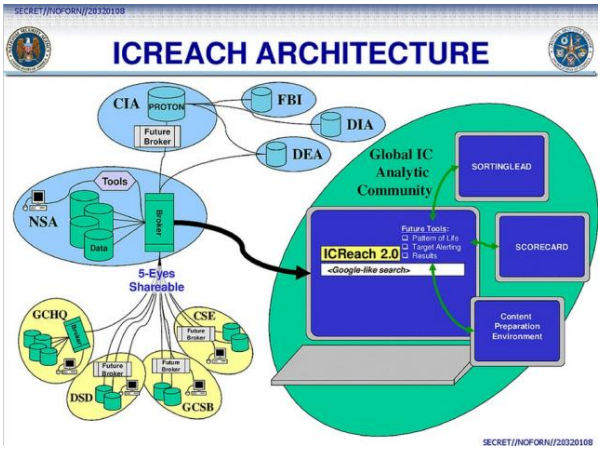
ICReach, le moteur de recherche secret «à la Google» de la NSA

ICReach, le moteur de recherche secret «à la Google» de la NSA

Certes, la NSA est une agence secrète, mais entre bons amis, elle concède volontiers de partager des informations. Et même beaucoup d'informations, comme le prouve l'existence d'ICReach.

Révélé par The Intercept, sur la base de documents d'Edward Snowden, ce programme de surveillance compile plus de 850 milliards de métadonnées récoltées dans le monde entier et les rend accessibles au travers d'un moteur de recherche « à la Google » auprès d'une vingtaine d'agences gouvernementales américaines. Comme par exemple la CIA (service secret), le FBI (police fédérale) ou le DEA (agence de lutte anti-drogue).



Plus d'un millier d'agents gouvernementaux américains ont ainsi accès à une véritable mine d'or informationnelle. En effet, ICReach compile non seulement des métadonnées téléphoniques, mais aussi des métadonnées relatives aux communications emails et aux messageries instantanées. Au total, ce moteur de recherche référence plus d'une trentaine de champs : temps et durée d'appel, numéros d'appel, protocole, IMEI (identifiant unique du smartphone), identifiant de la cellule mobile de réception, adresse email, identifiant chat, etc. Les données proviennent d'une multitude de bases de données gérées par la NSA, mais aussi par les partenaires du club « Five Eyes » (Royaume-Uni, Australie, Nouvelle-Zélande, Canada).

Les métadonnées surveillées par ICReach.
Ainsi, l'enquêteur pourra savoir qui communique avec qui et depuis quel endroit. Mais ce n'est qu'un début. En croisant toutes ces données, l'objectif est de pouvoir extraire les habitudes de vie quotidienne d'une cible : quels endroits elle fréquente, avec qui et à quel moment, etc. La NSA appelle cela « pattern of life analysis » (« analyse du mode de vie »).
Il est difficile de savoir combien de personnes peuvent être potentiellement surveillées par cet outil. Il concerne principalement des non-Américains, dans la perspective d'un « renseignement extérieur » (« foreign intelligence »). Ce qui est assez vague et peut aller de la guerre anti-terroriste à l'espionnage économique, en passant par la lutte contre la criminalité organisée.
Comme bon nombre de programmes de surveillance de la NSA, ICReach trouve son origine dans les attentats du 11 septembre, qui avaient révélé un manque de communication entre les différentes agences gouvernementales américaines. Un problème qui, visiblement, a été résolu. Attention, ICReach n'est pas à confondre avec XKeyscore, un autre moteur de recherche célèbre de la NSA. Mais celui-ci est davantage restreint au monde de l'espionnage. Par ailleurs, il ne cible que les données du web.

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Sources :
http://www.01net.com/editorial/625470/icreach-le-moteur-de-recherche-secret-a-la-google-de-la-nsa/#?xtor=EPR-1-NL-01net-Actus-20140826
https://firstlook.org/theintercept/article/2014/08/25/icreach-nsa-cia-secret-google-crisscross-proton/

La France en première ligne de cyber-espionnage face à Epic Turla

La France en première ligne de cyber-espionnage face à Epic Turla

Selon le centre de recherche de Kasperky, notre pays est le plus touché par une attaque de cyber-espionnage connue sous le nom d'Epic Turla.

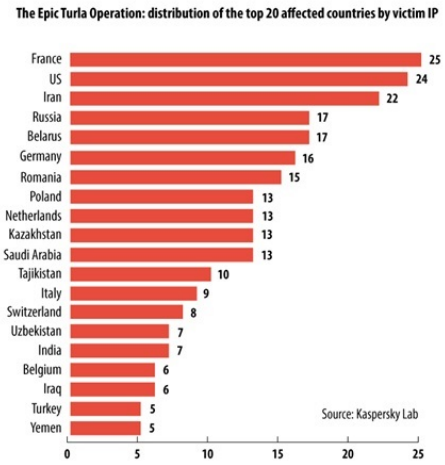
Selon Kaspersky Labs, la France est le pays le plus visé par une attaque de cyber-espionnage référencée sous le nom d'Epic Turla ou UroBuros, ou encore snake, pour d'autres éditeurs de logiciels de sécurité. La plupart des cibles sont des entités gouvernementales ou des ambassades sises en Europe ou au Moyen-Orient.

Une APT assez classique

Techniquement, l'attaque suit le schema classique d'une APT (Advanced Persistent Threat) avec hameçonnage par du spear phishing, l'utilisation d'exploits zero day, du social engineering et du waterholing par des sites infectés. Une fois dans la place, Epic se connecte au serveur de command and control et envoie les informations sur le système de l'utilisateur. Le système est ensuite compromis avec des outils spécifiques, des fichiers préconfigurés avec des commandes. L'attaque se déplace ensuite latéralement pour obtenir les bonnes accréditations et prendre la main pour soutirer les informations voulues. Selon le laboratoire, l'attaque est toujours en cours.

Tous les détails techniques ici :

https://securelist.com/analysis/publications/65545/the-epic-turla-operation/



Les statistiques d'infection par Epic Turla

par Bertrand Garé, le 22 août 2014 14:42

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Références :

http://www.linformaticien.com/actualites/id/33931/cyber-espionnage-la-france-en-premiere-ligne-face-a-epic-turla.aspx

Orange piraté : Le rapport de la Cnil et les sanctions à l’encontre de l’opérateur historique

L’autorité chargée de la protection des données personnelles publie un avertissement sans conséquences à l’encontre d’Orange. La Cnil critique l’opérateur pour avoir permis à des pirates de faire la copie des données personnelles concernant 1,3 million de clients.

La Cnil adresse un avertissement, sans sanction financière, à l’encontre d’Orange. L’autorité indique qu’en avril dernier, l’opérateur avait permis d’avoir accès aux noms, prénoms, date de naissance, adresse électronique et numéro de téléphone fixe ou mobile de 1,3 million de clients.
Pour Orange, la plateforme visée servait en particulier pour ses campagnes commerciales, notamment pour l’envoi de courriers électroniques et de SMS. Après que la société a admis ces dysfonctionnements, la Cnil a mené une enquête auprès de l’opérateur. Elle livre désormais ses conclusions.
Elle estime que les dysfonctionnements ayant engendré la faille de sécurité ont certes depuis été corrigés. « Toutefois, plusieurs lacunes en termes de sécurité des données ont été identifiées et ont justifié l’engagement d’une procédure de sanction », précise-t-elle. La Cnil reproche par exemple à Orange de n’avoir pas fait réaliser d’audit de sécurité avant d’utiliser la plateforme technique de son prestataire.
Second point à la charge d’Orange, l’organisme rapporte dans une note que la société a envoyé de manière non sécurisée à ses prestataires les mises à jour de ses fichiers clients et « qu’aucune clause de sécurité et de confidentialité des données n’avait été imposée à son prestataire ». La sécurité des données n’était donc pas assurée dans l’ensemble de la chaîne, ce que reproche la Cnil en émettant cet avis à l’encontre d’Orange.

Le rapport de la CNIL du 7/08/2014

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Références :
http://pro.clubic.com/legislation-loi-internet/cnil/actualite-722731-orange-recoit-carton-jaune-cnil.html?&svc_mode=M&svc_campaign=NL_ClubicPro_New_26/08/2014&partner=-&svc_position=6454261656svc_misc=-&crmID=639453874_6454261656estat_url=http%3A%2F%2Fpro.clubic.com%2Flegislation-loi-internet%2Fcnil%2Factualite-722731-orange-recoit-carton-jaune-cnil.html

---

La Xbox Live et le Vatican attaqués par les pirates informatiques de Lizard Squad

La Xbox Live et le Vatican attaqués par les pirates informatiques de Lizard Squad

Probablement l'œuvre de mauvais farceurs, les attaques répétées sur les réseaux de jeux en ligne continuent. Même le Saint-Siège se retrouve en ligne de mire des hackers.

Jusqu'où iront les pirates de « Lizard Squad » ? Après avoir attaqué, durant ce week-end, un certain nombre de services de jeux en ligne comme Sony Online, Blizzard et Battle.net, le groupe de pirates a changé de cible et pris en ligne de mire le site du Vatican.
Il a revendiqué une attaque par déni de service distribué (DDoS) il y a une dizaine d'heures. Comble du mauvais goût, le groupe fait référence, dans son message Twitter, à l'idéologie radicale de l'Etat Islamique. Ainsi, il estime que « tous les non-musulmans doivent mourir » (« all kuffar shall die »), ajoutant une série de mots-clés comme #ISIS, #Jihad, #ISIL et #IS. Visiblement, l'opération a été couronnée de succès, car, d'après plusieurs témoignages sur Twitter, le site du Saint-Siège était déconnecté ce matin.
Il ne l'est plus à l'heure actuelle.

Article de Gilbert Kallenborn01netle 25/08/14 à 17h34

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Références :
http://www.01net.com/editorial/625416/apres-sony-les-pirates-de-lizard-squad-attaquent-xbox-live-et-le-vatican/#?xtor=EPR-1-NL-01net-Actus-20140825

Les fraudes bancaires touchent plus d'une entreprise sur six

Un peu moins de 20% des entreprises victimes d'une fraude bancaire.

Les entreprises sont de plus en plus les cibles d'escrocs bancaires. Avec un préjudice estimé à ce jour à 250 millions d'euros, les pouvoirs publics et les organisations professionnelles tirent le signal d'alarme.

1 entreprise sur 6 affirme avoir été victime d'au moins une tentative de fraude en 2013. Ce chiffre est le résultat d'une étude interne au secteur bancaire publiée aujourd'hui par . Les grandes PME sont les cibles préférées des escrocs. En effet, une entreprise sur deux qui compte entre 500 et 1.000 salariés et qui a un chiffre d'affaires supérieur à 75 millions d'euros a déclaré avoir été la cible d'une tentative de fraude. Un chiffre qui retombe entre 10 et 15% pour les plus petites entreprises. Autre phénomène: si ces fraudes touchent tous les secteurs d'activité sans exception, elles visent très fréquemment le commerce, en raison du grand nombre de transactions réalisées dans ce secteur.

Trois types de fraude font fureur

Les fraudes aux virements internationaux peuvent se présenter sous plusieurs formes, comme l'indique une note d'information publiée par le Service Régional de Police Judiciaire de Clermont-Ferrand (SRPJ). La première d'entre elles est appelée «escroquerie à la nigériane», en raison du lieu d'agissement des escrocs, qui opèrent depuis la côte ouest africaine. Ceux-ci détournent des transactions entre les entreprises françaises et leurs fournisseurs asiatiques. Leur méthode: envoyer des courriels aux entreprises en se faisant passer pour le fournisseur. Les fraudeurs parlent alors de «dysfonctionnements bancaires» et souhaitent que le prochain virement soit réalisé sur un compte «plus sécurisé», qui va donc tout droit dans leur poche.

Une autre technique de fraude est celle de l'«escroquerie au président» ou arnaque «au faux patron». Selon le SRPJ de Clermont, cette méthode est «la plus redoutable». Les escrocs exigent des virements des responsables d'une entreprise, en se faisant passer pour leur PDG. Comme le décrit le SRPJ, ce genre d'escroquerie nécessite «une autorité naturelle, un certain aplomb et, il faut bien le reconnaître, un don pour la comédie». Un don qui passe par plusieurs ruses. Selon Les Echos, la première est d'insister sur le caractère urgent de la requête dans le cas d'un futur contrôle fiscal, d'une OPA ou autres. Les escrocs ne manquent pas d'imagination. La seconde, dite de «l'ingénierie sociale», est d'effectuer une collecte d'informations sur l'entreprise via les réseaux sociaux pour en adopter les codes. Et s'ajoute à cette pointe de réalisme une touche de flatterie. Comme l'indique le SRPJ, la supercherie aura plus de chance de fonctionner si le comptable de l'entreprise se sent «flatté d'être dans la confidence du patron». Cette méthode qui ne fait toutefois que peu de victimes est de loin la plus redoutable car elle émane de bandes parfaitement organisées. Pour les petites entreprises, les méthodes de fraude les plus répandues restent toutefois celles liées aux actions du quotidien, comme la fraude à la carte bancaire volée ou usurpée.

Enfin la dernière ruse à la mode est celle qui profite de la norme Sepa, l'espace de paiement unique européen. Les escrocs se font alors passer pour le responsable informatique de la banque qui gère les comptes de l'entreprise ciblée. Ils arrivent alors à convaincre l'interlocuteur de la société d'effectuer une série de tests et, à distance, ils prennent le contrôle de l'ordinateur et effectuent des virements directement sur leur compte en banque. Cette technique est rendue possible par le système Sepa grâce auquel la banque n'a plus à se soucier de l'accord du client avant d'effectuer un virement. Celui-ci peut toutefois contester l'opération dans le cas où il constate un virement anormal.

60% des entreprises sont satisfaites de la réaction de leur banque

Même si ces trois techniques sont les plus répandues, les fraudeurs ne manquent pas d'imagination pour escroquer les entreprises qui, dans bien des cas, ne pourront pas se faire rembourser les montants dérobés. Une fois le virement réalisé, elles peuvent en effet contacter leur banque, mais les établissements ne peuvent pas s'immiscer dans les ordres de paiement. Toutefois, les entreprises sont majoritairement satisfaites de la réaction de leur banque, à hauteur de 60%. Un pourcentage qui diminue pour les petites entreprises de moins de 20 salariés mais qui passe à 80% pour les grandes entreprises. Un chiffre qui dépend également du type de banque choisi par l'entreprise, les taux de satisfaction étant en effet plus élevés pour ceux qui optent pour une banque commerciale par rapport à une banque mutualiste.

Pour lutter contre ces fraudes, la Fédération bancaire Française (FBF) a annoncé qu'elle rencontrerait prochainement, avec des représentants de la police et de la justice, ses homologues chinois, pays d'où proviennent un grand nombre de fraudes. Pour le moment, elle a fait savoir dans une vidéo que «plusieurs centaines de procédures sont en cours au sein de la police judiciaire» pour un montant des préjudices qui se chiffre à «plus de 250 millions d'euros».

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Références :

http://www.lefigaro.fr/conjoncture/2014/08/22/20002-20140822ARTFIG00233-les-fraudes-bancaires-touchent-plus-d-une-entreprise-sur-six.php

---

Alerte : Arnaque par téléphone d'un agent Microsoft

Alerte : Arnaque par téléphone d'un agent Microsoft

Depuis quelques temps, une arnaque au cours de laquelle un agent vous appelle afin de résoudre avec vous vos soucis d'informatique prend de l'ampleur à la Police.

Le principe?
De nombreuses personnes témoignent à présent du même mode opératoire : vous êtes appelé par un opérateur à l'accent anglophone, se faisant passer pour un employé de « Microsoft », ou bien de son service client « Customer Care Center ».
Selon cet opérateur, des messages d'erreur leur seraient parvenus via votre ordinateur, et pour y remédier, il vous suffit d'accéder, avec un code, à une page web « infosis.net » ou bien « logme120.com ». Ces noms changent régulièrement, c'est pourquoi c'est essentiellement le mode opératoire qui doit vous alerter.
L'agent vous demande alors d'installer un logiciel pour voir votre écran et commencer un tutoriel afin que vous puissiez résoudre ensemble votre problème informatique. Vous l'avez compris: ce programme n'est autre qu'un espion informatique chargé de s'introduire dans des relations bancaires ou des données de cartes de crédit.
Que faire?
Important :La société Microsoft a déjà réagi dans de nombreux pays, en précisant qu'elle ne contacte jamais les usagers, sans que ceux-ci ne l'aient préalablement sollicitée. De plus, l'aide de spécialistes de dépannage Microsoft ne vous est jamais facturée ainsi en ligne !
Afin de protéger un ordinateur contre diverses formes d'escroquerie, il est conseillé d'utiliser un outil de suppression de logiciels espions fiables.
Si vous n'avez pas reçu un faux appel de téléphone mais cela ne signifie pas que vous êtes protégé contre d'autres types d'escroquerie, c'est pourquoi il est conseillé d'utiliser un programme de prévention de spyware.
Dans le doute, passez en revue tous les programmes de votre ordinateur en vérifiant la fonctionnalité de chacun d'entre eux, de détecter les éventuels programmes « espions » afin de les supprimer.
Vous pouvez également signaler ces messages à la police judiciaire via Pharos : www.internet-signalement.gouv.fr
N'oubliez pas le numéro « Info Escroqueries » 0811 02 02 17 (prix d'un appel local depuis un poste fixe ; ajouter 0.06 €/minute depuis un téléphone mobile)
! SOYEZ VIGILANT !

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Références :
http://www.police-nationale.interieur.gouv.fr/Actualites/Dossiers/Arnaque-via-un-appel-d-un-agent-Microsoft

L’utilisation juridique des documents numériques – Article de presse dans L’Echo du mardi du 12 08 2014

	L’utilisation juridique des documents numériques Article de presse dans L’Echo du mardi du 12/08/2014

L’utilisation juridique des documents numériques

«Dans le doute, après avoir numérisé un document officiel, vous avez probablement préféré conserver l’original dans son format matériel (bien souvent papier).

A l’heure de la dématérialisation à outrance (remplacement dans une entreprise ou une organisation de ses supports d’informations matériels, souvent en papier, par des fichiers informatiques et des ordinateurs, jusqu’à la création de « bureau sans papier » ou « zéro papier » quand la substitution est complète), il est temps de se poser des questions sur la valeur juridique des documents informatiques en cas de contestation ou de litige. Le traitement de documents dématérialisés présente un certain nombre d’avantages significatifs.»

Télécharger l’article complet

Cet article vous à plu ? Laissez-nous un commentaire (notre source d’encouragements et de progrès)

Alerte Ebola : Les arnaques sur Internet sur l’aide humanitaire ont déjà commencé

Alerte Ebola : Les arnaques sur Internet sur l’aide humanitaire ont déjà commencé

Les cybers-escrocs ne laissent aucune opportunité leur passer sous le nez. Pendant que le virus Ebola sévit en Afrique, ils tentent de profiter de la psychose pour vendre un remède miracle.D'après le site d'information burkinabé fasozine.com, un des messages envoyés par ces malfrats d'une nouvelle ère dirait ceci :
"Bonjour cher internaute, Sous le haut parrainage du Ministre de la santé canadienne Rona Ambrose Dans le cadre de la difficulté dans laquelle l'Afrique de l'ouest précisément a été confronté par le virus EBOLA et nous avons constaté que ce virus se développer et très bientôt".

Si vous ne l'avez pas encore dans votre boite mail, sachez que c'est avec ce français douteux que beaucoup d'internautes ont été abordés par ces "brouteurs" ces derniers jours.
(brouteurs = jeunes férus d'internet basés principalement en afrique qui ont trouvé le moyen de gagner de l'argent facilement grâce à des arnaques en escroquant des Occidentaux naïfs)
"Toute l'Afrique sera bientôt atteinte par ce virus", annoncent les oiseaux de mauvais augures. Pour tenter de vous soutirer une somme, ces voleurs proposent aux internautes une porte de sortie : **"Un laboratoire canadien vient justement de trouver deux remèdes miracles : l'un pour guérir et l'autre pour la prévenir". Toutefois, les doses seraient limitées selon leur propos. Pour avoir gratuitement ces doses, ces arnaqueurs vont suggérer de verser une somme de 180 dollars qui, toujours selon eux, "représente l'argent du service courrier DHL". Une somme variable " selon la distance aérienne de votre pays par rapport au republique du bénin"**.
Nous rappelons tout simplement que les médicaments qui existent aujourd'hui sont à un stade expérimental. Les conseils que l'on formule pour lutter contre ce virus sont entre autres d'éviter de toucher un animal trouvé mort en forêt, éviter de toucher sans protection les vomissures, le sang, la selle d'un malade, ni rester sans protection près de lui, ne pas toucher ou laver les vêtements et autres objets souillés ou d'un cadavre…

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Références :
http://www.afriqueitnews.com/2014/08/20/les-brouteurs-sautent-sur-lopportunite-offerte-par-ebola/

La CNIL veut encadrer le traçage des clients dans les magasins

La CNIL veut encadrer le traçage des clients dans les magasins

La Commission indique qu'elle souhaite garder le contrôle et encadrer les dispositifs de traçage et de profilage des clients dans les magasins, les supermarchés et les centres commerciaux.
A mesure que les smartphones équipent de plus en plus de personnes, les commerçants comptent bien tirer parti de ces appareils nichés dans nos poches. Que ce soit pour de la mesure de fréquentation ou simplement de l'analyse comportementale, les téléphones portables permettent d'identifier facilement les cibles. La CNIL tente de protéger les consommateurs que nous sommes en mettant plusieurs garde-fous.

Ainsi, dans certains centres commerciaux, la fréquentation des magasins est mesurée : des boîtiers captent les données émises par le téléphone portable (adresses MAC de la carte réseau par exemple) et calculent la position géographique des personnes. Ainsi, il est possible de connaître la fréquentation, mais aussi le parcours des personnes à l'intérieur du centre (la géolocalisation indoor).

La CNIL note que les personnes doivent d'abord en être informées. « Une information claire doit être affichée dans les lieux où sont mis en place ces dispositifs », demande-t-elle avant d'émettre des propositions de mesures. Par exemple, la suppression des données lorsque le client sort du magasin. Ou encore : l'algorithme d'anonymisation utilisé doit assurer un fort taux de collision, c'est-à-dire qu'un identifiant en base doit correspondre à de nombreuses personnes.

Mesure d'audience
Autre point sensible : la mesure d'audience avec par exemple les panneaux publicitaires. « Ils permettent de compter le nombre de personnes qui regardent la publicité et le temps passé devant celle-ci, d'estimer leur âge et leur sexe, voire d'analyser certains comportements », rappelle la CNIL.
Là encore elle émet des mesures simples à appliquer, comme l'interdiction de l'enregistrement des images, de leur transmission à des tiers ou de leur visualisation auprès des prestataires. Une nouvelle fois, les clients doivent être informés de ce qu'il se passe. Car « ces dispositifs reposent sur des caméras placées sur des panneaux publicitaires » et ne sont pas forcément visibles.

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Références :
http://www.linformaticien.com/actualites/id/33899/la-cnil-veut-encadrer-le-tracage-des-clients-dans-les-magasins.aspx

---

Internet des objets – L'industrie va être bousculée | Alliancy, le mag

Les objets connectés vont bousculer nos vies

Les objets connectés vont se multiplier dans les années qui viennent. Dès aujourd'hui, tous les industriels doivent intégrer cette nouvelle dimension, tant dans leur façon de concevoir et de fabriquer leurs produits que dans leur business model.80 milliards, c'est le chiffre choc publié par l'Idate, voici quelques mois. Il s'agit du nombre d'objets connectés qui auront été vendus à l'horizon 2020. Mais Idate, Gartner ou IDC… toutes les analyses prévoient une progression fulgurante de l'Internet des objets, un phénomène qui impactera toute l'industrie. D'une part, il y a aura des terminaux connectés à Internet, c'est-à-dire les smartphones, les tablettes et autres « phablettes »…, et, d'autre part, des objets intelligents, balances, bracelets, brosses à dents, montres connectés… Tous ces objets grand public bénéficient d'une très large couverture médiatique et connaîtront une forte croissance dans les années à venir. La généralisation du bouton d'appel d'urgence eCall, obligatoire dans toutes les voitures neuves vendues en Europe à partir de 2015, va imposer la voiture connectée sur nos routes. De même, tous les Français vont, tôt ou tard, disposer d'un compteur intelligent (Linky) et pourront suivre sur le Net l'évolution de leur consommation électrique ou de gaz quasi en temps réel.

Mais, pour Samuel Ropert, analyste à l'Idate, la grande majorité de cet Internet des objets sera peuplée de « choses » beaucoup moins technologiques. « La plus grande part de l'Internet des choses se composera d'objets ne disposant pas d'intelligence, mais capable d'interaction. 85 % de ces milliards d'objets connectés à venir seront porteurs d'une puce RFID ou même d'un simple code-barres 2D, et donc porteur d'une information. »

Dans un premier temps, les industriels vont déployer ces technologies pour optimiser leur supply chain. « Si la conjoncture actuelle freine les grands déploiements de puces RFID, les industriels et les grandes enseignes de la distribution peuvent espérer des gains significatifs dans l'efficacité de leur supply chain et dans la réduction de leurs stocks grâce à l'Internet des objets », ajoute l'analyste.

Les industriels de l'automobile préfèrent poser des puces RFID sur les conteneurs et hésitent encore à doter chaque pièce détachée d'une puce pour des raisons de coût.

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Références :

Internet des Objets – L'industrie va être bousculée