Norauto inaugure la « révision connectée » grâce au boîtier Xee | Le Net Expert Informatique

Norauto inaugure la « révision connectée » grâce au boîtier Xee

Les clients Norauto pourront, bientôt, se laisser installer un boîtier connecté dans leur auto. Le but : leur fournir des informations, des services, et les alerter de la prochaine révision.

En associant son application mobile, lancée en 2013, au boîtier connecté Xee, Norauto se dit désormais prêt à proposer un service d'un nouveau genre : la « révision connectée ». Alors que l'appli se limitait jusqu'alors au suivi des entretiens auto, elle sera bientôt capable de signaler aux automobilistes lorsqu'il est temps d'aller à la révision. Pour cela, l'enseigne équipera les voitures d'un petit appareil sur la prise diagnostic (OBD).
Fabriqué par la société lilloise Eliocity depuis l'automne 2014, Xee – concurrent des solutions Automatic ou Drust – a plusieurs fonctionnalités : localiser l'auto grâce à sa puce GPS, envoyer un SOS en cas de problème, déclencher une alerte s'il y a une effraction, aider à améliorer la conduite en observant le comportement du conducteur, et en lui prodiguant des conseils sur l'application (changements de rapports…), et d'autres.
Grâce à la connaissance du kilométrage en temps réel, l'application préviendra des révisions à venir, comme c'est déjà le cas dans certains véhicules haut de gamme. L'avantage pour le client est qu'aucune modification du véhicule n'est nécessaire pour le rendre compatible. La « révision connectée » sera dans un premier temps testée auprès d'un panel d'utilisateurs, afin de la peaufiner. Elle sera aussi limitée aux possesseurs d'iPhone.

L'ambition de Norauto, grâce à Xee, est de personnaliser sa relation client
À terme, l'application sera étendue à tous les automobilistes possédant un véhicule produit après 2000 – le plus susceptible d'embarquer une prise OBD – ainsi qu'à l'écosystème Android. Dans la mesure où Eliocity propose une plateforme ouverte aux développeurs, il est probable que de nouveaux services viennent enrichir l'application. Car la révision connectée n'est qu'une première étape. Plus tard, Norauto voudrait remonter davantage d'information de chaque véhicule, afin de personnaliser sa relation. Et attirer dans ses centres.

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : http://pro.clubic.com/actualite-e-business/actualite-774146-norauto-inaugure-revision-connectee-boitier-xee.html
Par Thomas Pontiroli

A Guédiawaye (Sénégal), la police démantèle un réseau de ressortissants nigérians | Le Net Expert Informatique

A Guédiawaye (Sénégal), la police démantèle un réseau de ressortissants nigérians

6 ressortissants nigérians ont été interpellés par les éléments de la Brigade de recherches du Commissariat de police de Golf Sud (Guédiawaye). Le matériel qui a été découvert chez eux a permis de conclure que ces derniers s'activaient dans la cybercriminalité, selon le journal Grand Place.

La police de Guédiawaye (Sénégal) vient de démanteler un vaste réseau de cybercriminalité entretenu par des ressortissants nigérians. C'est suite à une information anonyme relative aux agissements répréhensibles de ces derniers que l'agent de police en chef de la commune de Golf Sud a mis sur pied un plan de neutralisation. Ainsi, ses hommes en civil se sont rendus sur les lieux dans la nuit du vendredis 10 juillet, aux environs de 23h, et ont pu arrêter 6 ressortissants nigérians.
Une perquisition de l'immeuble où ils ont été trouvés a permis de mettre la main sur 6 ordinateurs portables de marques différentes. L'exploitation des différents logiciels et autres systèmes des machines a permis la découverte d'installations et de fichiers de comptes bancaires de tiers ainsi que de faux documents étatiques et de réfugiés politiques.
Il y avait aussi plusieurs systèmes sur les ordinateurs portables avec des noms de code permettant à leurs propriétaires d'exercer, en toute discrétion, une activité criminelle.
– L'un permet d'effacer toutes les données après chaque redémarrage de l'outil informatique,
– alors que le deuxième est un système de navigation qui consiste à utiliser Internet sans pour autant être tracé ou repéré par les opérateurs de téléphonie.
– Et le troisième logiciel installé sur la machine ouvre la possibilité aux présumés cybercriminels de pirater les comptes bancaires d'autrui sans laisser des traces.

Source : http://www.leral.net/Cybercriminalite-a-Guediawaye-La-police-demantele-un-reseau-de-ressortissants-nigerians_a149877.html

---

Le site de rencontre Madison Ashley piraté – l'analyse de Kaspersky Lab | Le Net Expert Informatique

Le site de rencontre Madison Ashley piraté – l'analyse de Kaspersky Lab

Le site de rencontres adultères canadien Ashley Madison, qui revendique plus de 37 millions d'inscrits, a été victime d'une attaque informatique ayant pour but de voler les données personnelles d'un grand nombre d'utilisateurs. Ces données ont été brièvement mises en ligne.

Marta Janus, chercheuse en sécurité au sein de l'équipe de recherche et d'analyse (GReAT) du spécialiste en sécurité Kaspersky Lab, revient sur cette attaque :
Marta Janus « L'attaque subie par Madison Ashley nous rappelle à quel point il est important pour toutes les entreprises de mettre en place des mesures de sécurité contre les cyberattaques, afin de protéger les données personnelles de leurs utilisateurs. Un internaute qui accepte de confier certaines de ses données privées à un site web devrait être assuré que ses informations seront conservées de la façon la plus sécurisée qui soit, et les entreprises concernées devraient pouvoir s'y engager.
Il faut également rappeler que toutes les failles de sécurité qui entrainent des fuites de données privées sont un problème, quelles que soit la nature du site visé, sa moralité et même sa légalité. Dans le cas de l'attaque contre Ashley Madison, l'affaire est très sérieuse car la fuite concerne des informations comme les noms, les adresses ou encore les données bancaires. Une fois rendues publiques, ces informations pourraient par exemple être utilisées pour voler de l'argent.
Les raisons pour lesquelles une entreprise peut être victime d'une cyber attaque sont nombreuses – argent, politique ou même éthique. N'importe quelle entreprise peut être la cible d'une attaque et même si les solutions de sécurité réduisent les risques que cette attaque soit fructueuse pour les criminels, d'autres mesures existent pour une protection renforcée. Je pense notamment aux mises à jour logicielles, encore trop souvent remises au lendemain, à la réalisation régulière d'audits de sécurité ou encore au test des infrastructures. Le meilleur moyen de lutter contre ce type de cyberattaques est de se protéger avant qu'elles ne frappent en disposant d'une stratégie de sécurité complète et efficace. »

Source : https://www.globalsecuritymag.fr/Site-de-rencontre-pirate-l-analyse,20150720,54540.html
par Kaspersky Lab

Les Etats Unis devraient avoir peur des prochaines cyber-attaques ? | Le Net Expert Informatique

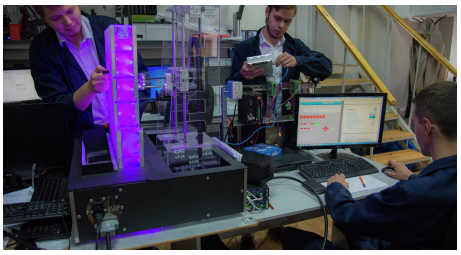
Le nouvel Economiste	Les Etats Unis devraient avoir peur des prochaines cyber-attaques ?

Mercredi dernier, la Bourse de New York et United Airlines ont suspendu leurs activités pendant plusieurs heures en raison de problèmes informatiques mystérieux, tandis que le site Internet du 'Wall Street Journal' a brièvement disparu.

Tous trois ont insisté pour dire qu'il s'agissait de problèmes techniques, et non d'attaques malveillantes. Mais l'inquiétude monte après des agressions contre de puissantes entreprises et agences américaines.
En février dernier, la compagnie d'assurance Anthem révélait que des pirates informatiques avaient volé les données de plus de 80 millions de clients. L'Office of Personnel Management, basé à Washington, révélait que des hackers avaient subtilisé des données de millions d'employés fédéraux. Commerçants ou banques, plusieurs entreprises ont aussi été attaquées.
Mercredi, au moment où la Bourse de New York était suspendue, l'université de Cambridge et le groupe d'assurances Lloyds publiaient un rapport affirmant que si une cyber-attaque s'en prenait au réseau électrique américain, les dommages pourraient s'élever à mille milliards de dollars. Quelques minutes plus tard, le directeur du FBI, James Comey, déclarait devant le Congrès qu'il avait des difficultés à venir à bout des systèmes de chiffrage des djihadistes. En mai, M. Comey expliquait que les terroristes islamiques avaient adopté l'idée d'utiliser des logiciels malveillants contre les infrastructures stratégiques. La chose est plutôt effrayante.
La question clé que les investisseurs, les politiciens et les électeurs doivent se poser est non seulement d'envisager qui pourrait être la prochaine cible, mais aussi de savoir si Washington est capable de face à ces attaques. La réponse est certainement non.
Sur le papier, les ressources ne manquent pas. En début d'année, le président Barack Obama a par exemple affecté 14 milliards de dollars à la lutte contre le cyberterrorisme. Mais le principal problème n'est plus tant un manque d'argent que de coordination : alors que la peur se propage, un nombre ahurissant d'organismes et de groupes de travail différents se sont lancés dans la lutte contre le cyberterrorisme, souvent en collaborant très peu entre eux. L'institution censée être en charge des menaces est le Département de la Sécurité nationale, mais ses compétences laissent sceptiques les responsables militaires. Le Pentagone a son propre personnel affecté aux cyberattaques, tout comme les services secrets.
"Certains pays ont trouvé des réponses : l'Australie possède un niveau impressionnant de coordination entre les secteurs public et privé sur les défenses cybernétiques. Mais avec le tribalisme exacerbé qui sévit à Washington, la triste vérité est qu'il faudra une crise majeure avant que quiconque puisse cogner sur les têtes des bureaucrates de manière efficace"
La Maison-Blanche a tenté d'obliger ces organismes à travailler ensemble. De leur côté, des organismes civils comme la Commission de réglementation nucléaire ont aussi commencé à tenir des réunions discrètes avec d'autres organismes cet automne sur ces questions. Mais la collaboration entre les secteurs reste inégale. "Le niveau de préparation des différents organismes varie énormément" admet un haut responsable de Washington au centre de cette mission. De plus, y ajouter des organismes du secteur privé entraînera une dégradation plus profonde de la situation : non seulement le Pentagone se méfie du partage de données avec d'autres institutions, mais les entreprises sont souvent terrifiées à l'idée de révéler les attaques dont elles ont fait l'objet.
Existe-t-il une solution ? Une réponse sensée pourrait être de créer une nouvelle entité qui serait l'entité centrale de lutte contre le cyberterrorisme. Il existe des précédents, la plupart des régulateurs de Washington ayant été créés pour répondre à une nouvelle menace. La Securities and Exchange Commission, par exemple, a été créée après le krach de 1929 ; la Food and Drug Administration, après des scandales concernant des médicaments dangereux. Une deuxième option serait de relancer le DHS (Department of Homeland Security) afin que celui-ci se focalise sur la lutte contre les cyberattaques. Il pourrait, par exemple, s'appeler ministère de la Sécurité Intérieure et Cybernétique.
Quoi qu'il en soit, Washington a besoin de répondre à la question qu'Henry Kissinger posait pour l'Europe : en temps de crise, "Qui dois-je appeler ?" Certains pays ont trouvé des réponses : l'Australie possède un niveau impressionnant de coordination entre les secteurs public et privé sur la défense cybernétique. Mais avec l'esprit de clan exacerbé qui sévit à Washington, la triste vérité est qu'il faudra une crise majeure avant que quiconque puisse cogner sur les têtes des bureaucrates de manière efficace. Il faut juste espérer que ce "quelque chose" ne sera pas trop dévastateur, comme une attaque réelle des transports ou des marchés.

Source : http://www.lenouveleconomiste.fr/financial-times/les-prochaines-cyber-attaques-contres-les-etats-unis-seront-terribles-27703/
Par David Pilling

Un nouveau système russe contre les cyberattaques industrielles | Le Net Expert Informatique



© PHOTO. INSTITUT D'INGÉNIERIE PHYSIQUE DE MOSCOU

Un nouveau système russe contre les cyberattaques industrielles

L'Université nationale de recherche nucléaire MePhI a conçu un système informatique baptisé Bouclier pour protéger les installations automatiques des entreprises industrielles contre les attaques cybernétiques.

Le système informatique « Bouclier » conçu par les spécialistes de l'Université nationale de recherche nucléaire MePhI pourra être utilisé pour protéger les installations automatiques des entreprises industrielles contre les attaques cybernétiques.
Il sera vendu aux pays membres du groupe des Brics, a déclaré le directeur adjoint du centre d'ingénierie de MePhI (MIFI en russe) Konstantin Mejankov dans une interview accordée à l'hebdomadaire de l'Académie des sciences de Russie Poïsk (Recherche).

La Russie présente une caméra médicale inédite
La protection des systèmes automatisés de contrôle des processus technologiques contre les cyberattaques est considérée comme l'un des principaux problèmes de l'industrie contemporaine. De telles attaques peuvent affecter la chaîne industrielle des entreprises et provoquer des accidents sur les sites, voire des catastrophes anthropiques. Les spécialistes du monde entier cherchent des moyens permettant d'améliorer la protection de l'automation industrielle.
« Les diplômés de la faculté de cybernétique et de la sécurité informatique, ainsi que le Centre de sécurité cybernétique ont participé à ce travail du MePhI. Ils ont créé ensemble le Bouclier qui protège l'automation industrielle de l'accès extérieur non autorisé et des attaques de piratage ou de subversion », explique Konstantin Mejankov.

La Russie relance sa production d'aimants haut de gamme
Il a ajouté que ce système pourrait également être installé sur les oléoducs pour contrôler l'acheminement des hydrocarbures ou encore constater l'apparition de coupures et de fuites.
Le groupe russe InfoWatch, spécialisé dans la sécurité informatique, lance aujourd'hui la vente du système Bouclier aussi bien en Russie qu'à l'étranger, notamment dans les Brics, déclare Konstantin Mejankov. « Par ailleurs, il faut savoir que ce système ne peut pas être transporté dans une boîte et être simplement branché – nos spécialistes se rendent chez chaque client pour diagnostiquer tous les systèmes de l'installation et proposer une solution personnalisée », conclut-il.

Source : http://fr.sputniknews.com/sci_tech/20150718/1017098784.html

Les entreprises attendraient-elles gentiment les attaques ? | Le Net Expert Informatique

Les entreprises attendraient-elles gentiment les attaques ?

Qu’on se le dise : n’importe qui peut se faire attaquer, qu’il s’agisse d’une petite comme d’une grande entreprise.

En 2013, le New York Times a subit une cyberattaque de l’armée électronique syrienne ; un groupe d’activistes soutenant Bachard El Assad. Les auteurs ont ciblé la partie la moins sécurisée du réseau, les serveurs DNS alors qu’ils sont devenus la pierre angulaire de toute applications internes ou externes.
En juin dernier, l’US Army s’est faite attaquée par les mêmes hackers. Et ce, alors même que l’Etat--Major américain avait fait de la cyberdéfense une priorité en investissant fortement. Pourtant, ces deux attaques démontrent qu’ils sont faiblement protégés et que, quelque soit leur taille, toutes les entreprises ou organismes sont des cibles potentielles. Les services informatiques n’ont donc pas su s’adapter à ces nouvelles menaces.
En France, le 1er semestre fut dense en matière de cyberattaques : TV5 Monde, Charlie Hebdo et Thales ont fait l’objet de sévères attaques de leur système informatique. On se souvient que des documents présentés comme des pièces d’identité et des CV de proches des militaires français impliqués dans les opérations contre l’EI avaient été postés sur le compte Facebook de TV5Monde par les pirates.
L’attaque avait été initialement revendiquée par des inconnus se réclamant de Daech (Etat Islamique). L’enquête s’oriente en juin vers des hackeurs russes. Le vol de données semble être le principal objectif des hackers.
Quelques semaines plus tôt, Manuel Valls annonçait que la défense française allait intégrer des community managers et hackers, plus à même de contrer les attaques. Une méthode innovante…. mais est--ce suffisant pour protéger une infrastructure réseau ?

Les entreprises françaises en mal d’inspiration ?
En général, les entreprises ne communiquent pas ou très peu sur leurs attaques. En effet, en regardant de plus près les cyberattaques subies en France, on s’aperçoit que les informaticiens n’ont pas su anticiper les nouvelles menaces. Ils ont préféré sécuriser leurs réseaux grâce à des méthodes utilisées depuis des décennies. Malheureusement, cela ne s’avère plus suffisant pour contrer les nouvelles menaces et les nouvelles techniques utilisées par les hackers.
En parallèle, cela met en exergue les problèmes d’investissement que les entreprises rencontrent et leurs manques de réactions.
Selon une étude menée par IDC [1], si la plupart des organisations sont conscientes des risques de sécurité liés aux serveurs DNS (82 % des répondants étaient conscients des menaces, qu’ils ont reconnues), l’essentiel des budgets en sécurité réseau est encore consacré à des solutions de sécurité plus traditionnelles telles que les pare--feu (68 %).
L’étude d’IDC a également révélé que même si 85 % des répondants disposent des fonctions de sécurité du DNS de base, les entreprises restent vulnérables, car ces fonctions sont généralement inefficaces en cas d’attaque.
Enfin, 73% des entreprises françaises ont subies des attaques sur leurs serveurs DNS mais elles ne sont que 7% à les considérer comme une très grande menace contre 27% aux Etats-- Unis, alors que les dégâts subies lors de ces attaques ont été très importants (vol de données, interruption de service, …).
Sans prise de conscience des responsables informatiques français, les cyberattaques ne cesseront de s’intensifier. Avec la multiplication des appareils connectés à internet, dans tous les domaines d’activités (hôpitaux, grandes administrations ou petites entreprises, dans la banque, l’énergie, la défense,), les données continueront d’avoir de la valeur aux yeux des pirates informatiques si les RSI ne changent pas leurs méthodes de protection.

[1] Enquête IDC sur la sécurité des serveurs DNS, avril 2014

Source : https://www.globalsecuritymag.fr/Les-entreprises-attendraient-elles,20150715,54386.html
par Hervé Dhelin, Directeur Marketing d’EfficientIP

L’attaque par impulsions électromagnétiques des réseaux ferroviaires | Le Net Expert Informatique

	L’attaque par impulsions électromagnétiques des réseaux ferroviaires

De nouveaux capteurs pour faire face aux attaques EM dans le secteur ferroviaire

Virginie Deniau, coordinatrice du projet SECRET, discute des dispositifs mis au point par son équipe afin d'identifier les attaques par impulsions électromagnétiques (EM) et permettre aux opérateurs de passer à un mode sûr.
Il y a onze ans, l'attentat du métro de Madrid a prouvé que le système de sécurité ferroviaire européen n'était pas assez efficace. Mais aujourd'hui où l'équipement ferroviaire (comme dans la plupart des autres industries) est de plus en plus normalisé et connecté, entre autres, un autre type d'attaque plus insidieuse est devenue plus probable: les attaques par impulsions électromagnétiques (EM). Un projet financé par l'UE a mis au point des technologies de détection permettant au secteur de faire face à cette nouvelle menace.
Saviez-vous que bientôt il y aura autant d'appareils connectés que d'êtres humains sur Terre? Cinq milliards de ces appareils sont actuellement opérationnels et ce nombre devrait atteindre les 25 milliards d'ici 2020. Évidemment, chaque nouveau type d'appareil connecté nous rapproche de l'aube des villes intelligentes et de leurs bénéfices attendus. Mais d'un autre côté, comme le montrent les récentes actualités, les pirates informatiques et autres passionnés par la technologie animés de mauvaises intentions représentent une menace croissante pour la sécurité.
Dans le secteur ferroviaire européen par exemple, l'homogénéisation des technologies de réseau et l'utilisation accrue des communications sans fil a rendu très probable le scénario d'une attaque EM. Les brouilleurs de communication sont faciles à utiliser et aisément accessibles à tous grâce à Internet, autrement dit les communications pourraient éventuellement être brouillées, pour notamment provoquer des retards, un blocage ou une déviation des trains.
Pour permettre au secteur de faire face à cette nouvelle menace, le projet SECRET (SECurity of Railways against Electromagnetic aTtacks) a développé un ensemble de sondes de détection capables d'identifier des attaques EM lorsqu'elles surviennent, afin que les opérateurs des équipements ferroviaires puissent passer le réseau à un « mode sûr » inviolable par le type spécifique de l'attaque EM utilisé.
Virginie Deniau, coordinatrice de SECRET, discute la probabilité du scénario d'attaque par impulsions EM, des dispositifs mis au point par son équipe et de la façon dont le secteur aura bientôt besoin de s'adapter à cette nouvelle réalité.

Quelles sont les chances d'un scénario d'attaque EM?
La définition d'une attaque par impulsions EM évolue parallèlement à la multitude des applications de technologies de communication sans fil. Par le passé, les attaques EM découlaient de la production d'interférences à haute tension (Electromagnetic pulse ou micro-ondes haute tension) intentionnelles capables de perturber ou d'endommager l'équipement électronique. Aujourd'hui, ces équipements peuvent être enclenchés par une commande ou une information transmise par des liens sans fil, autrement dit, il est désormais plus facile de perturber les informations transmises et d'endommager l'équipement. Ces attaques nécessitent un signal moins puissant qui peut être généré par des appareils mobiles et autres dispositifs discrets.
Ainsi, d'un point de vue technologique, la probabilité d'une attaque augmente proportionnellement à la vulnérabilité des infrastructures. Il est cependant difficile d'établir une nette probabilité car aujourd'hui il est impossible de faire la distinction entre un défaut technique et une attaque EM. Les attaques EM par un signal de puissance relativement « faible » impliquent des perturbations mais aucun dégât permanent.

Vous avez mentionné les dispositifs mobiles. Cela signifie-t-il que n'importe qui est capable d'effectuer de telles attaques?
La connaissance de la cible est essentielle si l'on veut définir les moyens nécessaires pour effectuer une attaque EM. De nos jours, les brouilleurs de communications publiques peuvent être facilement achetés mais leur puissance et action sont restreintes.
Maintenant, si nous prenons en compte les services de communication professionnels ou de sécurité, il faut des dispositifs spécifiques pour ce genre d'attaques. Ces appareils sont habituellement limités au marché professionnel ou doivent être conçus à partir de zéro. Mais cela nécessite un certain niveau d'aptitudes et de connaissances.
Néanmoins, lorsque ces applications professionnelles sont soutenues par des services publics sans fil, elles peuvent être perturbées par des brouilleurs communs. Cela peut donc poser de nombreux problèmes, et la sécurité et l'importance des services sans fil doivent être sérieusement prises en compte.

SECRET se concentre sur la sécurité ferroviaire. Quelles pourraient-être les conséquences des attaques EM dans ce secteur?
Le principal risque direct est la perturbation du trafic ferroviaire. Il serait possible d'empêcher le départ des trains, de forcer les arrêts de train mais cela provoquerait d'importantes pertes financières et des situations ingérables. Cependant, il est difficile d'évaluer précisément les risques en cascade qui dépendent des caractéristiques de chaque réseau ferroviaire (exploitation, infrastructure, applications, etc.).

Pouvez-vous nous en dire davantage sur les outils que vous avez développés?
La vision de SECRET est que si on est capable de détecter une attaque EM avec certitude, nous pouvons alors tenter de passer à un mode de sécurité ferroviaire parfaitement adapté à la situation et permettant aux opérateurs de regagner le contrôle. Le défi consiste donc à développer des solutions de détection rapide et fiable. C'est dans cet esprit que de nombreuses solutions ont été étudiées dans le cadre de SECRET. Certaines pourraient être mises en œuvre au sein des terminaux de communication et d'autres nécessiteraient des dispositifs dédiés mais offrent l'avantage de suivre divers canaux de communication.
À des fins de résistance, nos capteurs ont été couplés à un terminal d'acquisition et de décision chargé d'analyser les résultats de ces capteurs de détection et de commander une plateforme de télécommunications reconfigurable. D'après les résultats sortants des capteurs, le terminal de décision dirige les messages à transmettre vers le canal de communication le plus résistant à l'attaque EM. Manifestement, cette approche nécessite le déploiement de nombreux réseaux de communication.

Quand prévoyez-vous la commercialisation de la technologie de SECRET?
En raison de la mobilité et du large spectre d'environnements ferroviaires électromagnétiques, la fiabilité et l'absence totale de défauts des solutions de détection est difficile à démontrer à bord d'un train. Néanmoins, lorsque le train est immobile, les technologies de SECRET peuvent être vraiment efficaces. Nous pouvons donc envisager une commercialisation relativement rapide à l'aide de ces technologies afin de protéger les gares et autres infrastructures cruciales.
Parallèlement, les technologies de SECRET peuvent contribuer à l'évolution des normes de télécommunications employées dans les infrastructures critiques. Au lieu d'améliorer la performance en termes de vitesse de données, les normes peuvent évoluer pour fournir des informations en temps réel quant à la qualité des services ou de la présence des signaux brouilleurs (intentionnels ou non-intentionnels). Elles pourraient ensuite fournir un diagnostic pertinent et activer le processus d'intervention adéquat.

Les voies ferrées européennes font déjà l'objet d'une pression économique et sécuritaire importante. Pensez-vous que le secteur peut soutenir les coûts supplémentaires qu'impliquerait la mise en œuvre de solutions de SECRET?

Je pense qu'avec cette menace croissante, il sera nécessaire de garantir la résilience du réseau ferroviaire contre de telles attaques. Habituellement, les systèmes de communication sans fil ne représentent qu'un faible pourcentage du budget d'un projet ferroviaire. Or, ces systèmes sont essentiels dans les plans opérationnels et de sécurité. Les attaques à impulsions EM peuvent avoir des conséquences considérables en termes de coût, et avec un déploiement trop simple, elles peuvent également faire l'objet d'actions malveillantes. Ainsi, une solution contre les attaques EM devrait être envisageant en trouvant un équilibre entre les risques, les impacts et les investissements.

Quels sont vos projets maintenant que le projet touche à sa fin?
Nous aimerions tester notre analyse d'attaques EM avec d'autres types d'attaques telles que les attaques physiques ou les cyber-attaques. En effet, les attaques de brouillage peuvent facilement entraîner d'autres actions malveillantes afin d'empêcher les transmissions vidéo ou d'alarme. Par conséquent, les analyses de risques doivent prendre en compte le risque d'une combinaison d'attaques physiques et de brouillage. Nous pensons également que l'architecture de détection pour les attaques EM proposées dans SECRET devrait être associée à d'autres outils de surveillance de l'infrastructure afin d'obtenir une meilleure vue de ce qui se passe sur le réseau en temps réel.

Pour plus d'informations voir: projet SECRET

Source : http://www.techno-science.net/?onglet=news&news=14158

Les nouvelles technologies guideront bientôt nos virées shopping | Le Net Expert Informatique

Les nouvelles technologies guideront bientôt nos virées shopping

Cintres et miroirs intelligents, clés et porte-monnaie virtuels… Les objets connectés envahissent les centres commerciaux. Ils sont de plus en plus plébiscités par les Français.

Les centres commerciaux, futurs temples ultra connectés? C'est apparemment ce que souhaiteraient les Français. Une enquête* menée par Unibail-Rodamco, le géant de l'immobilier commercial spécialisé dans les centres commerciaux des grandes villes, analyse les comportements des Français en matière de shopping et identifie les tendances de demain. À chaque étape du shopping son innovation. Près de 65% des clients souhaiteraient voir le prix, la taille ou la composition du vêtement s'afficher automatiquement sur le cintre. Plus facile, le shopping.
Une majorité de clients voudrait avoir des conseils personnalisés de la part des vendeurs. Et plus surprenant – à l'heure où l'adoption de la loi sur le renseignement a tant fait polémique – presque la moitié des sondés désire recevoir chez eux des produits suggérés par un service qui analyse leurs données personnelles. L'autre enjeu, très attendu: celui de gagner du temps. Les «serial shoppers» sondés sont 62% à être favorables à l'essayage virtuel en magasin. Et pour cela, l'enseigne Uniqlo a trouvé le filon: le «magic mirror» est relié à une tablette et permet de modifier le coloris du vêtement porté sans avoir à le changer. Dans le même ton, plus de la moitié des Français pensent que les porte-monnaie virtuels seront démocratisés dans les années à venir (Paypal, paiement sans contact etc.). «Aujourd'hui, une clé virtuelle permet même de se faire livrer ses achats dans le coffre de sa voiture», raconte Clémentine Piaza, directrice marketing d'Unibail-Rodamco. Appelée «volvo on call», cette clé sollicitée par 55 % des sondés permet d'ouvrir la voiture uniquement pendant le laps de temps défini avec l'acheteur pour charger le coffre.

Expérience collective
Le centre commercial demeure le lieu de shopping privilégié des Français, et plus de 70% des hommes y vont accompagnés, selon l'étude. «L'époque du consommateur individualiste et narcissique est désormais révolue car il est maintenant à la recherche, à travers le shopping, d'une expérience durant laquelle il retrouve un moment commun, un engagement,une appartenance à un groupe de référence», analyse Stéphane Hugon, Docteur en sociologie, chercheur au Centre d'Etudes sur l'Actuel et le Quotidien.
Service de géolocalisation pour retrouver ses amis présents dans le centre, échanges de photos facilités ou café conçu pour partager une expertise et des conseils à l'image de DimensionAlley à Berlin, tout est pensé pour répondre à «un besoin de connexion permanent». Deux tiers des sondés rêvent enfin d'espaces plus aérés intégrant verdure et silence, mais aussi d'espaces vivants et animés. D'une sorte de ville nouvelle à la pointe de la technologie. À l'image du nouveau centre SuperPier à Manhattan, qui ouvrira ses portes cet été.
*La 3ème édition de L'Observatoire du Shopping Unibail-Rodamco a été menée auprès de 2006 individus constituant un échantillon représentatif de la population française âgée de 16 à 70 ans. Le recueil des données a été réalisé du 16 au 23 mars 2015, via l'Access Panel Online d'Ipsos, utilisant la méthode des quotas (âge, profession de la personne interrogée, région et catégorie d'agglomération).

Source : http://www.lefigaro.fr/conso/2015/07/11/05007-20150711ARTFIG00007-les-nouvelles-technologies-guideront-bientot-nos-virees-shopping.php

Cinq technologies de cyberespionnage utilisées sans connexion à Internet | Le Net Expert Informatique

Un système connecté à Internet est toujours sujet à des menaces, et ce quel que soit son niveau de protection. De nos jours, tous les adolescents en ont parfaitement conscience. Aucun logiciel de protection ne peut éviter complètement les erreurs humaines dans les codes de programmation ou empêcher des comportements d'utilisateur.

C'est pourquoi, en général, les appareils dont les fonctions sont spécialement importantes ou dont le contenu est top secret ne sont pas connectés à Internet. Il est toujours préférable d'accepter un inconvénient plutôt que de faire face à des conséquences fâcheuses. C'est de cette manière que sont protégés, par exemple, les systèmes de contrôle de gros objets industriels ou les ordinateurs de certaines banques.
Une déconnexion permanente semblerait être la meilleure solution pour garder des données secrètes : s'il n'y a pas d'Internet, alors il ne peut pas y avoir de fuite de données. Or, ce n'est pas vrai. Les techniques de transfert de données à distance, adoptées depuis longtemps par les services secrets, deviennent chaque année plus accessibles aux utilisateurs " commerciaux ".A présent, il est de plus en plus habituel de rencontrer certains gadgets d'espionnage que James Bond possédait.

Espionnage électromagnétique
Tout appareil connecté à une ligne de courant génère des émissions électromagnétiques qui peuvent être interceptées par des technologies éprouvées. Il y a près de cinquante ans, les services de sécurité des Etats-Unis et de l'URSS étaient impliqués dans de telles fuites. La quantité d'informations obtenues depuis lors est énorme. Une partie des activités menées par les Etats-Unis est connue sous le nom de code TEMPEST, et certaines affaires déclassifiées sont aussi passionnantes que des romans policiers.

Autrefois, les écrans à tube cathodique et les connecteurs VGA sans protection étaient les maillons les plus faibles. Ces dernières années, les claviers sont devenus les jouets favoris des chercheurs en protection des données.
Bien que beaucoup de temps se soit écoulé, de nouvelles méthodes pour " surfer " sur des ondes électromagnétiques apparaissent à mesure que les équipements électriques évoluent. Autrefois, les écrans à tube cathodique et les connecteurs VGA sans protection constituaient les maillons les plus faibles qui produisaient du bruit électromagnétique. Ces dernières années, les claviers sont devenus les jouets favoris des chercheurs en protection des données. Les recherches effectuées dans ce domaine portent régulièrement leurs fruits. En voici quelques exemples.
Les frappes peuvent être tracées avec haute précision par un appareil artisanal placé à vingt mètres, qui analyse le spectre radioélectrique et qui coûte 5 000 dollars. Il est intéressant de savoir qu'une attaque est aussi efficace si elle vise des claviers USB de premier prix, des claviers sans fil avec chiffrement du signal plus chers, ou encore des claviers intégrés à des ordinateurs portables.
Tous ces appareils fonctionnent de la même manière et génèrent du bruit électromagnétique. La seule différence réside dans la puissance du signal, qui dépend de la longueur de la ligne de transmission de données (par exemple, elle est plus courte avec des ordinateurs portables).
Tous ces appareils fonctionnent de la même manière et génèrent du bruit électromagnétique. La seule différence réside dans la puissance du signal, qui dépend de la longueur de la ligne de transmission de données (par exemple, elle est plus courte avec des ordinateurs portables).

Les données peuvent être plus facilement interceptées si l'ordinateur visé est relié à une ligne de courant. Les variations de tension, qui correspondent aux frappes, génèrent du bruit électromagnétique au niveau du sol. Ce bruit peut être intercepté par un hacker qui est connecté à une prise de courant proche. Le prix de l'équipement, avec une portée effective de 15 mètres, est de 500 dollars.

Comment contrecarrer cette menace ? La meilleure manière de se protéger contre l'espionnage électromagnétique serait de sécuriser une pièce (cage de Faraday) et d'utiliser des générateurs de bruits spéciaux. Si vos secrets ne sont pas si précieux, et si vous n'êtes pas prêts à recouvrir les murs de votre sous-sol avec de l'aluminium, alors vous pouvez simplement utiliser un générateur de bruit " manuel " : taper des caractères inutiles de manière sporadique et les effacer ensuite. Pour saisir des données précieuses, vous pouvez utiliser un clavier virtuel.

Cinq technologies de cyberespionnage utilisées sans connexion à Internet
1. Faites attention aux lasers
Il existe des méthodes alternatives d'enregistrement de frappes. Par exemple, l'accéléromètre d'un smartphone, posé près d'un clavier, présente un taux de reconnaissance d'environ 80%. Ce taux n'est pas suffisamment élevé pour intercepter des mots de passe, mais il permet de déchiffrer le sens d'un texte. Cette méthode compare les différentes vibrations produites par les paires de signaux successifs qui correspondent aux frappes.
Un rayon laser, discrètement dirigé vers un ordinateur, constitue la méthode la plus efficace pour enregistrer les vibrations. D'après les chercheurs, chaque frappe produit ses propres vibrations. Le laser doit être dirigé vers une partie d'un ordinateur portable ou d'un clavier qui réfléchit bien la lumière. Par exemple, vers le logotype du fabriquant.
Comment contrecarrer cette menace ? Cette méthode ne fonctionne que si le rayon laser est proche. Par conséquent, essayez de ne pas vous laisser approcher par des espions.

2. Ecouter la radio
Il n'est pas toujours utile d'intercepter les données d'un clavier, puisque cela ne donne évidemment pas accès à la carte mémoire d'un ordinateur. Cependant, il est possible d'introduire un malware dans un ordinateur déconnecté par des moyens externes. C'est de cette façon que le célèbre ver Stuxnet s'est infiltré dans un ordinateur cible au sein d'une infrastructure d'enrichissement de l'uranium. Après l'infection, le malware a fonctionné comme un espion infiltré, " aspirant" des informations grâce à un certain support physique.
Par exemple, les chercheurs israéliens ont développé un software qui module les émissions électromagnétiques dans le hardware des ordinateurs. Ces signaux de radio sont puissants et peuvent même être captés par des récepteurs FM standards de téléphone.
Pourquoi une telle complexité ? Les ordinateurs qui comportent des données classifiées sont placés dans des pièces sécurisées, et leur accès est limité afin d'éviter toute fuite possible. Cependant, contrairement à un analyseur de spectre, un téléphone espion peut être facilement introduit dans de telles pièces.
Comment contrecarrer cette menace ? Tous les téléphones, ainsi que tous équipements suspects, doivent rester à l'extérieur des pièces sécurisées.

Tiède… Chaud… Brûlant !
Récemment, les chercheurs israéliens que nous avons déjà mentionnés ont exposé un scénario de vol de données un peu plus exotique… par le biais d'émissions thermiques !
Le mode opératoire de l'attaque est le suivant. Deux ordinateurs de bureau sont placés l'un à côté de l'autre (environ 40 centimètres les séparent). Les capteurs thermiques de la carte mère interne de l'un de ces ordinateurs pistent les changements de température de l'autre.
Le malware change périodiquement la température du système en ajustant le niveau de charge et envoie un signal thermique modulé
Par commodité, un ordinateur déconnecté est souvent placé juste à côté d'un ordinateur connecté à Internet, et ce n'est que la stricte vérité. L'ordinateur déconnecté comporte des données classifiées, tandis que l'autre est un simple ordinateur connecté à Internet.

Si quelqu'un introduit un malware dans ces deux systèmes, voici ce qui se produit. Le malware lit les données classifiées, puis change périodiquement la température du système en ajustant le niveau de charge et envoie un signal thermique modulé. Le deuxième ordinateur reçoit et déchiffre ce signal, avant d'envoyer les données classifiées par Internet.

L'inertie thermique du système empêche une transmission rapide des données. La vitesse de transmission est alors limitée à huit bits par heure. A ce rythme, il est possible de dérober un mot de passe, mais le vol d'une base de données est remis en question.

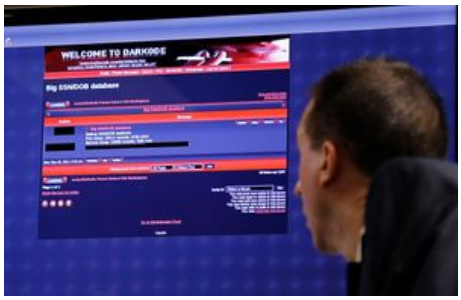
Toutefois, avec le succès que rencontrent les gadgets connectés à Internet, le rôle du deuxième ordinateur, qui aspire les données, peut facilement être rempli par une climatisation intelligente ou un capteur climatique, lesquels enregistrent les changements thermiques avec beaucoup de précision. Le taux de transfert pourrait augmenter de manière significative dans un futur proche.
Comment contrecarrer cette menace ? Ne placez pas un ordinateur déconnecté, qui comporte des données classifiées, à côté d'un ordinateur connecté à Internet.

Toc, toc, toc. Qui est là ?
Une pièce bien sécurisée classique n'assure pas une protection complète contre les fuites de données. Les murs en acier sont imperméables au bruit électromagnétique, mais pas aux ultrasons.
Dans le cas d'une technologie à ultrasons, un équipement espion se compose de deux unités compactes. L'une d'elles est discrètement placée à l'intérieur d'une pièce sécurisée, tandis que l'autre est placée quelque part ailleurs. Le taux de transfert de données à travers l'acier pour les ultrasons atteint 12 MB/s. En outre, l'une des unités n'a pas besoin d'être chargée car l'énergie est transmise en même temps que les données.
Comment contrecarrer cette menace ? Si vous possédez votre propre pièce sécurisée avec des murs en acier, alors vous devriez vérifier minutieusement chaque équipement qui y est installé.
En général, connaître les techniques modernes d'espionnage (" modernes " du moins aux yeux du grand public) vous permet de conserver vos données intactes. Sur le plan logiciel, une solution de sécurité élevée est indispensable.

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : https://blog.kaspersky.fr/when-going-offline-doesnt-help/4607/

Le forum de pirates Darkode est tombé après une opération menée par le FBI | Le Net Expert Informatique

	Le forum de pirates Darkode est tombé après une opération menée par le FBI

Sous la supervision du FBI , le forum Darkode, qui constituait un point de rendez-vous majeur des pirates pour mener des cyber-attaques, est tombé.

C'est la fin du forum dédié au piratage par lequel il était possible d'acheter, de vendre, de monnayer et de partager des informations ou des outils favorisant des cyber-attaques.
Il a fallu que le FBI s'infiltre dans ce monde underground pour en connaître les coulisses d'administration.
Un accès était uniquement possible par cooptation sous le contrôle des gestionnaires de Darkode : on recensait plusieurs centaines de membres (entre 250 et 300 selon LeMonde.fr).
Mais tout postulant devait démontrer au préalable ses « talents » c'est-à-dire ses capacités à alimenter les ressources malware diffusées via Darkode.
Selon les autorités américaines, des mandats d'arrêt concernant une douzaine de personnes présumées en charge de l'administration de Darkode ont été émis dans trois districts, mais en tout, on évoque 70 membres de Darkode interpellés ou recherchés dans le monde.
Une vingtaine de pays ont été associés à la coupure de ce forum qui entre dans une opération plus large contre la cyber-criminalité baptisée « Shrouded Horizon » : outre les Etats-Unis, on trouve des pays comme l'Australie, le Royaume-Uni, le Brésil, le Canada, la Colombie, la Croatie, le Nigéria, l'Allemagne ou Israël.
« Sur les 800 forums dédié à la criminalité sur Internet, Darkode représentait l'une des plus graves menaces à l'intégrité des données informatiques aux Etats-Unis et dans le monde », déclare David Hickton, procureur fédéral pour le district Ouest de Pennsylvanie, cité dans le communiqué du ministère de la Justice.

A travers le centre anti-cyberciminalité EC3, l'Europe était dans la boucle.
Europol a précisé de son côté que l'opération menée sous la supervision du FBI a abouti à 28 arrestations, 37 perquisitions et un nombre important de saisies de matériel informatique susceptibles d'abriter des preuves et des données pour pousser l'enquête encore plus loin.

Source : http://www.itespresso.fr/darkode-fbi-fait-tomber-forum-ombre-102787.html
Par Philippe Guerrier