La Marine Américaine reprend la navigation céleste | Le Net Expert Informatique

	La Marine Américaine reprend la navigation céleste

Face à la menace croissante des cyberattaques, l'US Navy repasse au sextant qui fait ainsi son retour dans l'armée la plus moderne au monde.

Après près de 20 ans d'interruption, l'Académie navale américaine d'Annapolis (Maryland) recommence à former ses aspirants à la navigation astronomique, vu le danger de plus en plus imminent des cyberattaques, rapporte le Washington Post.

« Nous nous sommes entièrement informatisés, en renonçant au sextant en faveur des ordinateurs qui sont vraiment excellents. Le problème, c'est qu'il n'y a plus de solution de secours », a déclaré au journal le lieutenant-colonel Ryan Rogers, titulaire de la chaire de navigation à l'Académie.

Le bon vieux sextant fait son retour dans l'armée la plus moderne au monde, car cet instrument restera fiable en cas de cyberattaque. La réintroduction du sextant marque en quelque sorte la fin de la croyance en l'infaillibilité technologique.

L'été dernier, les aspirants de l'Académie d'Annapolis ont commencé à recevoir trois heures de cours hebdomadaires. La promotion 2017 sera la première à avoir des rudiments dans l'utilisation du sextant.

Dans le contexte des scandales d'espionnage informatique qui défraient la chronique depuis un certain temps avec les révélations sur l'activité de l'agence américaine NSA, bien des pays, dont la Russie, envisagent un retour aux vieilles méthodes.

Les spécialistes soulignent que du point de vue de la sécurité, toute sorte de communication électronique est vulnérable. On peut capter n'importe quelle information depuis un ordinateur, il existe des moyens de protection, mais sans garantie à 100 % de leur sûreté. Pour garder des secrets, la « méthode primitive » est préférable: la main humaine avec un stylo ou la machine à écrire.

Source :

http://fr.sputniknews.com/international/20151017/1018907696/usa-marine-sextant-cyberattaques.html

Le hack étonnant qui peut tromper Siri, Cortana et Google Now grâce aux ondes radio | Le Net Expert Informatique

	Le hack étonnant qui peut tromper Siri, Cortana et Google Now grâce aux ondes radio

Deux hackers français ont montré qu'il était possible d'injecter des commandes vocales par l'émission d'ondes radioélectriques. Mais cette attaque nécessite quand même un peu de matériel.

Les assistants vocaux sont bien pratiques et déployés sur pratiquement tous les smartphones aujourd'hui, qu'il s'agisse de Siri pour iOS, de Google Voice pour Android ou de Cortana pour Windows 10 Mobile. Mais ces interfaces présentent des vulnérabilités que deux chercheurs en sécurité de l'ANSSI – José Lopes Esteves et Chaouki Kasmi – ont mis en lumière dans un article publié par le magazine scientifique IEEE Electromagnetic Compatibility. Ils ont également présenté leurs recherches en juin dernier, à l'occasion de la conférence académique SSTIC, qui s'était déroulée à Rennes.

Les deux chercheurs ont montré qu'il était possible d'injecter des commandes vocales dans ces systèmes par l'intermédiaire d'ondes radio. Comment? Au travers des écouteurs du kit mains-libres. « Le câble des écouteurs est une bonne antenne pour des fréquences comprises entre 80 et 108 MHz », explique José Lopez Esteves, dans la vidéo de leur présentation SSTIC. L'idée du hack est donc d'enregistrer une commande vocale, de la moduler en amplitude sur une onde porteuse de la bande 80-108 MHz et de l'envoyer vers les écouteurs. Ce rayonnement va induire dans le câble un signal électrique qui va automatiquement être traité par le système de commandes vocales, après avoir été filtré et amplifié. Au final, « on obtient un signal relativement proche du signal vocal original », précise M. Lopes Esteves.

Cette attaque fonctionne avec tous les principaux systèmes vocaux disponibles, à savoir Cortana, Siri et Google Voice. Il y a néanmoins une condition nécessaire, c'est que la commande vocale soit activée, c'est-à-dire que l'on puisse interroger l'assistant virtuel par un simple mot-clé (« OK Google », « Dis Siri » ou « Hey Cortana »), ce qui n'est pas une option par défaut sur les smartphones.

L'impact de l'attaque dépendra de l'état du téléphone. Il sera maximal s'il est déverrouillé. L'assistant vocal pourra alors accéder au carnet d'adresse, envoyer un message, ouvrir une page web, lancer une application, etc. « On pourra par exemple envoyer une commande pour que l'appareil ouvre un site web malveillant », souligne M. Lopes Esteves. Le mieux dans cette affaire, c'est que l'utilisateur pourrait ne rien remarquer du tout car la commande vocale injectée est totalement silencieuse pour lui. Seul l'assistant vocal l'entendra.

Limité à quelques mètres

En revanche, si le téléphone est verrouillé, l'assistant vocal n'aura qu'un accès limité, comme par exemple interroger l'appli météo ou appeler un numéro. Ce qui n'est pas rien quand même, car il est possible alors de passer des coups de fil en douce pour générer des revenus frauduleux (via des numéros surtaxés) ou pour simplement espionner les conversations environnantes.

Si ce piratage est relativement simple sur le principe, il nécessite quand même du matériel. Avec un équipement radio de la taille d'un sac à dos, le rayon d'action est de seulement deux mètres. Pour atteindre cinq mètres, il faut déjà une camionnette. Et dans ce cas, mieux vaut ne pas se trouver à proximité de l'émetteur, car le niveau de rayonnement sera alors plutôt intense.

Source :
http://www.01net.com/actualites/siri-cortana-et-google-voice-sont-vulnerables-aux-attaques-radio-922670.html
Par Gilbert KALLENBORN

La stratégie du gouvernement pour la sécurité du numérique | Le Net Expert Informatique

La stratégie du gouvernement pour la sécurité du numérique

Le gouvernement a présenté vendredi sa stratégie pour la sécurité du numérique, un document qui fait la synthèse des différentes mesures en place pour lutter contre les hackers et protéger la vie numérique des citoyens, et met l'accent sur la formation.

Les « cyberattaques sont susceptibles de désorganiser des activités vitales de notre pays, de déstabiliser des entreprises, de vampiriser leur savoir-faire », a souligné le Premier ministre Manuel Valls, évoquant comme conséquence directe « la destruction de nombreux emplois, de valeur industrielle et culturelle ».
« Les citoyens sont également exposés, que ce soient des tentatives d'escroquerie, qui s'accompagnent parfois de chantage, ou la captation de données personnelles », a-t-il remarqué.
Le document de 40 pages présenté vendredi par le chef du gouvernement, vient remplacer un premier « pensum » publié début 2011, et mis à jour car « la donne a fondamentalement évolué (…) en quatre ans, parce que le monde va très vite ».
La menace est polymorphe, venant tout aussi bien de petits escrocs, de groupes mafieux, d'islamistes radicaux ou encore de services étrangers –y compris alliés.
La spectaculaire attaque, en avril, de la chaîne francophone TV5Monde, a donné toute la mesure du danger. Car les hackers ne chôment pas, comme l'a rappelé le directeur général de l'Agence nationale de la sécurité des systèmes d'information (Anssi, chargée depuis 2009 de coordonner la défense française face aux cybercriminels), Guillaume Poupaud.
« Des attaques du niveau de TV5, on en a tous les quinze jours », a-t-il indiqué à des journalistes. « Seulement, ce n'est pas du sabotage, mais de l'espionnage », moins spectaculaire.

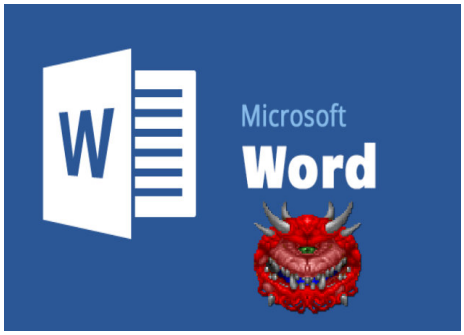
– Sensibiliser, former, informer –

L'une des idées fortes est donc logiquement de **renforcer la défense contre les cybermenaces** en consolidant la sécurité numérique de ses infrastructures, à commencer par les entreprises vitales au pays.
Et on va **sensibiliser les Français aux menaces du cyberespace**, dès l'école. Former. Informer.
« On n'imagine plus des constructeurs automobiles proposer des véhicules sans freins et sans ceintures de sécurité. Mais aujourd'hui, sur ce qu'on appelait les autoroutes de l'information, la plupart des voitures sont sans freins et sans ceintures de sécurité », a relevé Guillaume Poupaud, qui s'étonne de voir des gens « parcourir ces autoroutes de l'information à vélo, et sans casque, alors que des poids lourds passent à côté ».
La stratégie gouvernementale présentée vendredi est « un bon équilibre entre la prise en compte de la sécurité et dynamisme économique » et un « bon équilibre entre sécurité et liberté », a jugé Manuel Valls.
Le chef du gouvernement s'en est d'ailleurs pris à la « position caricaturale » de ceux qui opposent « le numérique », qui devrait être le monde de la liberté absolue, à la +sécurité+, qui se traduirait nécessairement par une restriction dangereuse des libertés fondamentales ». Une position observée selon lui lors du débat sur la loi sur le renseignement.
Si cette loi dote les services de renseignement de moyens de surveillance des citoyens, le gouvernement « reste favorable » à ce que les acteurs privés « continuent de bénéficier pleinement » de « toutes les ressources qu'offre la cryptologie légale », a relevé M. Valls.
Des dirigeants des principaux opérateurs internet français –Bouygues Telecom, Free, Orange, La Poste et SFR-Numericable– ont même signé dans la foulée une charte les engageant à crypter les courriels de leurs clients circulant entre leurs serveurs, afin de pallier une grande faiblesse de la sécurité informatique.
Le gouvernement, qui a fait de la protection de la vie numérique des citoyens un objectif majeur, entend aussi les aider en cas de problème, avec notamment la création l'an prochain d'un « **dispositif national d'assistance » aux victimes d'actes de cybermalveillance**, pour les PME et les particuliers (des procédures étant déjà en place pour les institutions de l'Etat et les grandes entreprises).
Un groupe d'experts doit également être constitué pour mieux faire émerger les nouvelles technologies de sécurité informatique et améliorer les formations dans l'enseignement supérieur.
Enfin, la stratégie française vise aussi à muscler une filière déjà dynamique. Car la lutte contre les cyber-criminels est un secteur d'avenir.

Denis JACOPINI est Expert Informatique, conseiller et formateur en entreprises et collectivités et chargé de cours à l'Université.
Nos domaines de compétence :
• **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
• **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
• **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.
Contactez-nous

Source :
http://www.leparisien.fr/flash-actualite-politique/cybersecurite-valls-presente-la-strategie-de-la-france-16-10-2015-5191401.php#xtref=https%3A%2F%2Fwww.google.com%2F

Alerte Ransomware : Attaque massive dans le doc | Le Net Expert Informatique



Alerte Ransomware : Attaque massive dans le doc

Depuis ce mardi matin, des milliers de courriers malveillants visent entreprises et collectivités locales françaises. Prudence !

Ils se font passer pour des fax en attente ou pour un communiqué de presse. Ils sont cachés dans des courriels publiés ce mardi matin, dans une diffusion massive et malveillante. ZATAZ.COM a pu en référencer 300 différents, en quelques minutes. Des courriers électroniques contenant des pièces jointes qu'il ne faut surtout pas ouvrir. Des fichiers Word, PowerPoint piégés. Ils vont chercher sur la toile un code malveillant qui, dans la majorité des cas, était un ransomware ou encore le code pirate Dridex.

Dridex, est un outil qui exploite la technologie du peer-to-peer (P2P) afin d'attaquer le contenu des ordinateurs infiltrés. Mission, mettre la main sur des données bancaires. Le département américain de la Sécurité intérieure (DHS), en collaboration avec le Federal Bureau of Investigation (FBI) et le ministère de la Justice (DOJ) ont publié une alerte quelques heures après l'annonce de ZATAZ, preuve que cette diffusion massive est à échelle internationale.

Dridex est un ensemble de logiciels malveillants multifonctionnel qui exploite le langage Macro proposés dans les outils de Microsoft. L'objectif principal de Dridex est d'infecter les ordinateurs, voler des informations d'identification, et obtenir l'argent des comptes bancaires des victimes infiltrées. Exploitée principalement comme un cheval de Troie bancaire, Dridex est généralement distribué par courrier électronique, comme le cas de ce lundi matin.

Un système infecté par Dridex peut être utilisé pour envoyer du spam, participer à DDoS… la question est de savoir pourquoi une telle attaque, en pleine semaine. Le bot des pirates a-t-il été mis en action car le besoin en données bancaires se fait sentir chez les malveillants après les dernières importantes arrestations dans le monde du carding international ?

Microsoft propose un outil pour scanner votre ordinateur à la recherche du malveillant code : http://www.microsoft.com/security/scanner/en-us/default.aspx

---

Denis JACOPINI est Expert Informatique, conseiller et formateur en entreprises et collectivités et chargé de cours à l'Université.

Nos domaines de compétence :

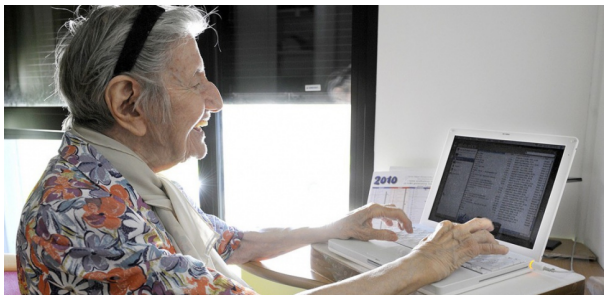
- **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
- **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
- **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.

Contactez-nous

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

Source : http://www.zataz.com/attaque-massive-ransomware-dans-le-doc/
Par Damien Bancal

Pas assez connectée pour être menacée ? Madame Walsh s’est pourtant fait pirater | Le Net Expert Informatique



Pas assez connectée pour être menacée ? Madame Walsh s’est pourtant fait pirater

Le piratage, ça n'arrive pas qu'aux autres. Et il n'y a pas besoin d'être ultra-connecté pour en être victime. C'est ce que raconte le « New York Times », avec l'exemple de Madame Walsh, vivant en Californie.

Cette grand-mère de six petits-enfants a accepté de servir de cobaye à deux hackeurs, se pensant à l'abri, puisque n'étant pas quelqu'un de « connecté ».
Mme Walsh explique ne disposer d'aucun objet connecté (montre, etc.), sa maison n'est équipée d'aucun appareil technologique récent (thermostat connecté ou autre), et elle n'est pas une grande adepte des gadgets électroniques. Bien sûr, elle dispose d'un compte Facebook, mais n'y publie jamais rien, et s'en sert uniquement pour rester en contact avec des amis. Et pourtant.

E-mail, PaylPal, télévision et garage piratés

Les hackeurs ont bien réussi à pirater Madame Walsh. Le quotidien raconte que les pirates ont successivement testé plusieurs pistes pour tenter de s'attaquer à la grand-mère. Si son compte Facebook se révèle bien protégé, la découverte d'un « J'aime » pour une page de la plateforme de pétitions Change a été le déclic.
Dix minutes plus tard, les hackeurs adressent à Mme Walsh un faux e-mail émanant de Change.org proposant de signer une fausse pétition. Bingo, la grand-mère clique, et entre son identifiant et son mot de passe. La voilà victime de « phishing ».
Madame Walsh confesse au « New York Times » utiliser le même mot de passe sur l'ensemble des services internet. Les pirates sautent sur la brèche et s'introduisent dans sa messagerie e-mail pour récupérer ses données de sécurité sociale et d'assurance maladie, et de ses comptes PayPal et Miles.
Pis, les hackeurs s'introduisent également dans le compte e-mail de sa fille, dont le code était « caché » dans un message. Enfin, ils laissent sur l'ordinateur de Mme Walsh un virus qui enregistre tout ce qui est tapé et remplace les publicités des sites visités afin de leur générer des revenus.
Pas repus, les deux hackeurs se sont attaqués à sa maison. En une heure et demie, ils ont pris le contrôle de sa télé (l'installateur du câble n'avait pas protégé la connexion) et trouvé un moyen d'ouvrir à distance la porte de son garage (via un procédé de « brute force » qui a essayé des centaines de combinaisons possibles avant de tomber sur la bonne pour la porte électrique).

Le phishing, risque numéro un

L'exemple du « New York Times » est extrême mais illustre bien que personne n'est à l'abri d'un piratage, même ceux qui se pensent « trop peu connecté pour être en danger ». Et le risque premier demeure le phishing, aussi appelé hameçonnage.
Aujourd'hui, plus de 90% des attaques dans le monde démarrent par un e-mail de phishing », affirme Ismet Geri, directeur général pour la France et l'Europe du Sud de Proofpoint, société spécialisée dans la sécurité des e-mails.
Un e-mail sur 392 serait une tentative de phishing, estime l'entreprise de sécurité informatique Symantec dans son dernier rapport. Au total, 37,3 millions d'internautes sont tombés dans le panneau dans le monde, affirme une enquête de la société de sécurité Kaspersky. La France se classe septième pays au monde dans les victimes avec un internaute sur 30 floué.

LIRE »J'ai cliqué » : chronique d'un phishing ordinaire

L'objectif des pirates est simple : récupérer des coordonnées bancaires, mais aussi des informations personnelles. Selon Symantec, au marché noir, les détails d'une carte de crédit se revendent entre 0,50 et 20 dollars, un passeport scanné 1 à 2 dollars, l'accès à un compte cloud 7 à 8 dollars, l'accès à un compte de jeux vidéo en ligne 10 à 15 dollars, etc.
L'utilisation de ces données est évidente. Les données bancaires permettent d'effectuer des achats en ligne, tandis que les informations personnelles vont permettre de s'identifier sur l'ensemble des services. Surtout que le sésame identifiant/mot de passe devient un Graal, quand on sait que 75% des Français utilisent toujours le même mot de passe.
Je m'estimais plutôt malin, je m'étais trompé ! », a confié le blogueur Thomas Messias au « Parisien » après un piratage de ses comptes. « Evidemment, j'utilisais le même mot de passe pour eBay et pour tous les autres sites… »
Voilà Madame Walsh prévenue. Et pour ce qui est de la maison, de nombreux experts en informatique démontraint régulièrement comment prendre le contrôle d'objets usuels. Cet été, le hackeur Samy Kamkar a démontré comment ouvrir des portes de garage à partir d'un jouet Mattel en moins de 10 secondes :

Denis JACOPINI est Expert Informatique, conseiller et formateur en entreprises et collectivités et chargé de cours à l'Université.
Nos domaines de compétence :
• **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
• **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
• **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.
Contactez-nous

Source :
http://tempsreel.nouvelobs.com/tech/20151015.OBS7721/pas-assez-connectee-pour-etre-menacee-madame-walsh-s-est-pourtant-fait-pirater.html#xtor=EPR-1-ObsActu8h-20151016

Encore une faille 0-day sur Flash Player menaçant vos ordinateurs | Le Net Expert

Informatique

Encore une faille 0-day sur Flash Player menaçant vos ordinateurs

Ces derniers mois, Flash Player a subi les foudres de grands noms de l'informatique suite à de nombreuses vulnérabilités découvertes en plus des innombrables précédentes corrigées auparavant. Déjà alors, certaines institutions comme Facebook réclamaient l'abandon du plug-in Flash alors cet aveu issu de la société de développement Adobe ne risque pas d'arranger le sort de son Flash Player.

Un rapport publié par la société Adobe a été publié mercredi et confirme la présence d'une faille critique au sein de la dernière version du Player mais aussi des précédentes. Celle-ci peut être employée « lors d'attaques limitées et ciblées ». Sont concernées les dernières versions,19.0.0.207 incluse mais également toutes les précédentes itérations sur Windows et Mac, Adobe Flash Player Extended Support Release pour l'intégralité des versions 18 ainsi que les versions pour Linux.

En plus des vulnérabilités 0-day employés par la Hacking Team, cette faille avait été décelée au cours de l'été par TrendMicro qui mettait alors au jour une attaque informatique de grande envergure orchestrée par le groupuscule Pawn Storm, pirates visant différents ministères des affaires étrangères à travers le monde ainsi que certains média.

Si cette attaque reposait principalement sur l'utilisation de malwares, des méthodes de phishing et exploitait une faille inhérente à Java (la première repérée depuis des années), le magazine spécialisé a par la suite découvert que les hackers s'appuyaient aussi sur une faille présente dans Flash Player.

Confirmée par Adobe, celui-ci a aussitôt assuré se mettre à l'élaboration d'un correctif. Initialement prévu pour une distribution au 16 octobre, ce patch devrait finalement être disponible vers le 19 du même mois. Reste que la plus sûre des solutions en attendant sa mise à jour consiste à désinstaller complètement le lecteur. Si la faille ne concerne pas directement la personne lambda mais principalement les hautes institutions, le principe d'action pourrait tout de même être repris par d'autres pirates et appliqués à une plus grande partie de la population. Prudence.

Denis JACOPINI est Expert Informatique, conseiller et formateur en entreprises et collectivités et chargé de cours à l'Université.

Nos domaines de compétence :

• **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;

• **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;

• **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.

Contactez-nous

Cet article vous plait ? Partagez !

Un avis ? Laissez-nous un commentaire !

Source :

http://www.phonandroid.com/flash-player-encore-faille-0-day-menacant-ordinateurs.html

Oups ! Uber dévoile les données personnelles de chauffeurs | Le Net Expert Informatique

Oups ! Uber dévoile les données personnelles d

Un bug permettait de voir les données personnelles d'autres chauffeurs Uber. La société assure que seuls 700 conducteurs US ont été affectés et que la faille a été corrigée en seulement 30 minutes.

Uber l'assure, ses services sont bons pour l'économie et créent de l'emploi – pas salarié cependant, les chauffeurs ne signant pas de contrat de travail avec la multinationale. En France, la société a dû faire face au mécontentement, et pas des taxis cette fois, mais des chauffeurs eux-mêmes. La faille de sécurité dont a été victime cette semaine le service devrait probablement moins affecter ces travailleurs que la diminution tarifaire imposée par Uber. La société a ainsi, accidentellement, divulgué les données personnelles de plusieurs centaines de chauffeurs.

Un bug de débutant, mais des conséquences mineures

Cette fuite de données est la conséquence d'un bug logiciel. Elle a abouti à la divulgation de l'identité de conducteurs Uber, dont leurs numéros de sécurité sociale, parmi d'autres données sensibles. En enregistrant des documents d'assurance auprès d'Uber, des chauffeurs ont constaté que s'affichaient les informations d'autres utilisateurs de la plateforme.

Mais pas de panique, assure la société américaine. Selon cette dernière, qui a notamment été interrogée par The Register, moins de 700 chauffeurs américains sont concernés par cet incident. Et par ailleurs, poursuit Uber, le bug a été corrigé dans les 30 minutes qui ont suivi sa découverte.

Selon Gawker, ce bug pourrait être lié à la sortie d'une nouvelle application : Uber Partner. Celle-ci permet aux conducteurs de gérer leurs comptes et de suivre leurs courses, mais aussi de transmettre des données pour l'enregistrement des nouveaux chauffeurs.

En comparaison de la faille de sécurité du début d'année, la dernière semble mineure. Une base de données de 50.000 chauffeurs Uber avait en effet fuité sur GitHub. La société a été critiquée à plusieurs reprises pour ses pratiques en matière de sécurité et de confidentialité des données.

Pour redorer son blason et améliorer la sécurité de ses développements, Uber a créé cette année un poste de responsable de la sécurité informatique (RSSI) et embauché deux hackers renommés, Charlie Miller et Chris Valasek.

Denis JACOPINI est Expert Informatique, conseiller et formateur en entreprises et collectivités et chargé de cours à l'Université.

Nos domaines de compétence :

- **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
- **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
- **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.

Contactez-nous

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

Source :
http://www.zdnet.fr/actualites/oups-uber-devoile-les-donnees-personnelles-de-chauffeurs-39826600.htm

Piratage de TV5 Monde: une facture très salée | Le Net Expert Informatique

	Piratage de TV5 Monde: une facture très salée

L'attaque subie par la chaîne francophone internationale en avril lui aura coûté plus d'une dizaine de millions d'euros. De quoi obliger TV5 à tailler dans son budget 2016.

« La sécurité informatique coûte cher, mais combien coûte l'absence de sécurité? », pourrait-on s'interroger, en paraphrasant Lincoln.

Chez TV5 Monde, on commence à avoir une idée du coût du piratage subi par la chaîne le 8 avril dernier: il dépassera largement la dizaine de millions d'euros.

Création d'une cellule de sécurité informatique

Précisément, ce piratage entraînera un surcoût de 4,8 millions d'euros cette année; de 2,4 millions d'euros l'an prochain; et pour les années suivantes 2 à 2,5 millions d'euros par an.

En pratique, la chaîne internationale a dû bien sûr investir pour renforcer la sécurité de ses réseaux. Un plan a été élaboré à partir des recommandations de l'ANSSI (Agence nationale de sécurité des systèmes d'information). Ce plan comprend notamment la création d'une cellule permanente dédié à la sécurité informatique qui n'existait pas auparavant. Une équipe de six nouveaux salariés est actuellement en cours de recrutement.

Sites web « sinistrés »

Mais ce n'est pas tout. La chaîne francophone fonctionne encore « en mode dégradé », indique son budget 2016. Interrogée, la chaîne n'a pas précisé ce que cela signifiait précisément. Mais le budget 2016 indique que de nombreuses missions (notamment la mise en ligne des émissions sur le site web), jusqu'à présent réalisées automatiquement, se font désormais manuellement, ce qui nécessite du personnel supplémentaire. « Les sites internet de la chaîne sont sinistrés », indique le budget.

Evidemment, de telles sommes sont significatives au regard du budget de la chaîne (110 millions d'euros). Des économies ont donc dû être recherchées sur d'autres postes. « Les budgets d'opérations (programmes, sous-titrage, marketing, communication) » ont été réduits. Notamment, « les budgets destinés aux acquisitions de programmes et au sous-titrage sont fortement affectés ».

La publicité sur internet « s'effondre »

Les malheurs de la chaîne ne s'arrêtent pas là. Le site web, dont l'audience déjà en chute libre depuis plusieurs années, a été inaccessible, puis ensuite rétabli avec un contenu réduit, ce qui accéléré la chute de l'audience. Au total, les visites ont chuté de 13% au premier semestre, et les vidéos vues de 15%. « La baisse significative des audiences numériques risque de s'accentuer dans les mois à venir », prévient le budget. Conséquence logique: « les recettes publicitaires sur le numérique s'effondrent ».

Rappelons que de nombreuses erreurs avaient été mises à jour après le piratage. Le site spécialisé Zataz a assuré avoir signalé à la chaîne publique une dizaine de failles depuis deux ans. Selon 01net.com, le réseau bureautique et le réseau de production télé de TV5 n'étaient pas totalement cloisonnés, ce qui a permis au piratage du premier de contaminer le second, entraînant un écran noir…

Enfin, Arrêt sur images avait relevé que les mots de passe étaient affichés sur le mur. Filmés lors d'un reportage effectué dans les locaux par France 2 suite à l'attaque, ils avaient été donc été potentiellement vus par des centaines de milliers de téléspectateurs… Le mot de passe du compte YouTube était ainsi lemotdepassedeyoutube… TV5 avait admis « une bourde » et assuré que les mots de passe n'étaient pas affichés ainsi avant le piratage.

Denis JACOPINI est Expert Informatique, conseiller et formateur en entreprises et collectivités et chargé de cours à l'Université.

Nos domaines de compétence :

- **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
- **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
- **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.

Contactez-nous

Source : http://bfmbusiness.bfmtv.com/entreprise/piratage-de-tv5-monde-une-facture-tres-salee-922231.html
Par Jamal Henni

Surveillance : le spyware FinFisher détecté dans 32 pays | Le Net Expert Informatique

Le spyware FinFisher détecté dans 32 pays

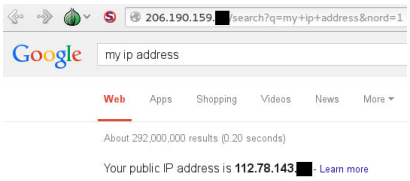
Malgré les mesures prises pour en dissimuler l'existence, le Citizen Lab a réussi à remonter à nouveau la trace du spyware FinFisher vendu aux autorités policières de nombreux états dans le monde, y compris dans des pays autoritaires.

Le business de l'espionnage des communications électroniques fonctionne toujours très bien. Alors que le piratage spectaculaire de la société Hacking Team n'a semble-t-il eu aucun effet notable sur ses relations commerciales avec les autorités qui exploitent ses services, son concurrent britannique FinFisher n'a visiblement lui non plus aucun problème à continuer ses activités, malgré la divulgation de ses codes sources et d'autres données internes en 2014.
Les gouvernements continuent de faire confiance à ces entreprises privées qui proposent ça et là des outils permettant de placer sur écoute des smartphones, d'accéder aux données d'un PC, de collecter toutes les touches frappées sur un clavier, d'activer discrètement des webcams, de géolocaliser des appareils, ou encore d'accéder au contenu de conversations en principe privées et chiffrées. Les intérêts pour la sécurité nationale priment sur les quelques questions éthiques que peuvent poser certaines méthodes, qui valent à ces firmes d'être placées sur une liste des « sociétés ennemis d'internet » par Reporters Sans Frontières.

Car les services qu'elles vendent ne sont pas achetés que par des démocraties bien sous tous rapports, malgré les restrictions à l'exportation qu'elles sont censées respecter.

Le laboratoire Citizen Lab a ainsi publié de nouvelles démonstrations de la présence des outils de Finfisher dans au moins 32 pays, dont plusieurs états peu recommandables du point de vue du respect des droits fondamentaux, comme la Malaisie, l'Arabie Saoudite, le Kazakhstan, l'Ethiopie, le Maroc ou le Bengladesh.
Déjà en 2012, le laboratoire avait prouvé que la suite d'outils d'espionnage Finfisher vendue à l'époque par la société britannique Gamma International (elle a depuis donné son indépendance à Finfisher GmbH, basée à Munich), était utilisée par au moins une quinzaine d'États dans le monde. Parmi eux figuraient déjà des pays autoritaires comme le Bahreïn, l'Ethiopie, l'Indonésie, le Turkménistan, ou les Emirats-Arabes Unies.
Comme Hacking Team, Finfisher assure qu'elle respecte l'arrangement de Wassenaar qui limite les possibilités d'exporter les outils de surveillance vers des pays autoritaires qui peuvent en faire un usage non conforme aux droits de l'homme, par exemple pour traquer des opposants politiques ou rechercher les sources de journalistes hostiles au régime. Mais la présence continue de ses outils sur des serveurs appartenant à des régimes dictatoriaux permet, au minimum, de douter de la véracité de telles affirmations.
Depuis les révélations de 2012, FinFisher a amélioré ses méthodes de dissimulation et systématiquement caché ses outils derrière des serveurs proxys, configurés pour paraître inoffensifs. Mais les chercheurs du Citizen Lab ont regorgé d'ingéniosité pour les trouver.
Depuis décembre 2014, l'organisation a scanné un maximum d'adresses IPv4 pour trouver des serveurs dont certaines caractéristiques correspondaient à ce qu'ils connaissaient de FinFisher. Ils ont trouvé 135 serveurs, dont la plupart étaient des serveurs proxys qui affichaient la page d'accueil de Google ou Yahoo. Ces serveurs là, qui servent uniquement de relais intermédiaire, n'avaient aucun intérêt puisqu'ils masquaient la géolocalisation des serveurs « maîtres » sur lesquels étaient installés les outils de FinFisher. Mais aux yeux de Google et Yahoo, c'est bien l'adresse IP du serveur maître qui communique.

PREMIÈRE ASTUCE :
« DIS-MOI MON ADRESSE IP »

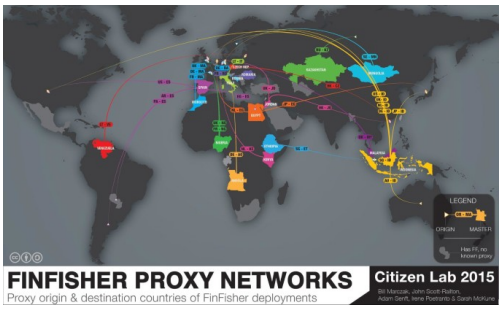


Lorsque Google était affiché, il suffisait d'exécuter la requête « my IP adress » (qui ne fonctionne pas avec Google France) pour que Google réponde au serveur maître, et que celui-ci renvoie la réponse au serveur relais, qui lui-même l'affichait à Citizen Lab. Ils ont ainsi pu trouver des adresses IP de serveurs maîtres installés dans différents pays, et découvrir leur géolocalisation.

DEUXIÈME ASTUCE :
« DIS-MOI QUEL TEMPS IL FAIT »

Sur Yahoo, la commande n'existe pas. Mais le service sait afficher la météo qui correspond au lieu qu'il associe à l'adresse IP de l'internaute. Les chercheurs ont donc demandé à Yahoo d'afficher la météo et découvert que, par exemple, un serveur qui était censément installé en Lituanie renvoyait la météo de Caracas, au Venezuela. Un pays où les journalistes sont régulièrement persécutés. Ca ne permettait pas d'obtenir en direct l'adresse IP, mais au moins de savoir où elle était attachée.

La carte des proxys :



Denis JACOPINI est Expert Informatique, conseiller et formateur en entreprises et collectivités et chargé de cours à l'Université.
Nos domaines de compétence :
• **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
• **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
• **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.
Contactez-nous

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

Source : http://www.numerama.com/tech/126760-surveillance-le-spyware-finfisher-detecte-dans-32-pays.html
Par Guillaume Champeau
Crédit photo de la une : Thibaut Démare

Une panne informatique bloque le contrôle des passagers dans les aéroports US | Le Net Expert Informatique

Une panne informatique bloque le contrôle des passagers dans les aéroports US

Avant-hier soir, plusieurs aéroports américains parmi les plus importants ont été victimes d'une panne informatique – probablement un problème de bases de données – bloquant le contrôle des passagers lors du débarquement et avant l'accès aux terminaux des portes d'embarquement.

Le système informatique du Department of Homeland Security, le service des douanes aux États-Unis, a connu une défaillance majeure dans plusieurs aéroports américains ce qui a entrainé des attentes et des retards pour certains passagers. CNBC rapporte que le système informatique en question est celui qui vérifie les noms des passagers aériens avec la liste des personnes soupçonnées de terrorisme par la Homeland Security. Dans ces circonstances, le personnel des douanes et de la protection des frontières est censé utiliser des méthodes alternatives pour le traitement des passagers dans les aéroports où les systèmes informatiques sont hors services.

Les médias sociaux ont commencé à remonter les problèmes hier soir vers 8 h (heure de la Côte Est des États-Unis) soit 2 h du matin en France. Jusqu'à présent, les alertes ont rapporté le problème à l'aéroport JFK de New York, Logan de Boston, San Francisco, Baltimore-Washington, Hartsfield Jackson d'Atlanta, Dallas-Fort Worth, Charlotte Douglas, et éventuellement d'autres aéroports.

Un fonctionnaire du DHS a toutefois confirmé à NBC qu'un « pépin » dans les systèmes informatiques – surement un problème de bases de données – est à l'origine du problème à l'aéroport JFK. NBC, de son coté, cite des responsables gouvernementaux de haut niveau confirmant les problèmes, et précise que les fonctionnaires ne pouvaient pas indiquer quand le problème serait réglé.

Source :
http://www.lemondeinformatique.fr/actualites/lire-une-panne-informatique-bloque-le-controle-des-passagers-dans-les-aeroports-us-62672.html