Les salariés doivent aussi prendre conscience des conséquences des failles de sécurité | Le Net Expert Informatique

Les salariés doivent aussi prendre conscience des conséquences des failles de sécurité

Lors des Assises de la Sécurité MobileIron présentera sa plateforme conçue pour sécuriser et gérer les systèmes d'exploitation tout en préservant la confidentialité des données personnelles. Pour Sid-Ahmed Lazizi, Directeur Général France, MobileIron Il est essentiel de faire prendre conscience aux salariés des conséquences potentielles des failles de sécurité, tout comme définir le type de données auquel on peut ou ne peut pas accéder depuis un appareil portable.

Global Security Mag : Qu'allez-vous présenter à l'occasion des Assises de la Sécurité ?
Sid-Ahmed Lazizi : Lors des Assises de la Sécurité, MobileIron présentera sa plateforme conçue pour sécuriser et gérer les systèmes d'exploitation modernes dans le cadre d'une utilisation de terminaux divers et variés. Elle prend en compte l'identité, le contexte et les règles de confidentialité établies pour définir le niveau approprié d'accès aux données et services des entreprises. MobileIron sécurise les données statiques sur les terminaux, dans les applications et dans le cloud. Son action de sécurisation porte également sur les data-in-motion (données dynamiques) lorsqu'elles circulent entre le réseau d'une entreprise, les terminaux et les référentiels de stockage. Grâce à MobileIron, les services informatiques peuvent assurer la sécurité des données des entreprises où qu'elles soient, tout en préservant la confidentialité des données personnelles des employés. Cette plateforme se compose de trois produits :
MobileIron Core : serveur qui permet aux services informatiques de définir des règles de sécurité et de gestion sur les systèmes d'exploitation mobiles les plus répandus
MobileIron Client : logiciel qui réside sur les appareils afin d'y appliquer les règles définies par le service informatique
MobileIron Sentry : passerelle intelligente qui sécurise le trafic des données entre les appareils mobiles et les systèmes back-end de l'entreprise

GS Mag : Quelle va être le thème de votre conférence cette année ?
Sid-Ahmed Lazizi : Le thème de notre conférence qui aura lieu le 2 octobre à 11h est « Le nouveau modèle de sécurité en entreprise ». Les employés choisissent de plus en plus de travailler sur des terminaux mobiles dotés de systèmes d'exploitation modernes tels que Android, iOS ou Windows 10, et ce en lieu et place des ordinateurs de bureau traditionnels et des outils conçus pour Windows. Le défi engendré en termes de sécurité par ces nouveaux systèmes d'exploitation est bien différent de ceux de l'ancienne ère du PC, ce qui nécessite d'aborder la situation sous un autre angle et d'utiliser une technologie nouvelle.

GS Mag : Quel est votre message aux RSSI ?
Sid-Ahmed Lazizi : À mesure que les terminaux mobiles et objets connectés se multiplient, s'adaptent et intègrent le monde de l'entreprise, les services informatiques découvrent de nouvelles menaces qui pèsent sur les données et doivent relever de nouveaux défis pour les protéger. Ils doivent repenser leurs stratégies et infrastructures informatiques pour permettre une utilisation sûre et efficace de ces terminaux et objets, qui représentent une véritable opportunité d'augmenter la productivité des collaborateurs de l'entreprise.
Les technologies portables étant relativement récentes, elles se développent et s'améliorent constamment. Elles présentent le même défi que celui des smartphones quand ces derniers sont apparus. En effet, lorsque les technologies mobiles ont commencé à s'imposer, la réponse initiale des directions informatiques fut de réguler ou restreindre les accès mobiles. Cette approche s'est révélée majoritairement inefficace, les employés trouvant de plus en plus de solutions pour contourner les recommandations de leur département IT.
Liés aux smartphones, les technologies portables vont très rapidement débarquer en entreprise Etant donné que la restriction n'est pas toujours une option viable, reste le problème de la sécurité des données. Pour commencer, les départements informatiques devraient se concentrer sur les plateformes qui permettent de gérer et de sécuriser au niveau fichier, ce que certaines sociétés avancées font déjà sur mobile. Ces types de services garantissent la protection des données de l'entreprise même si le dépôt central de stockage des données est corrompu.
Les départements informatiques devront également travailler main dans la main avec les équipes RH et juridique pour définir un cadre d'utilisation clair de ces appareils mobiles au sein de l'entreprise, tout comme rappeler les risques de sécurité induits par l'accès aux données de l'entreprise sur des appareils portables ou similaires. Idéalement, ces règlements devraient être communiqués aux employés de façon positive pour valider le potentiel d'exploitation des appareils mobiles à la fois sur le plan professionnel et personnel.

Il est essentiel de faire prendre conscience aux salariés des conséquences potentielles des failles de sécurité, tout comme définir le type de données auquel on peut ou ne peut pas accéder depuis un appareil portable. Cela permettra de favoriser la relation de confiance entre les directions informatiques et les employés.

Source : https://www.globalsecuritymag.fr/Sid-Ahmed-Lazizi-MobileIron-Les,20150716,54434.html

---

Augmentation de la taille moyenne d'attaques DDoS | iTPro.fr | Le Net Expert

Informatique

Augmentation de la taille moyenne d'attaques DDoS

Arbor Networks, spécialiste de la protection contre les attaques DDoS, publie ses statistiques relatives aux attaques DDoS pour ce second trimestre.

Tant en bits par seconde qu'en paquets par seconde, il semblerait que les attaques de type DDoS soient de plus en plus imposantes. L'attaque la plus forte de ce second trimestre de type « UDP Flood » a atteint 196 bits/s. Le problème réside surtout dans le fait que cette amplitude n'est plus aussi rare qu'auparavant.Au deuxième trimestre, 21 % d'entre elles ont dépassé 1 Gbit/s, la progression la plus forte enregistrée étant celle dans la fourchette des 2 à 10 Gbit/s. Le mois de juin a aussi été marqué par l'augmentation des attaques entre 50 et 100 Gbit/s principalement de type « SYN Flood » ciblant le Canada et les Etats-Unis.
Darren Anstee, directeur des technologies de sécurité pour Arbor Networks explique que« si les attaques d'une ampleur extrême monopolisent les gros titres, c'est la progression de la taille moyenne des attaques DDoS qui inquiète les entreprises à travers le monde. Les entreprises doivent définir clairement leur risque en matière de DDoS. Face à des attaques moyennes capables de saturer l'accès Internet de bon nombre d'entreprises, il est essentiel de saisir les risques et les coûts d'une attaque et de mettre en place les plans, services et solutions appropriés. »
Du côté des attaques par amplification et réflexion, il semblerait que celles exploitant SSDP soient en baisse puisque 84 000 ont été détectées au second trimestre contre 126 000 au deuxième. Cependant, la taille moyenne des attaques d'amplification par réflexion DNS, NTP, SSDP et Chargen a augmenté au deuxième trimestre 2015 et 50 % de ce type d'attaques ciblaient le port UDP 80 (HTTP/U) pour une durée de 20 minutes (contre 19 pour le premier). A noter que ce type d'attaque permet d'amplifier la volumétrie du trafic par un nombre de réponses envoyé plus important tout en masquant les sources. Cette technique exploite notamment le manque de mesures mises en place par les opérateurs pour filtrer le trafic et la mauvaise configuration d'équipement fournissant des services UDP.

Source : http://www.itpro.fr/n/augmentation-taille-moyenne-dattaques-ddos-21404/

Carte de France des barrages des éleveurs en colère | Le Net Expert Informatique

	Carte de France des barrages des éleveurs en colère

Départ en vacances ? départ en congés ? Même si ça n'a aucun rapport avec la Cyber ou la Protection des données personnelles, il nous a semblé utile et même indispensable pour certains de partager avec vous la carte de France des barrages placés par des éleveurs en colère.Cette carte est intéractive et est mise à jour régulièrement par Le Figaro.
Denis JACOPINI

CENTRE-EST
Les éleveurs de Rhône-Alpes ont commencé à bloquer l'accès Nord et Est de Lyon mercredi soir avec des tracteurs, l'A6 et l'A42 étant coupées en direction de Lyon, selon Bison Futé. Ils devaient, au petit matin jeudi, paralyser l'accès Sud de la deuxième agglomération de France, selon la FNSEA régionale. A Clermont-Ferrand, la FDSEA et les JA du Puy-de-Dôme prévoyaient de bloquer cinq accès de la ville jeudi matin. Leur principale revendication: une intervention des pouvoirs publics pour faire monter les prix de la viande et du lait, élément fondamental qui ne figure pas, selon eux, dans le plan d'aide du gouvernement de 600 millions d'euros.
Mercredi, 300 à 400 agriculteurs ont bloqué-vers 22H00, selon la FDSEA de Saône-et-Loire, qui n'excluait pas de nouvelles actions jeudi matin. D'autres actions étaient prévues jeudi en Bourgogne, dans l'Yonne et la Nièvre, alors que François Hollande devait se rendre à Dijon, où il rencontrera la monde agricole à 9H00. Dans l'Yonne, ils prévoient dès 6H30 de bloquer l'abattoir de Migennes avant de se rendre à la laiterie Yoplait de Montéteau.
Dans la région voisine de Franche-Comté, 150 à 200 agriculteurs, aux volants d'une quarantaine de tracteurs, se sont réunis mercredi soir à Vesoul (Haute-Saône), selon un correspondant de l'AFP. Les agriculteurs ont notamment «intercepté» une citerne laitière d'environ 15.000 litres de lait. Ils l'ont conduite aux abords d'une grande surface du centre-ville, où ils ont commencé à en déverser le contenu vers 23H00.

CENTRE
Mercredi soir quelque 150 agriculteurs -avec une trentaine de tracteurs- se sont mobilisés pour bloquer les livraisons à un supermarché Lidl à Savigny (au sud de Tours), selon un dirigeant de la FDSEA d'Indre-et-Loire. Du fumier, de la paille et des poneys ont été déversés pour boucher l'accès aux camions. Et les agriculteurs envisagent de cibler aussi un atelier de découpe de viande bovine à Montbazon (entre Savigny et Tours) qui, selon la FDSEA, ne traite que de la viande de provenance étrangère.

CENTRE-OUEST
Les barrages filtrants mis en place mercredi sur les routes d'accès au château de Chambord ont été levés.
«On a l'impression que Stéphane Le Foll s'en fout» de nous.»
Le président des JA du département, Charles Guerlais.
En Loire-Atlantique, où aucun blocage n'aurait lieu ce mercredi, les actions prévues jeudi matin, suivant un mot d'ordre national appelant à viser les transformateurs, sont maintenues, selon le président des JA du département, Charles Guerlais. «Les annonces du gouvernement n'ont rien fait pour calmer l'élevage (...). Dans les campagnes, on a l'impression que M. Le Foll s'en fout» de nous», a-t-il affirmé.
En Vendée, le dernier point de blocage, le péage de Beaufief, a été levé. En Charente-Maritime, le blocage perdure sur le port de l'Ile d'Aix. «Sauf urgences médicales», les barrages filtrants ne laissent passer qu'une cinquantaine de véhicules toutes les 45 minutes, sur une file, puis sur l'autre, selon la préfecture.
Dans la Vienne, la circulation reste fortement perturbée autour de Poitiers. L'autoroute A20, reliant Paris à Toulouse, était bloquée dans les deux sens jeudi matin en Haute-Vienne par des éleveurs en colère, qui ont mis en place un barrage filtrant, a-t-on appris auprès des agriculteurs. L'opération de blocage, menée conjointement par les éleveurs de Haute-Vienne et de Creuse, a commencé peu avant 10h00, à quelques kilomètres de la Souterraine. Toutes les voies de l'autoroute sont neutralisées au niveau du rond-point de la Croisière, qui permet l'accès à la RN 145, axe routier important pour les poids-lourds, selon le Centre régional d'information routière.

CORRÈZE
A Brive-La-Gaillarde, dans la nuit de mercredi à jeudi, quelques 200 éleveurs et agriculteurs, certains avec leur tracteur, ont déversé du lisier devant plusieurs supermarchés et fournisseurs de restaurants (Metro, Promocash), a constaté un photographe de l'AFP. Ils ont également mis le feu à des pneus et dégradé plusieurs panneaux portant les enseignes des supermarchés, selon la même source.

HAUTES-PYRÉNÉES
Plusieurs centaines d'agriculteurs de la FDSEA et des JA des Hautes-Pyrénées ont déversé mercredi soir du fumier et du lisier devant des grandes surfaces de Tarbes et son agglomération, a-t-on appris auprès des manifestants et de la préfecture. Selon un responsable agricole local, Jean-Luc Cazabat, un rassemblé peu avant minuit plusieurs centaines d'agriculteurs et près de cent tracteurs engagés dans l'action devant 12 établissements. A la préfecture on faisait état de chiffres similaires portant de 300 personnes et 125 tracteurs au total mobilisés devant 12 grandes surfaces.

NORMANDIE
Les barrages ont disparu sur le périphérique de Caen, épicentre de la contestation, après un appel des dirigeants agricoles à suspendre le mouvement quelques heures après l'annonce du plan de l'«exécutif.
«Le mot d'ordre est d'aller renforcer les barrages des ponts,» Stéphane Dauchelle, vice-président de la FNSEA de Seine-Maritime.
En Haute-Normandie, l'un des trois grands ponts suspendus permettant de traverser la Seine entre Rouen et l'estuaire, celui de Tancarville, reste bloqué, tandis que les barrages sont devenus filtrants aux ponts de Normandie et de Brotonne. «Des collègues du Calvados ont commencé leur mouvement dimanche soir, nous n'avons démarré qu'hier matin, on peut encore tenir», a déclaré à l'AFP Stéphane Dauchelle, vice-président de la FNSEA de Seine-Maritime. «Le mot d'ordre est d'aller renforcer les barrages des ponts», a ajouté M. Dauchelle.
Des éleveurs bloquent à nouveau jeudi matin les accès au Mont Saint-Michel, qu'ils avaient dégagés la veille au soir après l'annonce d'une aide d'urgence du gouvernement, a annoncé la préfecture de la Manche.Des deux routes qui donnent accès à ce site touristique, l'un des plus visités de France, la RD976 est entièrement bloquée par une dizaine de tracteurs, tandis que la RD275 reste en cours de blocage», selon la préfecture.

BRETAGNE
En Ille-et-Vilaine, la situation est revenue à la normale sauf à Saint-Malo où les éleveurs bloquent depuis mardi le principal accès à la cité corsaire. Dans le Finistère, les éleveurs qui quitté le grand point de l'Iroise, à Brest, qu'ils occupaient depuis mardi mais celui-ci reste fermé pour sa remise en état. En revanche, d'autres barrages perduraient notamment à Quimper ou Morlaix. Dans un communiqué, les Bonnets rouges ont appelé «tous les Bretons à se joindre aux manifestations des agriculteurs partout où c'est possible».

OISE
A Lille, le blocage de l'A1 a été levé tôt dans la matinée et en Picardie, les dernières actions d'envergure ont été levées.

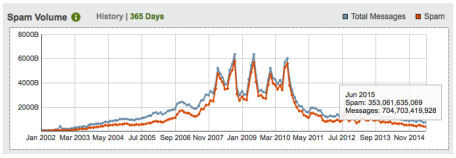
Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.
Besoin d'informations complémentaires ?
Contactez-nous
Denis JACOPINI
Tel : 06 19 71 79 12
Formateur n°93 84 03041 84

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure sécurité des systèmes informatiques et améliorer la protection juridique du chef d'entreprise.
Contactez-nous

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

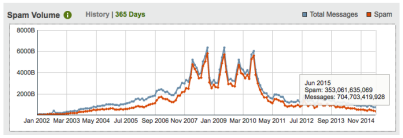
Source - http://www.lefigaro.fr/actualite-france/2015/07/22/01016-20150722ARTFIG00111-eleveurs-en-colere-la-carte-de-france-des-barrages.php

Le spam est à son niveau le plus bas | Le Net Expert Informatique



Le spam est à son niveau le plus bas

Aurons-nous finalement raison du spam ? Il semblerait en tout cas que les efforts menés sur ce secteur commencent à porter leurs fruits selon un rapport du cabinet Symantec.
Les analystes de Symantec ont publié leur rapport de sécurité portant sur le mois de juin. Selon les chiffres internes, le taux de spam sur l'ensemble des emails envoyés le mois dernier n'était que de 49,7%. « C'est la première fois depuis plus de dix ans que ce taux passe sous la barre des 50% », expliquent ainsi les experts. Plus précisément, la proportion de courriers indésirables est donc à son plus bas depuis le mois de septembre 2003.
Symantec affirme que les actions en justice menées contre les réseaux criminels contrôlant les réseaux de botnets portent véritablement leurs fruits. Il est possible que le spam ne soit plus une source de revenus stables pour les cybercriminels.



Symantec ajoute que le taux d'attaques par phishing ou le déploiement de malware par email est également en baisse. En revanche, sur le mois de juin, 57,6 millions de nouvelles variantes de malware ont été identifiées, contre 44,5 millions au mois de mai et 29,2 millions en avril. Cela signifie donc que si les activités criminelles ne ralentissent pas, elles sont désormais effectuées de manière différente (par exemple via les réseaux communautaires, la messagerie instantanée, les applications mobiles ou les pages Web malveillantes).
Récemment, l'équipe de Gmail annonçait avoir optimisé l'intelligence artificielle appliquée aux filtres anti-spam avec un réseau de neurones artificiels. Les algorithmes s'en trouvent alors plus performants et devraient être capables de mieux discerner les courriers indésirables. En octobre dernier, Microsoft expliquait pour sa part bloquer 10 millions de spams chaque minute. La firme de Redmond a notamment participé à la fermeture de plusieurs botnets.
Consulter le rapport dans son intégralité sur cette page (PDF)

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure sécurité des systèmes informatiques et améliorer la protection juridique du chef d'entreprise.
Contactez-nous

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

Source :
http://www.clubic.com/antivirus-securite-informatique/virus-hacker-piratage/spam-pourriel/actualite-773950-spam-niveau-bas-12-ans.html?estat_svc=s%3D223023201608%26crmID%3D639453874_1070073452#pid=22889469

Au Journal officiel, l’encadrement des mouchards de Skype (et assimilés) | Le Net Expert Informatique

Après les yeux, les oreilles Crédits : alphaspirit/iStock/Thinkstock	Au Journal officiel, l’encadrement des mouchards de Skype (et assimilés)

Journal officiel, un arrêté vient encadrer, sous l'œil de l'ANSSI, la définition des mouchards que les juges peuvent désormais utiliser pour faire espionner non seulement les données saisies au clavier ou affichées sur l'écran, mais également celles « reçues et émises par des périphériques audiovisuels ».

En 2011, la loi d'orientation et de programmation pour la sécurité intérieure (LOPPSI) avait permis à la police, sur autorisation d'un juge, la mise en place de mouchard, même à distance. L'enjeu ? Enregistrer les frappes au clavier (keylogger) ou les images affichées sur un écran afin d'espérer glaner quelques preuves, dans le cadre d'enquête pour des infractions sérieuses (criminalité organisée, terrorisme).
Seulement, il y avait un trou dans la raquette. En visant les données affichées « sur un écran » ou celles introduites « par saisie de caractères », le texte initial excluait mécaniquement la captation de parole. Une lacune très contrariante pour qui veut épier une conversation sur Skype par exemple.

La loi contre le terrorisme et Skype
La loi contre le terrorisme de novembre 2014 a comblé la faille. Depuis, non seulement les données saisies au clavier peuvent être espionnées judiciairement, mais également celles « reçues et émises par des périphériques audiovisuels ». La rustine se trouve à l'article 706-102-1 du Code de procédure pénale.
Toutefois encore, une dernière étape manquait pour parfaire ce système. Un autre article, le 226-3 du Code pénal, soumet ces armes de surveillance intrusive à un arrêté du Premier ministre, épaulé par le directeur général de l'Agence nationale de la sécurité des systèmes d'information (ANSSI). Son objet ? Dresser la liste de ces outils sensibles dont est autorisée la fabrication, l'importation, la détention, l'exposition, l'offre, la location ou la vente. Sans ce feu vert, ces mêmes opérations, susceptibles de générer des atteintes à la vie privée ou au secret des correspondances, sont en effet sanctionnées de cinq ans d'emprisonnement et de 300 000 euros d'amende.
Cet arrêté du 4 juillet 2012 « fixant la liste d'appareils et de dispositifs techniques prévue par l'article 226-3 du code pénal » n'avait pas non plus été mis à jour depuis la loi contre le terrorisme. Cet oubli empêchait donc la commercialisation sous contrôle de mouchards de nouvelle génération.
Ce nouveau manque a été corrigé aujourd'hui au Journal officiel. Le Premier ministre a en effet complété le texte de 2012 en y remplaçant l'expression « ou telles qu'il les y introduit par saisie de caractères » par les mots « telles qu'il les y introduit par saisie de caractères ou telles qu'elles sont reçues et émises par des périphériques audiovisuels ». Sous l'œil de l'ANSSI, certains espiogiciels capables de surveiller Skype (et assimilés) peuvent donc maintenant être introduits en France et utilisés par les services autorisés.

De la surveillance judiciaire à la surveillance administrative
Rappelons au passage que le projet de loi Renseignement permet elle aussi la captation des données informatiques dans un cadre cette fois strictement administratif. Donc sans juge. La même loi s'est servie de l'article 226-3 du Code pénal pour également étendre l'aspiration des métadonnées.
Pour la poursuite de finalités jugées très floues, les services du renseignement pourront en effet utiliser l'ensemble des appareils mentionnés à cet article, afin de moissonner « les données techniques de connexion permettant l'identification d'un équipement terminal ou du numéro d'abonnement de son utilisateur ainsi que les données relatives à la localisation des équipements terminaux utilisés ». Cet arsenal (IMSI catcher, mais pas seulement) pourra par exemple être utilisé pour connaître « directement » les données générées par un smartphone, situé à proximité d'un point déterminé.

Source :
http://www.nextinpact.com/news/95893-au-journal-officiel-encadrement-mouchards-skype-et-assimiles.htm
Par Marc Rees

Inquiétude sur les données de connexion | Le Net Expert Informatique

Inquiétude sur les données de connexion

C'est, pour le Conseil constitutionnel, un petit tour de chauffe avant sa décision, vendredi 24 juillet, sur la loi renseignement, un mois après avoir été saisi par le président de la République et 106 parlementaires. Le Conseil examinait en effet, mardi 21 juillet, une question prioritaire de constitutionnalité (QPC), transmise par le Conseil d'Etat, sur la délicate surveillance des données Internet.

Trois associations (French Data Network, la Quadrature du Net et la Fédération des fournisseurs d'accès à Internet associatifs) attaquaient un article décisif, repris par la loi renseignement, de la loi de programmation militaire de décembre 2013 sur « l'accès administratif [policier] aux données de connexion » qu'elles jugent contraire « aux droits au respect de la vie privée, à un procès équitable et à la liberté de communication ».
Les associations s'inquiètent d'une mesure, introduite dans le code de la sécurité intérieure, qui autorise « le recueil, auprès des opérateurs de communications électroniques, (…) des informations et documents traités ou conservés par leurs réseaux ».

Que sont exactement ces « informations et documents » ? Les données de connexion ? Le contenu des correspondances ?
La loi ne le dit pas et a donc, pour les associations, délégué au pouvoir réglementaire – à l'administration – le soin de faire pour le mieux. Ça ne se fait pas. Le Conseil constitutionnel supporte mal de voir « reporter sur des autorités administratives ou juridictionnelles le soin de fixer des règles dont la détermination…
Lire la suite….

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

Source : http://www.lemonde.fr/societe/article/2015/07/22/inquietude-sur-les-donnees-de-connexion_4693599_3224.html
Par Franck Johannès

Une Jeep quitte la route suite à son piratage par deux hackers | Le Net Expert Informatique

Une Jeep quitte la route suite à son piratage par deux hackers

Charlie Miller et Chris Valasek, deux experts en sécurité ont piraté une automobile à distance et pris le contrôle de plusieurs de ses fonctions, dont les freins, grâce à une faille du système Uconnect du fabricant Fiat Chrysler.

Le logiciel et l'électronique sont de plus en plus présents dans les véhicules. Mais, les constructeurs doivent sans doute encore renforcer leur expertise dans le domaine du logiciel et aussi de la sécurité informatique.
Ce n'est pas la première fois que des experts en sécurité démontrent des vulnérabilités dans les moyens de transports. Les deux chercheurs Charlie Miller et Chris Valasek en ont fait une nouvelle démonstration avec un journaliste de Wired, Andy Greenberg.

Un patch à déployer manuellement, sur chaque voiture
Les deux hackers ont profité d'une faille du système de bord Uconnect, déployé dans nombre de voitures connectées du constructeur Fiat Chrysler et permettant de communiquer avec le véhicule depuis un smartphone.
Le fabricant n'avait certainement pas pensé aux actions réalisées par Miller et Valasek. Ces derniers ont donc pu se connecter à distance à la voiture, grâce à son adresse IP, et en prendre le contrôle : freiner ou couper les freins, déclencher les essuie-glaces pour gêner le conducteur, éteindre le moteur…
D'après Wired, qui a publié un article sur la prise de contrôle de la voiture, la faille de Uconnect affecte plusieurs modèles de véhicules de 2013 et 2014 du constructeur, parmi lesquels les Jeep, Dodge Ram et Dodge Viper.
Fiat Chrysler, le fabricant, était informé et a diffusé un correctif de sécurité la semaine dernière, un petit mois avant la présentation des deux chercheurs en sécurité prévue à la Black Hat. Problème : le patch doit être installé manuellement, ce qui impose aux propriétaires des véhicules concernés de se rendre chez leur garagiste agréé.

VIDÉO – Pour une expérience, deux chercheurs américains sont parvenus à pirater une Jeep à distance, tandis qu'elle roulait sur une autoroute. Chysler a produit un correctif.

C'est une vidéo très angoissante que vient de publier Wired. On y voit un des journalistes du magazine spécialisé, Andy Greenberg, rouler à plus de 100 kilomètres par heure sur une autoroute du Missouri, dans une Jeep Cherokee récente. Sans qu'il n'actionne aucun bouton, les ventilateurs s'activent au niveau maximum. Il poursuit sa conduite, tandis que sa radio se met en route et diffuse du hip-hop à un niveau sonore dont il n'est pas coutumier. Une minute plus tard, son réservoir de liquide lave-vitres se vide et ses essuie-glaces battent la mesure. Il ne voit plus grand-chose. Mais un problème plus important arrive. La transmission de son véhicule est coupée, la Jeep ralentit. Pendant une longue minute, durant laquelle il craint de se faire emboutir par un semi-remorque, Andy Greenberg ne peut rien faire.

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

Source : http://www.zdnet.fr/actualites/deux-hackers-piratent-une-jeep-et-lui-font-quitter-la-route-39822718.htm

Déjà des backdoors et keyloggers pour Windows 10 chez Hacking Team | Le Net Expert Informatique

Déjà des backdoors et keyloggers pour Windows 10 chez Hacking Team

Anticipant sur les besoins de ses clients, Hacking Team s'est assuré d'être prêt au lancement de Windows 10. La société italienne a adapté ses outils pour être capable d'installer un backdoor sous Windows 10, et ainsi de pouvoir collecter à distance toutes les frappes de touches au clavier.

Windows 10 n'est pas encore officiellement sorti, mais les firmes qui fournissent aux autorités les outils permettant d'accéder à distance aux données sont déjà à pied d'oeuvre pour s'adapter au niveau système d'exploitation de Microsoft. Ainsi l'entreprise italienne Hacking Team, dont les e-mails ont fuité ce mois-ci, s'est assurée dès l'an dernier de pouvoir fournir à ses clients de quoi espionner des utilisateurs de Windows 10.

« Nous avons testé Windows 10 Preview et ça fonctionne », a ainsi expliqué Marco Valleri, le directeur de Hacking Team, dans un e-mail du 4 novembre 2014. Il répondait à l'ancien responsable des opérations à Singapour, Serge Woon, qui se demandait si « RCS 9.4 supporte Windows 8.2 » (en fait Windows 10). RCS est l'acronyme de « Remote Control System », le malware qui permet à Hacking Team de prendre à distance le contrôle d'un ordinateur pour accéder à ses données.

Un autre e-mail du 29 juin 2015 montre que deux employés de Hacking Team, Marco Fontana et Andrea Di Pasquale, ont testé avec succès l'installation hors ligne de plusieurs outils sur Windows 10 Enterprise Insider Preview. Ils disent avoir vérifié notamment « l'installation d'un backdoor », « l'exportation de preuves depuis le backdoor », et la « désinstallation du backdoor ».

« Super ! », s'enthousiasme le directeur technique Marco Valleri, qui propose aussitôt une réunion pour déployer la mise à jour dans un git, probablement celui de RCS.

La société Hacking Team dispose également d'un outil invisible pour Windows 10 permettant de collecter toutes les frappes de touches au clavier (un « keylogger »), comme le montre un courriel du 5 juin. Marco Fontana, qui semble être une petite star dans l'entreprise, y rend compte d'une réunion du mercredi 3 juin 2015, où « l'un des thèmes de la réunion était le test du mécanisme d'injection dans l'application Metro ».

Il explique que « le POC du keylogger pour Windows 10 est prêt et peut être testé pour vérifier sa « compatibilité » avec les antivirus ». Le POC (Proof-of-concept) est une démonstration de faisabilité.

Dans un e-mail du 15 juin, Marco Fontana précise à son équipe qu'il a testé une « technique d'injection dans l'application Metro de Windows 10 », et que « l'exécutable 'ExeLoader' injecte la DLL ApiHookDll dans un processeur notepad.exe et capture les touches ». Il s'agit d'un POC visant à collecter les touches tapées sous sur l'application « Bloc Notes » de Windows 10.

« Si tout fonctionne correctement, dans le dossier temporaire de Windows (%temp%) vous verrez un fichier texte créé qui contient les touches enfoncées dans notepad. Le fichier a un préfixe KBD_ et une valeur aléatoire (ex: KBD_000407E600C553CE.txt) ».

Tout l'objet du logiciel RCS de Hacking Team est justement d'installer à distance les backdoors qui permettent d'installer des outils tels que ce keylogger, lequel permet ensuite de récupérer, par exemple, les mots de passe saisis pour accéder à des comptes e-mail, ou des mots de passe de clés de chiffrement.

« On ne peut pas croire à la sécurité d'un OS pour le grand public », s'était amusé en novembre dernier David Vincenzetti, le président de Hacking Team, en lisant une actualité selon laquelle Windows 10 pourrait signer la fin des malwares.

Source : http://www.numerama.com/magazine/33727-deja-des-backdoors-et-keyloggers-pour-windows-10-chez-hacking-team.html
par Guillaume Champeau

Hacking Team a travaillé sur un drone capable d'infecter des ordinateurs à distance | Le Net Expert Informatique

Hacking Team a travaillé sur un drone capable d'infecter des ordinateurs à distance

De nouvelles informations émergent des centaines de milliers d'e-mails piratés au fabricant de logiciels espions Hacking Team. Des échanges ont montré que l'entreprise italienne a été contactée par Insitu, un fabricant de drones appartenant à Boeing, pour travailler sur un système qui permettrait aux engins de pirater des réseaux Wi-Fi à distance, a relevé le site The Intercept.

Un rapport daté du 1er juillet montre d'ailleurs qu'Hacking Team travaillait sur un système d'injection réseau utilisable par drone, c'est-à-dire « un équipement conçu pour insérer du code malicieux dans les communications d'un réseau Wi-Fi », explique le site spécialisé Ars Technica.

« Nous ne pouvons vendre nos produits qu'à des entités gouvernementales »

Selon un premier e-mail envoyé en avril, Insitu s'est montré intéressé par une présentation de Hacking Team à l'IDEX 2015, un salon de la défense qui s'est tenu aux Emirats arabes unis en février. « Nous aimerions potentiellement intégrer votre système de piratage de Wi-Fi à un système aérien et nous souhaiterions prendre contact avec un de vos ingénieurs qui pourrait nous expliquer, plus en détail, les capacités de l'outil, notamment la taille, le poids et les spécifications de votre système Galileo [un logiciel espion] », écrit alors Giuseppe Venneri, ingénieur mécanique en formation chez Insitu.

« Gardez à l'esprit que nous ne pouvons vendre nos produits qu'à des entités gouvernementales », répond un responsable de Hacking Team, sans fermer la porte à une collaboration. Selon un e-mail interne, le même responsable de Hacking Team indique qu'Insitu travaille avec des agences gouvernementales et demande quels produits seraient les plus adaptés à la demande du fabricant.

Aucun accord trouvé

La correspondance entre Insitu et Hacking Team s'est arrêtée en mai et a été fortement retardée par des discussions d'ordre légal, chaque entreprise souhaitant utiliser son propre accord de non-divulgation avant de démarrer les discussions commerciales. Les courriels les plus récents suggèrent que les négociations n'ont jamais commencé.

Le vendeur de logiciels espions italien Hacking Team est sous pression depuis un piratage qui a conduit à la publication de plus de 400 gigabits de données confidentielles début juillet. Certains documents indiquent notamment que l'entreprise pourrait avoir vendu des solutions de surveillance à des pays sous embargo comme le Soudan et la Russie.

Source : http://www.lemonde.fr/pixels/article/2015/07/20/hacking-team-a-travaille-sur-un-drone-capable-d-infecter-des-ordinateurs-a-distance_4691260_4408996.html
Par Florian Reynaud

Ashley Madison tente de rassurer ses clients infidèles | Le Net Expert Informatique

12	Ashley Madison tente de rassurer ses clients infidèles

Alors qu'un maître-chanteur menace de diffuser un fichier de près de 40 millions d'hommes et de femmes inscrits sur Ashley Madison pour tromper leur conjoint, l'éditeur affirme qu'il a trouvé la parade : la loi américaine de protection du droit d'auteur.

Ce matin, nous rapportions que l'éditeur canadien du site de rencontres adultères Ashley Madison s'était fait pirater une base de données avec les noms de quelques 37 millions d'utilisateurs du service qui promet discrétion et anonymat. Alors qu'ils n'en ont publié que des extraits, les hackers promettent de publier l'intégralité de la base de données sur internet si la société Avid Life Media basée à Toronto ne ferme pas Ashley Madison et deux autres sites internet qu'elle édite.
Mais l'entreprise n'entend visiblement pas céder aux pressions et essaye de rassurer tant bien que faire se peut ses clients. Dans un communiqué envoyé à Numerama, Avid Life Media explique les contre-mesures mises en place, qui pourraient toutefois s'avérer vaines si les hackers décidaient de mettre leurs menaces à exécution et de passer par un réseau P2P incontrôlable comme BitTorrent pour publier la base de données intégrale. La société mise sur la loi américaine sur le droit d'auteur sur internet (le DMCA) qui impose aux plateformes de supprimer les contenus publiés sans l'autorisation des ayants droit lorsqu'elles sont notifiés. Elle estime que sa base de données est couverte par le DMCA.
Jusqu'à présent, les extraits des bases communiqués à titre de preuve du piratage ont effectivement été mis en ligne sur des sites de téléchargement direct qui acceptent de retirer les liens illicites qui leur sont notifiés, et qui l'ont fait. Mais ce ne sera pas le cas si les hackers (ou « le » hacker si l'on en croit les soupçons que porte l'entreprise sur un ancien collaborateur) décident, par exemple, de publier un simple fichier .torrent, comme l'ont fait récemment les pirates de Hacking Team. Il n'y a alors personne à qui envoyer une demande de DMCA, et/ou beaucoup de sites de liens BitTorrent qui ne les respectent pas.

Voici le communiqué reçu :
Suite à une intrusion injustifiée et criminelle dans notre système samedi 18 juillet 2015, Avid Life Media a immédiatement engagé l'une des équipes de sécurité informatique les plus pointues au monde afin de prendre toutes les mesures possibles pour résoudre cette crise.
En utilisant la Digital Millennium Copyright Act (DMCA), notre équipe a supprimé avec succès tous les messages liés à cet incident ainsi que toutes les Informations Personnelles Identifiables (PII) publiées en ligne à propos de nos utilisateurs.
La confidentialité des informations concernant nos utilisateurs a toujours été notre plus grande priorité, et nous sommes rassurés que les dispositions contenues dans le DMCA aient permis de résoudre ce problème efficacement. Notre équipe de spécialistes et de professionnels sécurité informatique, en plus de faire appliquer la loi, continuent d'enquêter sur cet incident, et nous publierons de futurs bulletins dès que de nouveaux éléments verront le jour.

Source : http://www.numerama.com/magazine/33730-quand-ashley-madison-tente-de-rassurer-ses-clients-infideles.html
Par Guillaume Champeau