Adobe : failles critiques dans Acrobat et Reader | Le Net Expert Informatique

Adobe : failles critiques dans Acrobat et Reader

Ces vulnérabilités, qui ne seraient pas exploitées, feront l'objet d'un patch salvateur ce mardi, assure l'éditeur.

Nouvelle fournée de correctifs en prévision chez Adobe. L'éditeur prévient en effet ses utilisateurs qu'Acrobat et Reader sont victimes de failles critiques, permettant donc une prise de contrôle à distance. Un ou plusieurs patchs seront distribués ce mardi.
Adobe ne précise pas la teneur de ces vulnérabilités mais assure qu'elles ne sont pas exploitées. Adobe Acrobat XI et Reader XI (11.0.10 et versions précédentes), ainsi qu'Adobe Acrobat X et Reader X (10.1.13 et versions précédentes) pour Windows et OS X sont concernés.

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

Source : http://www.zdnet.fr/actualites/adobe-failles-critiques-dans-acrobat-et-reader-39819162.htm

Propriétaires de sites WordPress : attention aux »script-kiddies » pro-Etat Islamique | Le Net Expert Informatique

Le FBI alerte sur les attaques continues de défacement visant des sites Internet. Les victimes ont en commun d'utiliser des plugins WordPress vulnérables. Quant aux auteurs, ils utilisent le nom de l'EI par souci de visibilité.

En janvier, suite aux attentats en région parisienne, de très nombreuses attaques de défacement de sites Web avaient été constatées. Ces opérations de cybervandalisme étaient revendiquées par des partisans des islamistes radicaux, et notamment de l'Etat Islamique (Daesh).
« La très grande majorité de ces attaques sont des défigurations de sites Internet (ou défacement), ou des dénis de service (DDoS) qui exploitent les failles de sécurité de sites vulnérables » précisait alors l'Anssi.

Des cibles choisies pour leur usage de plugins WordPress
De telles attaques se poursuivent et pas seulement en France. Et elles ont souvent une cible de prédilection : les sites WordPress. Les Etats-Unis, par l'intermédiaire du FBI, viennent d'ailleurs de publier un bulletin de sécurité concernant ces attaques.
Certes, note le FBI, ces « défacements traduisent un faible niveau de sophistication » mais ils s'avèrent néanmoins coûteux en raison des pertes d'activité et des dépenses qu'ils génèrent afin de réparer les systèmes infectés.
Quant aux victimes de ces intrusions, elles sont très diverses. Et pour cause puisque les attaquants ciblent moins les propriétaires des sites que la plateforme technique de ceux-ci. Les victimes ont un point commun : l'utilisation de plugins WordPress vulnérables.

Les pirates pas membres de Daesh
« Le FBI estime que les auteurs ne sont pas des membres de l'organisation terroriste Etat Islamique. Ces individus sont des hackers exploitant des méthodes relativement simples afin d'exploiter des vulnérabilités techniques et utilisent le nom ISIS pour gagner plus de notoriété que l'attaque sous-jacente aurait autrement recueilli. »
C'était déjà l'analyse publiée par ZDNet en janvier. « Nous n'avons constaté aucune excentricité ou coordination dans les attaques, ni de déni de service bien outillé » confiait Loïc Guézo, expert en sécurité chez Trend Micro. « Le résultat est surtout visuel, c'est une volonté de communiquer » par des défacements.
Quant au profil des attaquants, il était « plutôt celui de personnes avec des compétences de base, au sens de la gestion du PC et de certains outils » ajoutait-il. Ils s'apparenteraient ainsi à des « script kiddies » plutôt qu'à des hackers chevronnés.

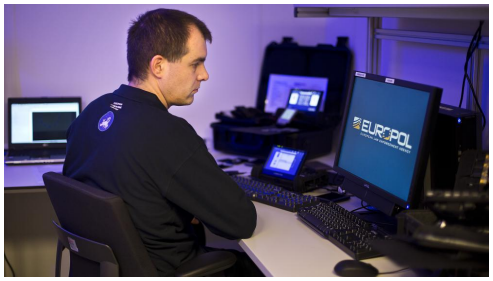
Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.zdnet.fr/actualites/proprietaires-de-sites-wordpress-attention-aux-script-kiddies-pro-etat-islamique-39817644.htm
Par Christophe Auffray

Cybercriminalité : trois techniques en vogue chez les

pirates | Le Net Expert Informatique

15

	**Cybercriminalité : trois techniques en vogue chez les pirates**

Avez-vous déjà entendu parler de « rançongiciels » ? Le rapport annuel de la société américaine de sécurité informatique Symantec, publié mardi 14 avril, assure que le recours à ce type de programmes malveillants parmi d'autres est de plus en plus fréquent. « De manière générale, la cybercriminalité a encore crû en 2014, avec 317 millions de nouveaux programmes malveillants créés au niveau mondial, soit près d'un million par jour », explique à l'AFP Laurent Heslault, expert en cybersécurité de Symantec et Norton.

La France progresse d'une place et passe donc au 14e rang mondial (6e rang européen) des pays où la cybercriminalité est la plus active, selon le rapport. **Au niveau mondial, cinq grandes entreprises sur six ont été attaquées en 2014**, soit une progression de **40 % sur un an**, avance Symantec. Francetv info vous présente certaines techniques d'attaque remarquées en 2014.

Viser les éditeurs de logiciels

Les pirates ne sont pas toujours là où on les cherche. Alors que les entreprises se méfient de plus en plus des vols de mots de passe et des usurpations d'identité de leurs employés, les cybercriminels changent de tactique, selon le rapport de Symantec. Pour échapper à toute détection, ils détournent les infrastructures des grandes entreprises, pour les utiliser contre elles.

« Beaucoup sont capables de faire s'auto-infecter les infrastructures des entreprises, via des 'chevaux de Troie', lors de mises à jour de logiciels standards, et d'attendre ensuite patiemment que leurs cibles téléchargent ces mises à jour infectées, leur donnant ainsi libre accès au réseau de l'entreprise », détaille Laurent Heslault. Les cyberattaquants ciblent donc de plus en plus les fournisseurs des grandes entreprises, comme les éditeurs de logiciels.

Réclamer des rançons

Les « rançongiciels » ont plus que doublé dans le monde en 2014, selon le rapport de Symantec. Ces logiciels malveillants prennent le contrôle des PC, tablettes et smartphones et les utilisateurs se voient ensuite réclamer de l'argent pour pouvoir à nouveau utiliser leur machine. **L'an dernier, l'utilisation de ce type de programme (appelé en anglais « ransomware ») a augmenté de 113%**.

Sa variante, dite « cryptolocker », qui retient en otage les données personnelles, a fait 45 fois plus de victimes qu'en 2013. Dans ce système, si la rançon n'est pas payée au terme d'un compte à rebours, les données de la victime sont détruites. « Là où un particulier doit payer 300 euros, une entreprise française s'est vu réclamer 90 000 euros pour récupérer 17 téraoctets de données », relèvent Les Echos.

Miser sur les vulnérabilités encore non détectées

L'année 2014 aura connu un record avec 24 découvertes de vulnérabilités « zero day », c'est-à-dire des pirates qui utilisent des failles non détectées jusque-là dans un logiciel. Ces vulnérabilités entraînent un délai de réponse fortement accru et donc offrent plus de temps aux pirates pour s'en servir.

« Il aura fallu en moyenne 59 jours aux éditeurs de logiciels pour créer et déployer des correctifs [en 2014] alors qu'ils en avaient besoin de seulement quatre en 2013 », relève Laurent Heslault.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.francetvinfo.fr/internet/cybercriminalite-trois-techniques-en-vogue-chez-les-pirates_876373.html
Par Par Yann Thompson

Est-ce que l’iPhone est vulnérable ? | Le Net Expert Informatique

	**Est-ce que l’iPhone est vulnérable ?**

Est-ce que les iPhone sont vulnérables à l'espionnage, c'est la question que l'on peut se poser en sachant que la CIA cherche à le casser depuis sa création.

Selon la récente publication de The Intercept, on sait que la CIA a tenté de « casser », percé le chiffrement, des produits Apple depuis 2006. Cela signifie que l'agence américaine a bien évidemment aussi tenté de percer les sécurités de l'iPhone vu que la première édition est sortie en 2007. La grande question est de savoir si la CIA est arrivée à ses fins.
Sans revenir sur tous les détails de cette révélation faite sur la base des documents dévoilés par Edward Snowden, on peut comprendre de nombreuses choses à partir de cette nouvelle affaire d'espionnage des utilisateurs.
Pour commencer, il n'y avait pas que la NSA qui cherchait à collecter des données personnelles des utilisateurs de smartphones. Alors que les lois américaines empêchent normalement l'espionnage des citoyens américains, on peut sérieusement se poser la question si ces textes n'ont pas tout simplement été bafoués en essayant de casser le chiffrement des iPhone alors que les Américains sont friands de produits Apple.
Si découvrir des failles dans les systèmes Apple s'explique par le fait de vouloir obtenir des données des utilisateurs, on peut se poser la question de savoir pourquoi la CIA n'a pas averti Apple de l'existence de ces failles ? Il semble évident que cela aurait été un aveu de culpabilité. Par contre, un peu prendre cet aspect d'un autre point vu en considérant que ce que les agences américaines ont fait, d'autres agences de pays hostiles ont également pu le faire. De fait, ne pas communiquer ces failles serait une mise en danger des données personnelles des citoyens américains.
En sachant tout cela, on comprend parfaitement pourquoi les constructeurs, notamment Apple, ont renforcé la sécurité de leurs systèmes et refusent d'ouvrir des backdoors « légales » pour les autorités. En effet, comment pourrait-il exister une moindre confiance ?
En sachant tout cela, on ne comprend par contre pas la véhémence des agences américaines qui dénoncent les méthodes de cryptage mises en place par les entreprises. En effet, ces mesures ne visent que la protection des données des utilisateurs, notamment des biens appartenant à des Américains.
Au final, le débat sur la protection des données personnelles va encore faire couler beaucoup d'encre.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.linformatique.org/est-ce-que-liphone-est-vulnerable/

Sécurité : OS X et iOS auraient été les systèmes les plus vulnérables en 2014

Sécurité : OS X et iOS auraient été les systèmes les plus vulnérables en 2014

Le spécialiste des solutions de sécurité GFI a publié un nouveau rapport mesurant le degré de vulnérabilité des systèmes d'exploitation en 2014. L'OS de Microsoft ne ferait plus partie du top 3.

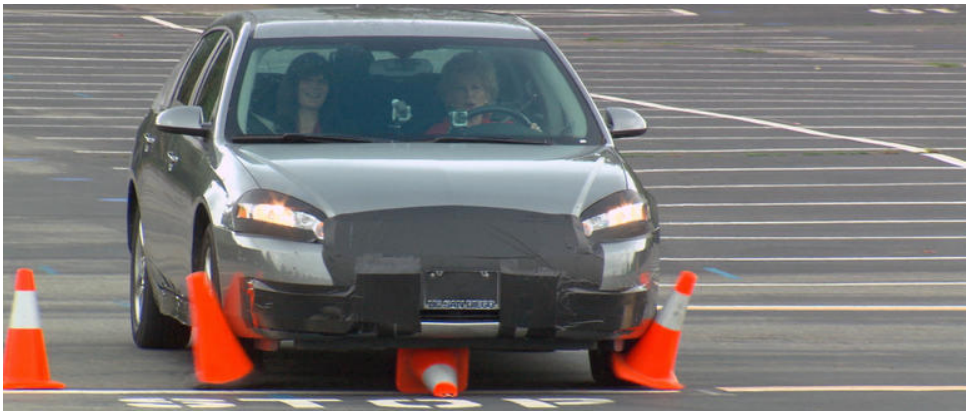
Au sein de la base de vulnérabilités nationale hébergée par le gouvernement américain, 7038 vulnérabilités auraient été rapportées au total en 2014, à raison de 19 par jour en moyenne, selon GFI. Celles-ci concernent aussi bien les systèmes d'exploitation que les applications. A titre de comparaison, en 2013, 4794 failles avaient été ajoutées.
L'année dernière 24% de ces vulnérabilités ont été jugées sérieuses, soit 1887 contre 1492 l'année précédente. Selon GFI, les applications seraient responsables pour 83% de ces failles de sécurité contre 13% pour les systèmes d'exploitation eux-mêmes et 4% pour le matériel.
C'est OS X qui se trouve en pôle position des systèmes vulnérables avec 147 mentions saisies au sein de la base de données dont 64 jugées importantes. En seconde place, nous retrouvons iOS avec 127 failles devant le kernel de Linux. « Bien que les systèmes de Microsoft ont toujours un nombre considérable de vulnérabilités, il est intéressant de noter qu'ils ne sont plus dans le top 3 », affirme GFI. Reste que combinés, Windows Server 2008 et 2013 ainsi que Windows Vista, 7, 8, 8.1 et RT détiennent au total 4010 failles rapportées dont 168 importantes.
Les navigateurs trônent en tête des logiciels les moins sécurisés avec, en première place du palmarès, Internet Explorer suivi de Chrome et Firefox. Le plugin Flash Player et la plateforme Java sont respectivement en quatrième et cinquième place devant le client mail Thunderbird.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

S o u r c e :
http://pro.clubic.com/it-business/securite-et-donnees/actualite-755309-securite-os-ios-auraient-systemes-vulnerables-2014.html?&xvc_mode=M&xvc_campaign=NL_ClubicPro_New_24/02/2015&partner=-&xvc_position=873687217&xvc_misc=-&crmID=639453874_873687217&estat_url=http%3A%2F%2Fpro.clubic.com%2Fit-business%2Fsecurite-et-donnees%2Factualite-755309-securite-os-ios-auraient-systemes-vulnerables-2014.html

---

Voitures connectées faciles à hacker



Voitures connectées faciles à hacker

Les promesses de la voiture connectée font rêver : sans conducteur, intelligente,… mais visiblement, elle est aussi facile à pirater. Un hackeur en prend ici le contrôle, faisant du véhicule un danger pour ses passagers. Dans son émission « 60 minutes », CBS News consacre un dossier aux voitures connectées et à leurs failles de sécurité. Kathleen Fisher, experte de la DARPA (Defense Advanced Research Projects Agency) présente la voiture connectée comme un « ordinateur sur roues », soulignant de fait la possibilité de hacker le véhicule.

Démonstration à l'appui : il est en effet possible de contrôler la voiture à distance, à l'aide d'un simple ordinateur portable. Si déclencher les essuie-glaces ou le klaxon peut sembler « inoffensif », quand le hackeur prend contrôle des freins, c'est tout de suite plus inquiétant. Ici, il ne s'agit que de plots en plastique, mais on imagine rapidement les dégâts si une voiture connectée perdait les pédales « dans la vraie vie ».

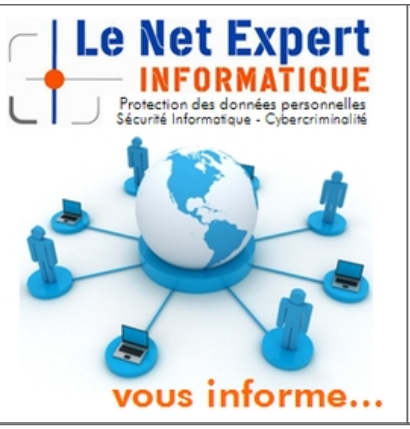
Plus tôt cette semaine, le sénateur américain Edward J. Markey a sorti un rapport sur les dangers des voitures connectées. Il y compile les données fournies par 16 constructeurs automobiles dont BMW, Fiat Chrysler, Ford, General Motors, Nissan, Mitsubishi ou Mercedes-Benz après qu'il leur ait adressé une lettre et un questionnaire en décembre 2013. Certains constructeurs dont Tesla ont cependant refusé de lui répondre… Selon ses résultats, aucune mesure ne serait mise en place pour détecter et empêcher les tentatives de piratage ou les vols de données. Par ailleurs, outre la sécurité, le rapport revient aussi sur les problèmes de confidentialité des données : les propriétaires de voitures connectés ne seraient pas au courant de tout ce qui est enregistré à leur propos… De quoi faire réfléchir avant d'investir dans la voiture du futur.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.ladn.eu/actualites/pop-insight,voitures-connectees-faciles-hacker,74,24953.html

---

Bases de données : près de 40.000 failles découvertes par des étudiants sarrois



Bases de données : près de 40.000 failles découvertes par des étudiants sarrois

Des étudiants du « Center for IT-Security, Privacy and Accountability » de Sarrebruck (CISPA – Sarre) ont récemment révélé des failles de sécurité portant sur 40.000 bases de données. Ces données, portant sur des entreprises basées en France et en Allemagne, listent des noms, adresses et courriels de millions de clients.

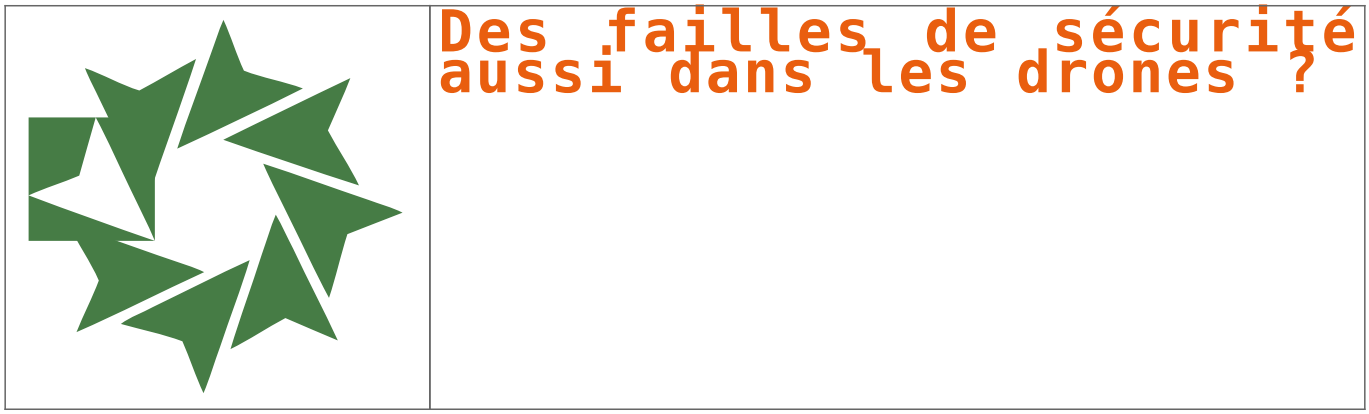
La cause en est une base de données open source mal configurée, utilisée par de nombreux sites de vente en ligne. Si les opérateurs adoptent les paramètres par défaut de ces bases, les données sont alors disponibles en ligne sans protection. Plus grave encore, ces données peuvent être modifiées. Or le fournisseur de la base de données, MongoDB Inc., est l'un des acteurs majeurs du secteur au niveau mondial. Les étudiants à l'origine de cette découverte ont ensuite interrogé un moteur de recherche public pour identifier les entreprises utilisant ces bases de données non protégées.
Selon le CISPA, les étudiants ont notamment détecté une base de données qui pourrait appartenir à un opérateur français de télécommunication, contenant les adresses et numéros de téléphones de huit millions de clients, en France et en Allemagne. Ils ont également identifié la base de données d'un site de commerce en ligne, comprenant des informations de paiement. Ces données facilitent, pour des personnes mal intentionnées, l'usurpation d'identité en ligne. A ce titre, le CISPA a contacté différentes autorités chargées de la protection des données (les « Computer Emergency Response Teams – CERTs », la Commission nationale de l'informatique et des libertés – CNIL, et le Bureau allemand pour la sécurité de l'information – BSI. Le fournisseur a également été informé des problèmes générés par une mauvaise configuration des bases de données par les entreprises clientes.
Le CISPA, rattaché à l'Université de la Sarre, a été fondé en 2011 par le Ministère fédéral de l'enseignement et de la recherche (BMBF) en tant que centre de compétence pour la cybersécurité. En plus de l'Université de la Sarre, l'Institut Max Planck pour l'informatique (MPII), l'Institut Max Planck pour les systèmes logiciels (MPI-SWS), ainsi que le Centre allemand de recherche sur l'intelligence artificielle (DFKI) travaillent conjointement au sein du CISPA. Avec environ 200 chercheurs, le centre est l'un des plus grands centres de recherche sur la cybersécurité en Europe.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.bulletins-electroniques.com/actualites/77892.htm

Des failles de sécurité aussi dans les drones ?

28



Un chercheur indien croit avoir décelé une faille de sécurité lui permettant de prendre le contrôle d'un drone Parrot. Il a mis au point un malware capable de prendre le contrôle de l'appareil à distance et de modifier les instructions de vol.

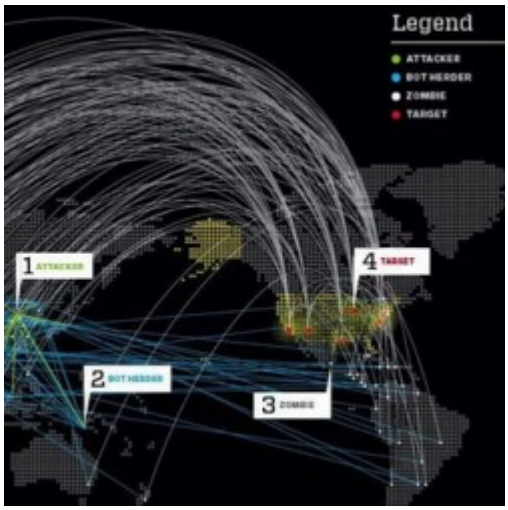
Les drones, comme à peu près tout ce qui repose de près ou de loin sur les technologies numériques, ne sont pas exemptés de failles de sécurité. Le chercheur indien Rahul Sasi s'est lancé le défi de prendre le contrôle à distance d'un drone fabriqué par Parrot et pense y être parvenu, à l'aide d'un malware conçu par ses soins et sobrement baptisé Maldrone.
Rahul Sasi n'a pas encore publié de prototype détaillé de sa méthode, mais explique sur une page web la façon dont il a procédé et accompagne le tout d'une petite vidéo de son programme en action.
La faille trouvée par le chercheur indien lui permet de prendre dans une certaine mesure le contrôle de l'appareil en profitant d'une faille de sécurité du programme d'autopilotage du drone. En jouant avec les processus d'échanges d'informations entre les différents capteurs du drone et le programme d'autopilote, le pirate est capable de prendre la main sur un drone, et ce à distance.

Nos drones sont-ils dignes de confiance ?
Selon Rahul Sasi, la backdoor ainsi mise en place est du genre tenace et un simple reboot du drone ne suffit pas à s'en débarrasser, conférant à l'attaquant un accès persistant au système de contrôle du drone. Rahul Sasi explique que son malware est également capable de s'auto-répliquer et de se propager à d'autres drones.
Potentiellement inquiétant, le malware développé par le chercheur ne cherche néanmoins pas à nuire particulièrement aux utilisateurs mais a été crée dans un simple but de recherche et par pure curiosité selon Rahul Sasi. On peut donc écarter pour le moment la possibilité de voir un groupe de cybercriminels pirater à distance une armée de drones civils afin de faire passer de la drogue en douce à la frontière à l'insu de leurs propriétaires.
Mais pour l'instant, on prendra quelques pincettes : il faudra attendre le 7 février pour disposer de plus d'informations techniques sur le sujet, date à laquelle Rahul Sasi prévoit de revenir plus en profondeur sur son hack à l'occasion de la conférence Nullcon. Nous avons contacté Parrot à ce sujet et nous mettrons à jour cet article si la société souhaite réagir à cette annonce.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.zdnet.fr/actualites/les-drones-aussi-ont-des-failles-de-securite-39813694.htm
Par Louis Adam

500 000 PC infectés à cause d’une faille Windows XP



500 000 PC infectés à cause d’une faille Windows XP

Selon les chercheurs en sécurité de Proofpoint, 52% des PC infectés par le botnet Qbot font tourner Windows XP. Exploitant une faille de Windows XP mais également de Seven et Vista, un groupe de cybercriminels russe a réussi à activer le botnet Qbot fort 500 000 PC zombies, essentiellement localisés aux Etats-Unis. Son objectif : Aspirer les identifiants bancaires des utilisateurs de ces PC corrompus.

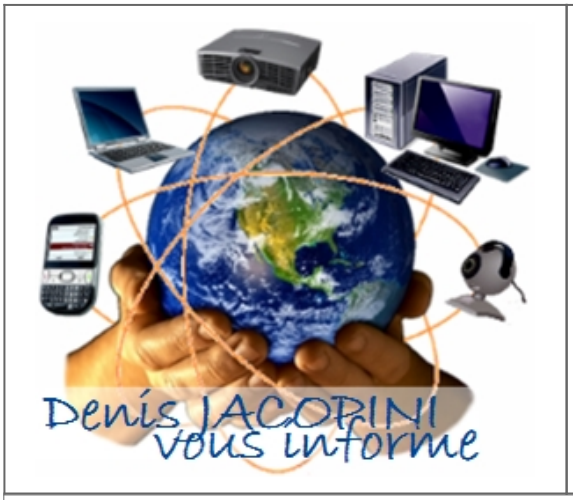
Des pirates russes à l’origine du botnet Qbot ont construit une impressionnante armée de 500 000 PC zombies en exploitant des failles non corrigées dans des ordinateurs tournant sous Windows XP mais également Windows 7 et Vista. Des PC localisés principalement aux Etats-Unis, a fait savoir la société Proofpoint. Ces derniers temps, les hackers russes ont fait monter la pression avec des incursions sérieuses telle que l’attaque qui a visé la banque américaine JPMorgan Chase. Avec ce botnet, baptisé Qbot, les chercheurs de Proofpoint ont fait ressortir que le groupe qui est à l’origine de sa création l’a élaboré de façon méticuleuse à travers le temps, sans faire de vague, au point de rester sous les radars des sociétés de sécurité et donc de ne pas avoir attiré leur attention.

Selon Proofpoint, 75% des 500 000 PC infectés par le botnet Qbot sont situés aux Etats-Unis, sachant que parmi eux, 52% font tourner Windows XP, 39% Windows 7 et 7% Windows Vista. En Grande-Bretagne, la proportion de PC infectés est bien moindre, 15 000 postes environ. « Avec 500 000 clients infectés volant les identifiants des comptes bancaires en ligne des utilisateurs, le groupe de cybercriminels a le potentiel pour réaliser des bénéfices vertigineux », ont indiqué les chercheurs de la société de conseil en sécurité. Mais le botnet Qbot ne s’attaque pas seulement aux comptes bancaires, il compromet également les sites WordPress, soit en infectant le site lui-même ou bien en injectant des contenus corrompus dans leurs newsletters.
Article de Dominique Filippone

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

Source :
http://www.lemondeinformatique.fr/actualites/lire-500-000-pc-infectes-a-cause-d-une-faille-windows-xp-58878.html

Google monte une équipe de supers hackers pour traquer les failles informatiques



Une équipe de supers hackers pour traquer les failles informatiques

Google veut éradiquer les bugs qui peuvent être exploités par les pirates, mais aussi le gouvernement.

On croirait lire le scénario d'un film d'espionnage. Google a annoncé la création d'une équipe spéciale chargée de traquer les failles informatiques. Dénommée Project Zero, cette nouvelle équipe de sécurité sera composée des meilleurs hackers. Parmi eux, George Hortz, un Américain de 24 ans, surtout connu pour avoir piraté l'écran verrouillé de l'iPhone à l'âge de 17 ans et la Playstation 3, raconte le magazine spécialisé Wired. Quand il a découvert, au début de l'année, des failles dans le système d'exploitation de Google, Chrome OS, l'entreprise l'a payé 150.000 dollars pour les corriger. Outre Hortz, Project Zero accueille d'autres hackers célèbres, et Chris Evans , le recruteur du projet, continue de chercher des talents.

Project Zero sera chargée de trouver les failles dîtes «zero-day», c'est à dire des vulnérabilités qui n'ont pour l'instant jamais été découvertes et peuvent être dangereuses si elles sont exploitées par des pirates. L'équipe travaillera sur n'importe quel produit, et donc pas uniquement sur ceux de Google. «Nous ne posons pas de limite particulière à ce projet et travaillerons à l'amélioration de la sécurité de n'importe quel programme informatique utilisé par de nombreuses personnes. Nous porteront une grande attention aux techniques, aux cibles et aux motivations des attaquants», explique Chris Evans dans son communiqué.

Une réponse de Google à Heartbleed

Ce projet de Google arrive après Heartbleed, la faille de sécurité qui a secoué Internet il y a quelques mois. Fin avril déjà, l'entreprise s'associait à Facebook, Microsoft et d'autres pour lancer la Core Infrastructure Initiative. Un regroupement qui finance les projets Open Source en difficulté financière, et donc ceux qui seraient le plus exposés à une faille de sécurité passée inaperçue. Project Zero c'est aussi la réponse de Google à la NSA. La firme a mal encaissé les failles utilisées par l'agence américaine pour espionner ses utilisateurs. Google a déjà mis en place de nouveaux mécanismes de sécurité pour mieux protéger ses données.

Le mythe des hackers embauchés par les entreprises dont ils révèlent les failles n'est pas nouveau. En 2011, Apple embauchait Nicholas Allegra. À 19 ans, il était un membre éminent de la communauté du jailbreaking, c'est à dire du débridage d'iOS (le système d'exploitation des iPads et iPhones). Un an plus tard, la firme embauchait Kristin Paget dans son équipe de sécurité. Cette informaticienne avait longtemps fait partie d'un groupe de hackers éminents qui avait révélé des failles chez Microsoft.

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

Références :

http://www.lefigaro.fr/secteur/high-tech/2014/07/16/01007-20140716ARTFIG00221-google-monte-une-equipe-de-supers-hackers-pour-traquer-les-failles-informatiques.php