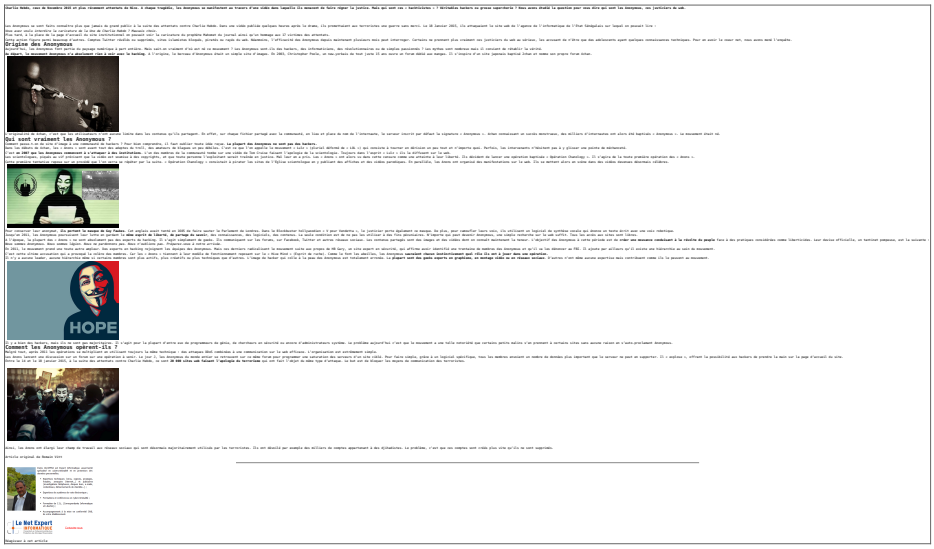
Qui sont vraiment les Anonymous, ces justiciers du web ?

Qui sont vraiment les Anonymous, ces justiciers du web ?



Original de l’article mis en page : Anonymous : qui sont vraiment ces justiciers du web ?

L’ANSSI alerte sur les risques liés à Pokémon Go

L’ANSSI alerte sur les risques liés à Pokémon Go

Face au phénomène Pokémon Go, l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'information) a publié un bulletin de sécurité sur l'installation et l'usage de cette application.

Devant l'ampleur du phénomène (près de 100 millions de téléchargements), l'application Pokémon Go pose quelques problèmes de sécurité. L'ANSSI (en quelque sorte le Gardien de la sécurité des Systèmes d'Information des Organisme d'Importance Vitale, des Organes et Entreprise de l'état Français selon Denis JACOPINI expert Informatique assermenté spécialisé en cybercriminalité) ne pouvait pas rester sourde à cette question et vient de publier via le CERT-FR un bulletin de sécurité dédié aux « *cyber-risques liés à l'installation et l'usage de l'application Pokémon Go* ».

Applications malveillantes et collectes de données

Dans ce bulletin, il est rappelé qu'avec le succès, de nombreuses fausses applications se sont créées. Le CERT-FR en a recensé 215 au 15 juillet 2016. Elles sont surtout présentes dans les pays où le jeu n'est pas présent. Il recommande donc de ne pas télécharger cette application sur des sites tiers, et de n'installer que les versions originales disponibles sur Google Play ou l'Apple Store. Nous nous étions fait l'écho de la disponibilité d'APK Pokémon Go pour Android qui contenait des malwares. Le bulletin constate aussi que Niantic a résolu le problème de permission qui exigeait un accès complet au profil Google de l'utilisateur.

Sur les données personnelles, l'ANSSI observe comme beaucoup d'autres organisations que Pokémon Go collecte en permanence de nombreuses données personnelles. Informations d'identité liées à un compte Google, position du joueur par GPS, etc. L'UFC-Que Choisir avait récemment alerté sur cette question de la collecte des données. La semaine dernière la CNIL a publié un document concernant « jeux sur votre smartphone, quand c'est gratuit… » où elle constatait que ce type d'application était très gourmande en données. L'ANSSI préconise la désactivation du mode « réalité augmentée » lors de la phase de capture d'un Pokémon.

BYOD et Pokémon Go, le pouvoir de dire non

L'ANSSI répond sur le lien qu'il peut y avoir entre le BYOD (Bring Your Own Device), c'est-à-dire l'utilisation de son terminal personnel dans un cadre professionnel et Pokémon Go. Le CERT-FR constate qu'il est « *tentant d'utiliser un ordiphone professionnel pour augmenter les chances de capturer un Ronflex (un Pokémon rare à trouver)* ». Surtout quand la demande émane d'un VIP et qu'il est souvent difficile de refuser. Eh bien comme Patrick Pailloux (prédécesseur de Guillaume Poupard à la tête de l'ANSSI) l'avait dit en son temps, il faut avoir le pouvoir de dire non à l'installation de ce type d'application dans un environnement professionnel.

Toujours dans le cadre du travail, l'agence déconseille l'usage de l'application dans des lieux où le geo-tagging du joueur pourrait avoir des conséquences (lieu de travail, sites sensibles).

Article original de Jacques Cheminat

Réagissez à cet article

Original de l’article mis en page : L’ANSSI alerte sur les risques liés à Pokémon Go

---

#PokemonGo hacké en moins de 2h…

#PokemonGo hacké en moins de 2h…

Suricate Concept, un GIE (Groupement d'Intérêt Economique) spécialisé dans la cyber-sécurité, a publié un rapport de 10 pages sur des failles de sécurité majeures identifiées dans le nouveau phénomène de société « Pokemon Go », après avoir réussi à pirater le jeu en un temps record.

L'étude intitulée « Comment on a hacké Pokemon Go en moins de 2h… » explique en détails comment l'équipe d'experts en cyber-sécurité s'est penché par hasard sur l'application et a rapidement identifié des failles qui permettaient aux joueurs de gagner des niveaux sans efforts en manipulant le programme.

Monir Morouche, à la tête du département cyber-sécurité et Président du GIE Suricate Concept a déclaré : « Chez Suricate Concept, tous les jours nous nous battons pour rendre le web un endroit plus sur et pour protéger les données et la vie privée des utilisateurs ainsi que les ressources en ligne de nos clients. Lorsque l'on a découvert Pokemon Go, complètement par hasard, on voulait savoir si le programme avait été suffisamment sécurisé par ses développeurs et si nous serions capable de trouver des failles dans l'application « .

Ce qui débuta comme un challenge interne au détour d'une pause de travail devint rapidement la base pour une étude plus poussée lorsque l'équipe réalise comment ils parvenaient facilement à manipuler le programme, générant ainsi des gains de niveaux et de ressources rapides pour un joueur à qui il faudrait normalement plusieurs semaines d'efforts pour y parvenir.

« Au sein de l'équipe, nous sommes toujours en train de nous challenger les uns les autres lorsque que quelque chose de nouveau dans l'univers du web ou des nouvelles technologies apparait. Pokemon Go était un sujet d'étude rêvé, du fait qu'il était présent partout dans l'actualité. Nous ne pouvions pas passer à côté. Dans toutes les démonstrations de hacking que nous conduisons, l'objectif premier est de sensibiliser les utilisateurs aux risques encourus et les éduquer sur comment être un utilisateur du web responsable », poursuit Monir Morouche.

L'étude publiée par Suricate Concept inclut une analyse technique de la façon dont l'équipe a procédé au hack en contournant les systèmes de sécurité existant du jeu, sans pour autant dévoiler tous les détails, qui « seront mis à disposition des développeurs de Pokemon Go sur demande » a indiqué Monir Morouche. Cela afin de que ces derniers ne soient pas utilisés à mauvais escient par des joueurs ou hackers mal intentionnés. Il ne s'agit pas du premier coup d'essai de la team Suricate Concept qui régulièrement au travers de démonstrations choc met en avant des failles de sécurité dans des services en ligne, ou objets connectés utilisés quotidiennement par le public. On peut par exemple citer parmi leurs récents travaux le hacking du moteur de recherche Google ou celui des cartes de paiement sans contact.

Suricate Concept a également annoncé il y a quelques mois lors du dernier Forum International de la Cyber-sécurité avoir réussi à hacker un objet médical connecté , un pace-maker, afin d'en prendre le contrôle complet. La démonstration a été dévoilée dans une vidéo avec un scénario d'inspiration hollywoodienne intitulée « The hacking dead » , en rapport avec la série à succès The Walking Dead.

Article original de

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet…) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Original de l'article mis en page : Lille, 28 Juillet 2016 – Communiqué de presse: « Comment on a hacké PokemonGo en moins de 2h… » | Farouk JEBALI | LinkedIn

---

L'application Telegram a aussi sa faille

L'application Telegram a aussi sa faille

Un chercheur a trouvé une faille de sécurité sur la version Mac de Telegram. L'éditeur minimise l'importance de cette vulnérabilité.

Une grave affaire prise à la légère ou, au contraire, beaucoup de bruit pour rien ? Les avis sont partagés à propos de la faille de sécurité découverte sur **Telegram** par le dénommé Kirill Firsov.
Ce chercheur russe s'est aperçu que la version Mac du service sécurisé de messagerie enregistrait, dans les journaux système (*syslog*), chaque message collé dans le champ de discussion depuis le presse-papiers. Le 23 juillet, il avait, sur Twitter, interpellé Pavel Durov, cofondateur du service avec son frère Nikolai.
S'est ensuivi un échange de tweets à l'issue duquel le bug a été résolu… sans qu'on puisse mesurer quelle était sa réelle ampleur. L'explication entre les deux hommes s'est effectivement terminée sur un « Imagine que la police saisisse ton ordinateur portable et qu'elle retrouve trace de tes messages 'secrets' dans syslog » lancé par Kirill Firsov.

La sandbox pour limiter les dégâts

Pour Pavel Durov, la vulnérabilité, repérée sur les versions 2.16 et 2.17 de Telegram, n'est pas aussi importante qu'elle en a l'air : n'est concerné que le texte collé depuis le presse-papiers… auquel toutes les autres applications Mac ont accès.
Sans nier cet état de fait, Kirill Firsov avait pointé du doigt le fait que les messages font l'objet d'une journalisation. Ce à quoi Pavel Durov avait répondu qu'avec le mécanisme dit de « bac à sable » (*sandbox*), les applications téléchargées sur l'App Store d'OS X – à l'image de Telegram – ne peuvent qu'écrire dans *syslog* ; pas y accéder en lecture (voir, à ce propos, la documentation d'Apple).
Bilan pour celui qui a financé Telegram via son fonds Digital Fortress, corriger la faille revient juste à éliminer une redondance : le fait que toutes les applications peuvent accéder au contenu du presse-papiers.

Le service qui monte

L'histoire de Telegram est particulière. Ses fondateurs s'étaient installés à Berlin après avoir, sur fond de lutte d'influence politique avec l'entourage de Vladimir Poutine, perdu le contrôle du réseau social vKontakte, qu'ils avaient créé en Russie.
Utilisé à l'origine par les seules équipes de vKontakte, Telegram avait basculé, en 2013, dans une exploitation ouverte au grand public.
En insistant sur la dimension de confidentialité des échanges, le service a dépassé, fin février, les 100 millions d'utilisateurs actifs par mois, souligne ITespresso.
Une ascension qui n'a pas laissé la concurrence indifférente. Illustration chez WhatsApp, qui avait décidé, fin 2015, de bloquer, sur Android, les liens vers l'application Telegram diffusés par ses utilisateurs.
Le service, qui exploite un protocole de chiffrement maison (MTProto), a aussi été mis en lumière pour des considérations plus sombres : selon Trend Micro, 34 % des organisations terroristes l'utilisent comme point de contact.
Article original de Silicon

Réagissez à cet article

Original de l’article mis en page : Sécurité : Telegram, une vulnérabilité qui prête à discussion

---

Piratage de 1,6 million de comptes Clash of King

Piratage de 1,6 million de comptes Clash of King

Pour ne pas avoir corrigé une faille vieille de 3 ans, le jeu Clash of King se retrouve avec 1,6 million de comptes de joueurs dans la nature.

vBulletin, un framework (un outil Internet NDR) de forum très utilisé sur le réseau des réseau a subi à plusieurs reprises des failles de sécurité. Des « bugs » que s'empressent d'utiliser les pirates informatique. La dernière campagne malveillante officielle visant ce forum concerne la société Elex qui produit le jeu sur mobile « Clash of Kings ». Ce jeu est utilisé par des millions de joueurs sur les plateformes mobiles. Ces joueurs s'enregistrent sur le forum afin d'échanger avec d'autres utilisateurs.
Le pirate a profité d'une faille vBulletin connue pourtant depuis 2013. Comme le rappel Matthieu Dierick, de chez F5 Networks, les failles ne sont pas nouvelles et l'ANSSI avait déjà alerté les autorités au sujet de vBulletin. Bref, si vous ne patchez pas, il ne faut pas pleurer ! vBulletin n'est pas responsable du fait que les entreprises ne programment pas leur mise à jour.
Pour détecter si un serveur est vulnérable, il suffit de lancer une requête HTTP sur une liste de serveurs et d'attendre un code retour. Voici un exemple de requête utilisée pour détecter la vulnérabilité d'un serveur : *h t t p : / / [l ' u r l d u site]/ajax/api/hook/decodeArguments?arguments=O:12: »vB_dB_Result »:2{s:5: »*db »;O:11: »vB_Database »:1:{s:9: »functions »;a:1{s:11: »free_result »;s:6: »assert »;}}s:12: »*recordset »;s:20: »print_r(md5(92829)) »;}.*
Si le code retour contenait le hash 92829, alors l'espace numérique est vulnérable. C'est l'action qu'a orchestré le pirate de Clash of King. C'est la recherche qu'aurait du faire les équipes de Clash of King pour se protéger et sécuriser les utilisateurs.
Nous ne connaissons pas encore la vulnérabilité exploitée mais lors des dernières campagnes de piratage sur vBulletin, les pirates ont réussi à envoyer leur SHELL (Outil installé dans le serveur qui permet au pirate d'être maître de l'espace infiltré, NDR) sur le serveur et a exécuter des requêtes SQL en mode « root ». Pour cela, ils passaient par des fonctions PHP, par exemple la fonction system() qui permet l'exécution de commande shell.

Mot de passe hashé ? la belle affaire !
Les données volées concernent les identifiants avec mot de passe hashé, l'adresse mail, l'adresse IP et les tokens liés aux réseaux sociaux. Par hashé, comprenez que le mot de passe ne se lit plus directement (ZATAZ se transforme en hashé md5 par *79e35664717c21b96225d8d6ed4f0b16*). Les utilisateurs du forum doivent donc changer leur mot de passe même si ceux-ci étaient rendus illisibles au niveau de la base de données. Le hash MD5 ne sertb à rien si un mot de passe trop simple a été enregistré. Reprenons mon exemple avec *79e35664717c21b96225d8d6ed4f0b16*. Allez sur le site crackstation.net et rentrez *79e35664717c21b96225d8d6ed4f0b16*. En quelques millièmes de secondes, le mot de passe hashé n'est plus illisible. Pour une meilleure sécurité, dirigez-vous plutôt vers bcrypt !
« ***Toute infrastructure de données doit être protégée par des mécanismes d'analyse de niveau 7 tels que les Firewall Applicatifs ou Web Application Firewall.*** Indique Matthieu Dierick (Il commercialise ce genre d'outil, NDR). ***Cela peut empêcher un pirate de lancer des commandes sur un serveur même si celui-ci est concerné par une faille de sécurité***« . La politique de WAF empêche l'exécution de scripts, de commandes shell et de commandes PHP non autorisées.
En attendant, les 1,6 millions de clients impactés de Clash of King sont invités à changer leur mot de passe… surtout si ce dernier est aussi utilisé sur d'autres espaces web !

0Day vBulletin dans la nature ?
A noter que la société Trillian a alerté ses utilisateurs de l'utilisation d'un 0day vBulletin qui a touché l'un de ses services. La société ne sait pas vraiement quand a eu lieu l'attaque [on parle de décembre 2015, NDR] mais a fermé le site et le serveur contenant les forums impactés par la fuite de données. Dans les informations prises en main par le pirate : les données du blog de la société [sous WordPress] et « une poignée d'autres bases de données marketing qui contenait les noms d'utilisateurs Trillian et leurs adresses mail ». Les mots de passe étaient, eux aussi, en Md5. Le plus inquiétant à mon sens est que Trillian indique que les données « volées » étaient âgées de 3 à … 14 ans !
Article original de

Original de l'article mis en page : ZATAZ Piratage de 1,6 million de comptes Clash of King – ZATAZ

Les cyberattaques sont de plus en plus furtives

Les cyberattaques sont de plus en plus furtives

Comment détecter les cyberattaques les plus furtives ? Une priorité au quotidien pour toutes les entreprises. Tomer Weingarten, CEO SentinelOne, nous livre son expertise sur le sujet.

Alors que les cybercriminels – individus, groupements ou Etatiques – utilisent une combinaison de techniques complexes pour échapper à la détection, les cyberattaques deviennent plus intelligentes et furtives. Les techniques traditionnelles de protection reposant sur des signatures statiques – tels que les anti-virus (AV) – ou l'ignorance des vecteurs d'attaques comme les fichiers compromis, ne sont plus adaptés pour faire face au paysage de menaces d'aujourd'hui. Alors comment les entreprises peuvent tenter de se protéger contre les variantes de logiciels malveillants ou des nouveaux exploits, en constante évolution ?

Le poste de travail – incluant une série d'équipements : ordinateurs portables, tablettes, smartphones, serveurs ou même imprimantes – demeure l'une des cibles de choix dans toute attaque. Le poste de travail agit comme une passerelle pour les hackers dans leur intrusion au sein du réseau et une fois qu'un logiciel malveillant a été exécuté sur un poste de travail, les attaquants peuvent se déplacer librement. Ainsi, la détection et la protection doivent se produire sur les terminaux eux-mêmes. Ceci est d'autant plus important à l'ère du BYOD, car les utilisateurs peuvent facilement connecter leurs propres appareils au réseau de l'entreprise. Or, si les utilisateurs se connectent à un dispositif non autorisé ou infecté, le malware peut se déplacer librement au sein du réseau.

Evolution de la menace

Les techniques utilisées par les cybercriminels sont toujours en évolution pour garder une longueur d'avance sur les systèmes de protection et, comme la sophistication des logiciels malveillants se développe également, cela représente de nouveaux challenges pour les entreprises. Dans sa définition, un malware n'a pas changé. **Ce qui est en train de changer, ce sont les techniques d'évasion utilisées par de nouvelles formes de logiciels malveillants dans le but de voler des données précieuses présentent sur les postes de travail.**

Les "binders" sont un excellent exemple : ce sont de petits outils logiciels qui fusionnent deux fichiers .exe différents dans un seul fichier. L'exécution d'un .exe démarre simultanément le second de manière invisible. Ces outils piègent leurs victimes avec l'ouverture d'un fichier connu et qui semble légitime à l'extérieur ; mais qui est en fait malveillant à l'intérieur.

Aujourd'hui, les logiciels malveillants peuvent être conçus pour être « sensibles au contexte » et ont la capacité de détecter s'ils évoluent dans un environnement sandbox physique ou virtualisé. Une fois que ce type de malware détecte un environnement anormal, il échappe activement à la détection en agissant de façon bénigne ou en "dormant" pendant une période de temps définie. À partir de là, le malware tente d'interpréter les mouvements et de déchiffrer, si les actions proviennent d'un être humain ou d'un scanner de code automatisé. Cela permet au malware de contourner facilement les défenses traditionnelles telles que les sandboxes réseau, jusqu'à son exécution.

Reprendre le contrôle

Les attaques étant devenues plus sophistiquées, la protection des postes de travail annonce probablement la fin des anti-virus. Ces derniers reposant effectivement sur une analyse statique qui repère l'empreinte d'un fichier, les attaquants peuvent rapidement adapter des fichiers pour créer quelque chose de complètement nouveau et inconnu ; et ces nouvelles variantes peuvent facilement contourner la solution AV. Il a ainsi été estimé que les anti-virus ne peuvent repérer qu'environ 45 % des cyberattaques – ce qui en fait une solution obsolète face aux défis de la cybersécurité d'aujourd'hui.

Dans ce contexte, **une nouvelle génération de solutions de sécurité du poste de travail est en train d'émerger, telles que les techniques d'analyse comportementale,** afin que les entreprises puissent profiter des avantages des approches innovantes. Cette nouvelle ère de la protection se concentre, en temps réel, sur une approche proactive de la sécurité du poste de travail, réalisée par l'apprentissage automatique (machine learning) et l'automatisation intelligente afin de détecter et de protéger efficacement tous les terminaux contre les attaques les plus perfectionnées. Cette nouvelle génération de protection des postes de travail part du principe qu'elle ne connait rien sur les logiciels malveillants, mais qu'elle observe leur comportement dans le but de repérer les activités considérées comme des anomalies, et mettre en place les étapes de défense pour les dévier complètement.

De plus, **cette nouvelle génération de solutions a des capacités de remédiation pour inverser toutes les modifications apportées par les logiciels malveillants.** Cela signifie que lorsque les fichiers sont modifiés ou supprimés, ou lorsque des modifications sont apportées aux paramètres de configuration ou aux fichiers systèmes, le logiciel a la capacité de restaurer un poste de travail, comme il était, avant l'exécution du malware.

Dans la lutte contre la nouvelle génération de cyberattaques, cette approche plus dynamique et robuste des postes de travail permet aux entreprises de prendre l'avantage face aux cybercriminels.

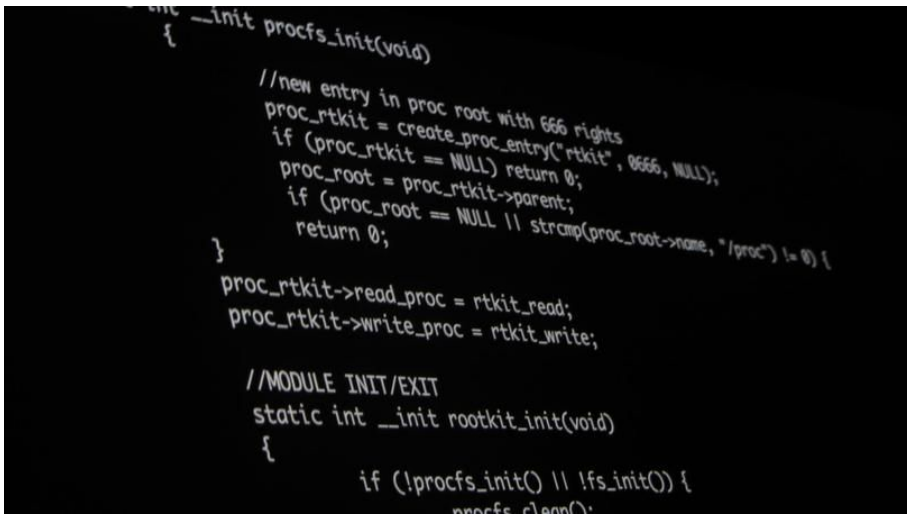
Article original de iTPro.fr

Réagissez à cet article

Original de l’article mis en page : Détecter les cyberattaques les plus furtives | iTPro.fr

---

Les américains s’inquiètent de la cyber-sécurité automobile



Les américains s’inquiètent de la cyber-sécurité automobile

Après l'attentat de Nice, les questions de cyber-sécurité sont devenues une urgence pour les américains, qui imaginent le scénario catastrophe d'un pirate informatique prenant le contrôle d'un véhicule.

L'attentat terroriste de Nice a ravivé dans le secteur automobile américain les craintes d'un scénario catastrophe où un pirate informatique prend à distance le contrôle d'une voiture pour l'utiliser comme projectile. Cette éventualité, digne d'un scénario hollywoodien, est alimentée par la circulation croissante de voitures semi-autonomes et connectées, équipées de systèmes multimédias embarqués censés les rendre plus sûres et fiables.

Paradoxalement, ces mêmes technologies de pointe en font des cibles privilégiées pour les hackers, selon les sociétés de sécurité informatique américaines Mission Secure Inc (MSi) et Perrone Robotics Inc. Car, selon celles-ci, les pirates informatiques pénètrent via les connexions sans fil, bluetooth et wifi, nécessaires à leur fonctionnement. «La technologie crée beaucoup d'opportunités nouvelles et excitantes pour les consommateurs mais (génère) aussi des défis», opine Mary Barra, la PDG de General Motors (GM). «L'un de ces défis est la problématique sur la cyber-sécurité», a-t-elle insisté vendredi devant un parterre composé de ses pairs, d'officiels et d'experts de l'automobile réunis à Detroit pour évoquer les cyber-attaques.

Le 14 juillet, Mohamed Lahouaiej-Bouhlel, un Tunisien, a foncé au volant d'un camion dans la foule à Nice tuant 84 personnes et blessant plus de 330 personnes.

«Nous connaissons ces terroristes (…) il ne faut pas beaucoup d'imagination pour penser qu'ils vont se servir d'une voiture autonome et la faire foncer dans une foule.»
John Carlin, un ministre-adjoint américain de la Justice.

«Nous connaissons ces terroristes. Ils n'en ont peut-être pas encore les capacités mais s'ils parviennent à convaincre les gens de foncer dans une foule avec un camion, il ne faut pas beaucoup d'imagination pour penser qu'ils vont se servir d'une voiture autonome et la faire foncer dans une foule», redoute John Carlin, un ministre-adjoint américain de la Justice. «Les méchants emploient de plus en plus de moyens sophistiqués», souscrit David Johnson, un des responsables du FBI chargé des cybercrimes et des menaces sur internet.

A l'été 2015, deux chercheurs américains en informatique ont démontré qu'il était facile de prendre le contrôle d'une voiture «connectée». Charlie Miller et Chris Valase étaient parvenus à pirater à distance la Jeep Cherokee d'un journaliste du site spécialisé Wired. Ils avaient ainsi pu allumer la radio, fait fonctionner les essuie-glaces et, surtout, couper le moteur. Ils étaient aussi parvenus à désactiver les freins. Les «menaces évoluent», avance Titus Melnyk chargé de la sécurité chez Fiat Chrysler Automobiles (FCA), qui vient de lancer un programme visant à encourager les hackers à informer le groupe des failles liées à la cyber-sécurité de ses voitures. Le constructeur des Jeep promet une prime pouvant aller jusqu'à 1.500 dollars par alerte. «On ne sait jamais. Cela peut être la base d'une attaque», défend M. Melnyk insistant sur le fait que ce programme est «très sérieux».

En 2015, le constructeur de véhicules électriques de luxe Tesla – dont les deux modèles commercialisés (Model S et Model X) sont équipés d'un système d'aide à la conduite leur permettant d'effectuer seuls certaines manoeuvres comme le freinage en urgence – avait été l'un des premiers à lancer un tel plan. Tesla, qui a construit sa réputation sur l'innovation, n'avait pas le choix: deux chercheurs avaient révélé qu'ils pouvaient couper à distance le moteur d'une berline Model S en piratant le système multimédia. GM, qui dit recevoir et résoudre plusieurs alertes liées à de possibles cyber-attaques par jour, gère un programme sur les vulnérabilités de ses voitures sur le site hackerone.com.

Les nouvelles technologies embarquées exposent également les conducteurs à un vol potentiel de leurs données personnelles quand ils connectent leur téléphone intelligent.

Article original de lefigaro.fr

Réagissez à cet article

Original de l’article mis en page : Les américains s’inquiètent de la cyber-sécurité automobile

---

Orange corrige un sérieux problème de sécurité dans l’une de ses boutiques en ligne

Orange corrige un sérieux problème de sécurité dans l’une de ses boutiques en ligne

---

Alterte ! Plusieurs problèmes découverts dans le site orangeboutique.fr. L'un d'eux aurait pu permettre d'injecter un document piégé directement dans une boutique Orange.
Imaginez, vous visitiez le site orangeboutique.fr [espace fermé depuis le 19/07/16] et téléchargiez ce que vous pensiez être un document officiel de l'opérateur téléphonique Français. Un PDF vous proposant les dernières réductions et promotions. Sauf que dans ce fichier Adobe, un code malveillant orchestrant le téléchargement d'un logiciel espion dans votre ordinateur.
De la science-fiction ? Malheureusement, non ! Le protocole d'alerte de ZATAZ a permis la correction de plusieurs problèmes dans le site orangeboutique.fr. Parmi les « bugs » que je peux vous révéler aujourd'hui, la possibilité d'injecter dans l'espace 2.0 n'importe quel fichier à partir d'une page dédiée non verrouillée.
L'équipe sécurité d'Orange a très rapidement pris en main et corrigé le problème dès la réception du Protocole d'Alerte. D'autres failles et fuites concernées ce même site, avec par exemple l'accès à des documents internes. Des fichiers non sensibles [pas de données clients], sauf dans les mains de la concurrence pouvant ainsi découvrir les actions commerciales à venir dans les agences physiques Orange (Tarifs, produits, cibles clientèles…). Des accès sans aucune restriction, ni mot de passe. Le site a été fermé le 19 juillet 2016.
Article original de Damien Bancal

Réagissez à cet article

Original de l'article mis en page : ZATAZ Orange corrige un sérieux problème dans l'une de ses boutiques en ligne – ZATAZ

L’Internet des objets, ce piège de cristal

	L’Internet des objets, ce piège de cristal

Encore une fois, l'actualité technologique nous démontre que l'Internet des objets est un problème de sécurité de masse en devenir.

Vous le savez sans doute si vous suivez mes articles, je suis un tantinet sceptique quant à la montée de l'Internet des objets, soit le mariage entre l'Internet et les objets du quotidien. Non pas que je doute des possibilités offertes par les systèmes qui émergeront de cette tendance, bien au contraire. Ce sont plutôt les problèmes de sécurité qu'ils engendreront qui me laissent quelque peu pantois.

Imaginez les grands titres : «Incapables de regarder le Canadien de Montréal à cause d'un maliciel». Je vous jure, là, les gens vont débarquer dans les rues.

Lorsqu'on prend du recul et qu'on regarde ce qui se passe, nous sommes littéralement en train de nous créer notre propre piège de cristal : c'est bien beau et reluisant à l'extérieur, mais un gros problème se cache à l'intérieur. Nous sommes en train de devenir dépendants de systèmes extrêmement poreux. Or, je ne serais pas surpris de voir que bon nombre d'objets connectés que l'on considère comme des «acquis» finissent par tomber en otage aux mains d'un Hans Gruber en puissance qui décide tout simplement de nous faire cracher le cash pour retrouver le contrôle desdits objets.
Ça semble peut-être bien théorique en ce moment, mais la journée où des voitures, des frigos, des systèmes de chauffages, ou des téléviseurs cesseront de fonctionner pour la simple et bonne raison qu'ils seront tombés entre les griffes d'un quelconque cryptorançongiciel remâché, ça risque de déranger pas mal de monde, et pire, en inquiéter encore plus. Imaginez les grands titres dans les tabloïds : «Incapables de regarder le Canadien de Montréal à cause d'un maliciel». Je vous jure, là, les gens vont débarquer dans les rues.

Die Harder

*Le pire dans tout ça, c'est qu'on est véritablement devant une chronique de mort annoncée. Déjà, on a constaté que certains objets connectés pouvaient être massivement piratés par toutes sortes de moyens. Il y a quelques mois de cela, on découvrait par exemple que des ampoules et des serrures connectées **pouvaient être ciblées et exploitées par des pirates informatiques malintentionnés**. On imagine déjà le potentiel de ce genre de vulnérabilités pour la sécurité résidentielle. Pourtant, on en est qu'aux débuts en ce qui concerne les problèmes dans les systèmes de sécurité.*

*(Photo : **Frédéric Bisson**)*

*Tout récemment, on a d'ailleurs vécu le comble de l'ironie dans les systèmes de sécurité alors que pas moins de 25 000 caméras de surveillance ont fait partie **d'un réseau de botnets lançant des attaques par déni de services**. Grosso modo, des pirates informatiques ont été en mesure de pirater des caméras de surveillance mal sécurisées, de les fédérer dans un réseau sous un serveur de commandement et de contrôle et de les réutiliser pour commettre des attaques informatiques ultérieures. C'est-y pas beau ça!?*

*Pourtant, on avait déjà eu des signes avant-coureurs de ce genre d'attaques. Des réseaux de botnetsconstruits avec des caméras de surveillance avaient déjà **été découverts dans des analyses précédentes**. Des analyses qui démontraient par ailleurs que ces objets connectés étaient passablement poreux.*
*Et on est loin d'être sortis du bois, je vous en passe un papier. Non seulement il existe **des moteurs de recherche permettant de trouver les objets connectés** présents sur Internet, mais en plus, on a des petits génies informatiques qui se mettent à les **géolocaliser en utilisant des drones**. Donc, si vous aviez espoir que ça ralentirait quelque peu, détrompez-vous.*

*Pourtant, je ne suis pas le seul qui a des problèmes de sommeil par rapport à cette situation. En 2014, Europol prédisait **qu'un meurtre mené par Internet allait probablement se produire dans les prochains mois**. Bon, moi je n'irais pas jusqu'à faire une prédiction temporelle, mais c'est clair que, tôt ou tard, un truc du genre va finir par arriver. Je ne suis pas certain que ce sera un événement intentionnel, mais considérant la vitesse à laquelle on intègre des objets connectés dans le réseau de la santé, ce n'est qu'une question de temps avant que quelqu'un meurt suite à un incident informatique.*

Marche ou crève

Bon, j'ai beau couiner et geindre, c'est bien dommage, mais on ne changera pas pour autant les avancées technologiques. Le néo-luddisme ne sert strictement à rien dans ce cas; il faudra à terme que l'industrie atteigne un niveau de maturité suffisant pour construire les objets connectés avec une architecture centrée sur la sécurité. En attendant, on est dû pour quelques coups fumants de piratage et de prises d'otages numériques.
En fait, la vraie question que l'on doit se poser est celle du «retour sur investissement». Dans le cas du secteur de la santé par exemple. Oui, c'est clair que des gens finiront par mourir dus à des problèmes liés à l'informatique. Cependant, il faut aussi considérer l'autre côté de la médaille, c'est-à-dire combien de personnes ont été sauvées par ces mêmes systèmes informatiques.
Il en va de même avec les gestes que posent John McClane dans la série Die Hard. Oui, il finit par causer beaucoup de dommages et par tuer beaucoup de monde au cours de ses aventures, mais il sauve également la vie de centaines de victimes innocentes.

Yippee Ki-Yay Mother$&@%!*
Article original de Benoît Gagnon

Réagissez à cet article

Original de l’article mis en page : L’Internet des objets, ce piège de cristal | Branchez-vous

---

Attention, faille découverte dans les réseaux mobiles GSM et 4G LTE !

Attention, faille découverte dans les réseaux mobiles GSM et 4G LTE !

Un audit de sécurité a trouvé une faille critique dans un compilateur de code utilisé par plusieurs logiciels propres aux réseaux mobiles GSM et 4G LTE

Plusieurs logiciels pour la gestion et l'interconnexion des réseaux mobiles du monde entier GSM et LTE (4G) sont vulnérables à une faille permettant une exécution de code à distance où un attaquant peut donc prendre le contrôle d'un équipement réseau. Le CERT-US a déjà lancé un avertissement sur cette vulnérabilité.

Classée sous le nom CVE-2016-5080, cette faille a été découverte lors d'un audit de sécurité d'Objective Systems, un éditeur américain qui commercialise asn1C, un compilateur de code servant à créer les applications de gestion et d'interconnexion des réseaux mobiles. Asn.1 (Abstract Syntax Notation One) est une norme internationale qui décrit les structures de données et les protocoles de transfert utilisés dans le domaine des télécommunications. Asn1c est une application qui récupère les instructions, les opérations et les structures des données pour le convertir en C, C++, C# ou en Java. Cette transformation peut ensuite être intégrée dans des applications fonctionnant sur des réseaux mobiles GSM ou LTE.

Peu d'acteurs concernés par la faille ?

Objective Systems précise que la vulnérabilité se trouve dans la compilation du code ASN.1 vers C et C++. La faille consiste en un débordement de la mémoire tampon ouvrant la porte aux attaquants pour exécuter du code sur les systèmes compromis, à distance et sans avoir besoin d'authentification sur le périphérique. L'éditeur a corrigé son logiciel et continue à vérifier la compilation vers C# et Java.

La question est de savoir qui est touché par cette faille. Le Cert américain a lancé son avertissement auprès de 34 opérateurs mobiles et équipementiers. Peu ont répondu à cet appel, Qualcomm a indiqué dans qu'il intégrait ce code dans ses produits cellulaires, mais que la faille n'est pas exploitable. Malgré cet optimisme, la société américaine a diffusé le patch d'Objective Systems sur ses solutions. D'autres entreprises comme HPE ou Honeywell ont précisé qu'elles n'étaient pas concernées.

Objective Systems revendique une base client comprenant plusieurs grands noms des réseaux mobiles comme Alcatel-Lucent, AT&T, BT, Cisco, Deutsche Telekom, etc. Le problème est qu'à la différence d'un terminal mobile, il est plus difficile de patcher les équipements télécoms.

Article original de Jacques Cheminat

Réagissez à cet article

Original de l’article mis en page : Une faille découverte dans les réseaux mobiles GSM et 4G LTE