150 Go de données médicales volées seraient dans la nature !

150 Go de données médicales volées seraient dans la nature !

Un pirate (ou un groupe) aurait mis en ligne 150 Go de données médicales d'un réseau de cliniques d'urologie américain, contenant des données précises sur le suivi de patients. Une tendance de plus en plus répandue outre-Atlantique.

Les données médicales semblent prisées des pirates. Un (groupe de) pirate(s), nommé Pravvy Sector, aurait ainsi mis en ligne 150 Go de données médicales d'un réseau de cliniques d'urologie de l'Ohio, rapportait hier Motherboard. Le contenu trouvé concernerait à la fois les cliniques elles-mêmes (avec des données sur ses ressources humaines) et les patients, avec des indications précises sur leur suivi médical, leur traitement ou encore leurs informations d'assurance.

Motherboard a contacté trois patients présents dans le fichier identifié, dont deux ont pu confirmer que les informations publiées étaient exactes pour eux. L'origine des données, qui semblent bien venir du réseau de cliniques lui-même, n'a pas pu être confirmée. Contactée par le site américain, l'organisation n'a pas encore répondu à ses demandes de commentaires.

Bien avant cette publication, Pravvy Sector aurait été en quête de reconnaissance, contactant directement certains médias avec les contenus de « fuites » précédentes. Mais le plus important est la tendance que deviennent les incidents liés aux données médicales. Comme le relève The Verge, 49 intrusions affectant plus de 500 personnes ont été signalées dans le secteur médical, depuis le début de l'année.

En juin, une autre fuite présumée concernait 655 000 enregistements médicaux, via plusieurs organismes. Si l'ensemble des données n'a pas pu être authentifié, un échantillon l'avait été à l'époque par Motherboard. Contrairement à la publication de Pravvy Sector, les informations étaient cette fois vendues sur un site spécialisé.

Article original de Guénaël Pépin

Réagissez à cet article

Original de l'article mis en page : États-Unis : 150 Go de données médicales seraient dans la nature

Attention à l’application « Rio Olympics 2016 «

	Attention à l’application « Rio Olympics 2016 «

Avec l'approche des jeux Olympiques de Rio, le téléchargement d'applications thématiques va battre son plein. Gare aux applications dangereuses !
Rio Olympics 2016 Keyboard, un clavier publicitaire dangereux !

La société Lookout Mobile Security vient d'alerter ZATAZ de certains problèmes de confidentialité et des enjeux rencontrés par les utilisateurs et les entreprises avec l'application Rio Olympics 2016 Keyboard. Une APP disponible en version iOS et Android.
L'application officielle de l'entreprise américaine NBC Universal Media, Rio 2016 Olympics keyboard est en apparence une simple extension de clavier pour les personnes qui suivent les jeux Olympics. Cependant, il a identifié que cette application était capable de compiler plus d'information qu'initialement prévu par son développeur, exposant ainsi la confidentialité des données des amateurs des JO de RIO et possiblement des entreprises pour lesquelles ils travaillent.
Finalement, l'équipe de recherche a informé NBCUniversal des enjeux de confidentialité identifiés dans les versions Android et iOS de l'application officielle Rio 2016 Keyboard. NBCUniversal a réagi rapidement pour résoudre les problèmes identifiés et s'assurer que les versions disponibles seraient sécurisées avant l'ouverture des Jeux Olympiques d'été de Rio. Si vous avez téléchargé l'application, effacez là. A vous de décider, ensuite, si vous installez la nouvelle version.

Réagissez à cet article

Original de l'article mis en page : ZATAZ L'appli Rio Olympics 2016 Keyboard dangereuse – ZATAZ

Hack de la Jeep Cherokee, le retour, malgré les mises à jour…

Hack de la Jeep Cherokee, le retour, malgré les mises à jour…

Les deux experts qui avaient piraté une Jeep Cherokee récidivent dans le cadre de la Black Hat en démontrant une attaque sur le même véhicule.

En 2015, la Black Hat avait vu deux spécialistes en sécurité, Charlie Miller et Chris Valasek, prendre le contrôle à distance d'une Jeep Cherokee de 2014. Un exploit qui a obligé Chrysler, propriétaire de Jeep, à procéder à un rappel de près de 1,4 million de véhicules. Une opération de mise à jour coûteuse pour le constructeur automobile. Il en a profité aussi pour lancer un Bug Bounty, avec des primes allant de 150 à 1500 dollars.

Un programme auquel les deux experts ne pourront pas concourir. Car ils démontrent à la Black Hat 2016 que la sécurité des voitures connectées n'est toujours pas optimale, malgré les récentes mises à jour. Dans une présentation, ils présentent une attaque contre la même Jeep Cherokee de 2014. A la différence de l'année dernière, cette attaque n'est pas menée à distance, mais avec un accès physique à la voiture. Néanmoins, le duo précise qu'avec du temps elle pourrait être réalisée via un terminal embarqué ou à distance via une liaison sans fil.

Blocage des freins et coup de volant intempestif

Une fois dans la voiture, Charlie Miller a branché son ordinateur sur le réseau du véhicule, nommé bus CAN, via un port situé sous le tableau de bord. Ce réseau envoie des instructions aux différents capteurs (consommation, confort, détection de panne, etc). L'accès à ce réseau est normalement sécurisé avec le patch de sécurité élaboré l'année dernière à la suite du premier piratage de la Jeep. Il semble que des failles subsistent et les deux spécialistes ont pu contourner certains garde-fous.

Parmi les actions réalisées, ils ont bloqué les freins. Charlie Miller s'est servi du mode maintenance pour rendre inopérant le freinage. D'habitude ce blocage des freins ne peut s'opérer qu'à une faible vitesse soit 5 miles par heure. Dans une vidéo, le duo roule sur une route de campagne et d'un coup (après un compte à rebours) le volant se met à tourner à 90 degrés plantant la Jeep dans le fossé. Pour se faire, Charlie Miller s'est servi de la fonction tourner le volant dans la fonction parking automatique (qui se fait habituellement en marche arrière et à faible vitesse). Concrètement pour réaliser leur piratage, les deux experts se sont attaqués à la fois aux bus CAN, mais surtout en ciblant directement les ECU (electronic control units) dont un a été placé en mode maintenance et un autre utilisé pour envoyer des commandes malveillantes.

Interrogé par nos confrères de Wired, Chrysler ne considère pas cette attaque comme un danger pour la sécurité des véhicules. En premier lieu, elle nécessite un accès physique à la voiture. De plus, les experts ont utilisé une Jeep Cherokee ne disposant pas de la dernière version du logiciel embarqué d'infotainment (vecteur de leur première attaque en 2015). Les experts précisent que même avec la dernière version, cette attaque est toujours possible.

Article original de Jacques Cheminat

Réagissez à cet article

Original de l'article mis en page : Direction, frein : les hackers de Jeep récidivent à la Black Hat

Le bitcoin victime d’une faille dans le système ?

Le bitcoin victime d’une faille dans le système ?

Bitfinex, plus grande place d'échange de bitcoins en dollars, suspend son activité après le vol de près de 120 000 bitcoins dans son système. La cryptomonnaie a perdu 5,5 % de sa valeur dans la journée.

La plateforme de change hongkongaise Bitfinex a annoncé mardi dans un communiqué avoir « *découvert une faille de sécurité qui l'oblige à geler toute transaction* […] *ainsi que tout dépôt et retrait de fonds* ». « *Je peux confirmer que la perte à la suite du hack est de 119 756 BTC* », a déclaré Zane Tackett, CTO du groupe, sur Reddit. Au cours actuel de 540 dollars pour un bitcoin, la valeur des bitcoins qui se sont volatilisés s'élève à environ 65 millions de dollars.

En noir, la valeur d'échange du bitcoin au dollar (échelle de droite). En vert et en rouge, les volumes des transactions (échelle de gauche en milliers de bitcoins).

Le cours du bitcoin a perdu 5,5 % contre le dollar dans la journée de mardi, soit une chute de 13 % en deux jours. La valeur de la cryptomonnaie avait cela dit perdu 6,2 % lundi, sans que le lien avec le hack soit avéré. C'est au total l'équivalent de 1,5 milliard de dollars qui s'est évaporé de la capitalisation marchande du bitcoin cette semaine.

Avant l'incident, Bitfinex était la plus grosse plateforme de change avec le dollar, totalisant 8,5 % de tous les échanges de bitcoins. Elle était néanmoins derrière le chinois OKCoin, dont 90 % du trading s'effectue en yuans.

LES ATTAQUANTS DOIVENT COMPROMETTRE LES DEUX ORGANISATIONS AVANT D'OBTENIR LES FONDS

La plateforme hongkongaise assure sa sécurité avec BitGo, une firme basée à Palo Alto (Californie), via un système de multi-signature. Lors du partenariat, Bitfinex avait déclaré que grâce à un tel procédé, « les attaquants doivent compromettre les deux organisations avant d'obtenir les fonds ». Aujourd'hui, BitGo affirme ***ne pas avoir découvert de brèches*** *de son côté.*

En février 2014 s'était déjà produit ***un événement similaire*** *d'une ampleur bien plus grave. La plateforme tokyoïte Mt.Gox, où s'échangeaient à l'époque 70 % des bitcoins du monde, avait également affirmé avoir été victime de pirates : 744 408 bitcoins, soit 450 millions de dollars selon la valeur du cours au moment de l'incident, avaient été dérobés au système.*

Depuis, MtGox a mis la clé sous la porte après de forts soupçons sur son honnêteté, et qui perdurent encore aujourd'hui. En l'espace d'un mois, la cryptomonnaie avait plongé 30 % mais, habituée à une volatilité extrême, elle s'en était vite remise.

Article original de Victoria Castro

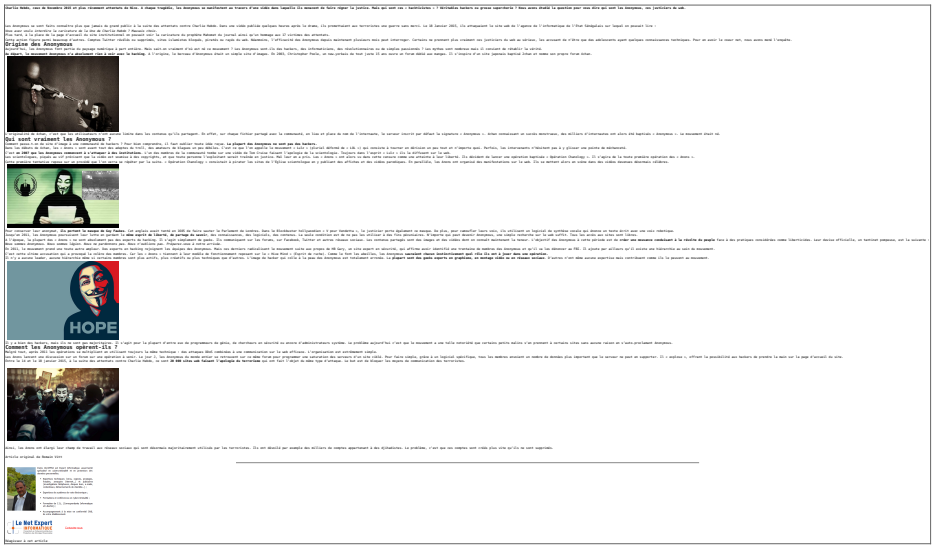
Réagissez à cet article

Original de l’article mis en page : Le bitcoin dévisse après un piratage à 65 millions de dollars – Business – Numerama

---

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 ?

#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.

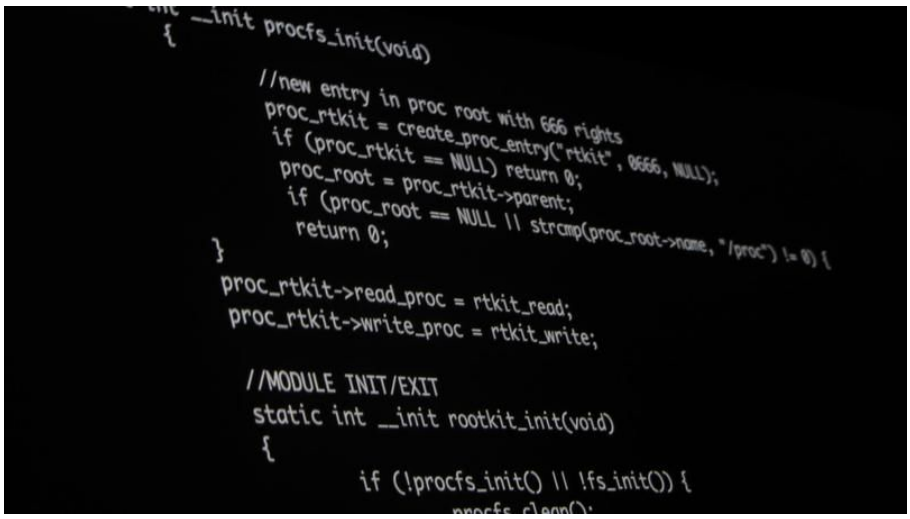
Article original de iTPro.fr

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