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

Si le E-commerce était retranscrit dans la réalité

Si le E-commerce était retranscrit dans la réalité

Une Vidéo qui retranscrit ce que nous vivons sur la toile dans le processus de vente des sites en ligne.

Je pense qu'énormément de personnes vont se reconnaitre dans cette vidéo si vous achetez régulièrement sur la toile. Vous le savez quand vous souhaitez acheter un produit, le « tunnel d'achat » est souvent long et fastidieux. Entre la première visite et la réception de l'email de confirmation de commande, il se peux que vous passiez un certain nombre de minutes. Surement trop long j'en suis sûr. Trop d'informations à donner, création de compte, j'en passe et des meilleurs. Je suis sur que vous avez déjà été confronté aux « Kapcha » indécodable ou encore à l'expiration de la session…

Voila ce que résume cette vidéo. Une caricature de ce qu'il nous arrive en ligne. J'ai trouvé cela très drôle et très bien monté.

Je pense que pour ceux qui réalise des sites web, c'est souvent la problématique principale. Comment ne pas perdre de clients potentiels dans un processus de vente fastidieux et trop complexe.

Article original de David Gaborit

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 : Si le E-commerce était retranscrit dans la réalité. – Olybop

---

Les conséquences inatendues des changements trop fréquents de mots de passe

Les conséquences inatendues des changements trop fréquents de mots de passe

---

Il est préférable d'opter pour des mots de passe robustes, plutôt que d'imposer des changements fréquents, réaffirme la responsable des technologies de la FTC.

Fraîchement nommée chef des technologies de la Federal Trade Commission (FTC), Lorrie Cranor (également professeur à l'université Carnegie Mellon), avait été surprise par un tweet officiel mis en ligne en janvier. Le régulateur américain du commerce préconisait alors un changement fréquent de mots de passe. La spécialiste s'y est opposée. Depuis, elle fait évoluer la politique interne sur le sujet.

« Je suis allée voir les personnes en charge des médias sociaux et leur ai demandé pourquoi [la FTC dit à tout le monde de changer de mots de passe] », a commenté Cranor lors de la conférence *Passwords* de BSidesLV 2016, dont *Ars Technica* s'est fait l'écho. *« Elles m'ont répondu ceci : 'C'est probablement un bon conseil, car à la FTC nous changeons nos mots de passe tous les 60 jours' »*.

Lorrie Cranor s'est alors entretenue avec le #DSI et le RSSI de la FTC. Elle a souligné, rapport d'experts à l'appui, que les changements fréquents n'améliorent pas la sécurité, mais encouragent au contraire l'utilisation de mots de passe plus susceptibles d'être découverts et détournés.

Un modèle, des mots de passe

Lorsque des utilisateurs doivent changer de mots de passe tous les 90 jours, par exemple, ils ont tendance à utiliser un même modèle. C'est ce qui ressort d'une étude publiée en 2010 par des chercheurs de l'université de Caroline du Nord (UNC) à Chapel Hill.

« Les utilisateurs prennent leurs anciens mots de passe, puis ils les changent légèrement [d'une lettre, d'un chiffre ou d'un symbole] pour obtenir un nouveau mot de passe », a expliqué Cranor. Or la capacité de ces mots de passe à résister aux attaques par force brute est faible. 17 % des mots de passe testés par les chercheurs de l'UNC auraient ainsi été découverts en moins de cinq tentatives.

Il est donc préférable, selon eux, d'utiliser des mots de passe forts, plutôt que d'en changer souvent. La double authentification est également recommandée, notamment pour les applications sensibles.

Article original de Ariane Beky

Réagissez à cet article

Original de l'article mis en page : Les changements fréquents

de mots de passe nuisent à la sécurité

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

---

Attention, Cheval de troie dans une Application sur Google Play découverte par Eset

Avant même la sortie sous Android de Prisma, une application populaire de retouche photos, Google Play Store s'était retrouvé inondé de fausses applications.

Les chercheurs d'ESET ont découvert de fausses applications imitant Prisma, dont plusieurs Chevaux de Troie dangereux. Dès l'avertissement d'ESET, le service sécurité de Google Play a retiré toutes les fausses applications du store officiel d'Android. Ces dernières auront tout de même atteint plus d'1,5 millions de téléchargements.
Prisma est un éditeur de photos unique publié par les laboratoires de Prisma. D'abord développé pour iOS, cette application a remporté d'excellents résultats de la part des utilisateurs d'iTunes et de l'App Store d'Apple. Les utilisateurs d'Android étaient à leurs tours impatients de la découvrir sur le Google Play (disponible depuis le 24 juillet 2016).
« La plupart des fausses applications de Prisma disponibles sur Google Play ne disposent pas d'une fonction retouche photo. A l'inverse, elles affichent uniquement des annonces, avertissements ou de faux sondages pour tromper l'utilisateur qui fournit des informations personnelles le concernant ; ou encore pour le faire souscrire à de faux services type SMS onéreux », commente Lukáš Štefanko, Malware Researcher chez ESET.
La plus dangereuse des fausses applications imitant Prisma et trouvée dans le Google Play est un Cheval de Troie téléchargeur détecté par ESET comme Android/TrojanDownloader.Agent.GY. Des informations sur les périphériques sont envoyées au serveur C&C, ce qui lui permet de télécharger sur demande des modules supplémentaires et de les exécuter afin de voler des données sensibles telles que le numéro de téléphone, l'opérateur, le pays, la langue etc.
A cause de ses capacités de téléchargement, la famille des malwares type Android/TrojanDownloader.-Agent.GY pose de sérieux risques pour les plus de 10.000 utilisateurs Android qui ont installé cette application dangereuse avant d'être retiré du Google Play Store.

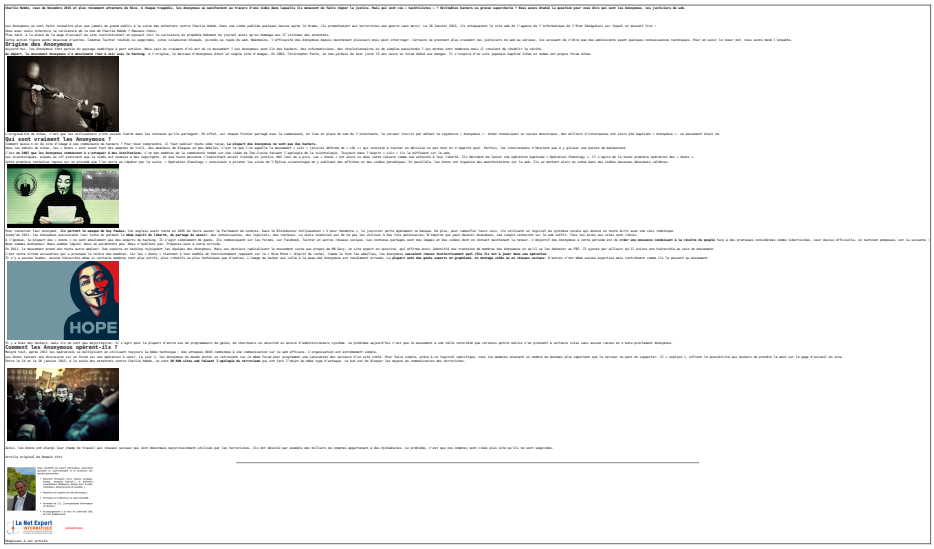
Pour se protéger, Denis JACOPINI recommande l'application suivante :

Article original de Eset

Réagissez à cet article

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 du 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

Réagissez à cet article

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