Campagne de fraude ciblant les utilisateurs American Express – Data Security BreachData Security Breach

	Campagne de fraude ciblant les utilisateurs American Express

On n’apprend jamais des erreurs des autres, en tout cas, c’est qu’il faut croire après le nombre élevé d’utilisateurs American Express victimes de la plus récente attaque de phishing.

Les attaques de phishing ciblées deviennent de plus en plus difficiles à détecter. Voilà pourquoi il est important de toujours redoubler de vigilance dans la vérification d’adresses des expéditeurs, même si elles peuvent sembler venir de sources sûres. Dans l’escroquerie American Express, les pirates ont envoyé des e-mails en se faisant passer pour la société, et en reproduisant un modèle fidèle de mail de l’entreprise, ils sont allés jusqu’à créer un faux processus de configuration, pour installer une « clé personnel de protection personnel American Express.
Les e-mails frauduleux exhortent les clients à créer un compte pour protéger leur ordinateur contre les attaques de phishing -quelle ironie !-. Lorsque les utilisateurs cliquent sur le lien dans le mail, la page vers laquelle ils sont redirigées, leur demande des informations privées telles que le numéro de sécurité sociale, date de naissance, nom de jeune fille de la mère, date de naissance, e-mail et tous les détails de leurs cartes American Express, y compris les codes et la date d’expiration.
L’augmentation massive des attaques de ce type devrait sensibiliser les utilisateurs à ne jamais répondre à des e-mails suspects, mais il est toujours difficile de distinguer le vrai du faux, surtout si l’utilisateur n’est pas doué en informatique ou s’il ne maitrise pas bien l’Internet…[lire la suite]

Notre métier : Sensibiliser les décideurs et les utilisateurs aux risques liés à la **Cybercriminalité** et à la **Protection des Données Personnelles** (Autorisation de la Direction du travail de l’Emploi et de la Formation Professionnelle n°93 84 03041 84).
Denis JACOPINI anime dans toute le France et à l’étranger des conférences, des tables rondes et des formations pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles (Mise en Place d’un Correspondant Informatique et Libertés (CIL) dans votre établissement.
Plus d’informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Réagissez à cet article

Original de l’article mis en page : Campagne de fraude ciblant les utilisateurs American Express – Data Security BreachData Security Breach

Signes indiquant qu’un compte a été piraté et procédure à suivre

	Signes indiquant qu’un compte Yahoo a été piraté et procédure à suivre

Nous espérons que vous n'aurez jamais à craindre qu'une autre personne accède à votre compte sans votre autorisation, mais vous ne pouvez jamais être sûr à 100 % de la sécurité de votre compte. Voici comment déterminer si une autre personne s'est connectée à votre compte Yahoo et les étapes à suivre pour récupérer l'accès à celui-ci.

Quelle que soit la situation, si vous pensez qu'une autre personne a accédé à votre compte sans votre autorisation, **changez votre mot de passe immédiatement**. Si vous n'avez pas accès à votre compte, utilisez l'aide relative aux mots de passe pour le récupérer.

Signes indiquant que votre compte a été piraté

• Vos informations de compte ont été modifiées à votre insu.

• Des connexions ont été établies depuis des endroits que vous ne reconnaissez pas sur la page de vos activités de connexion.

• Vous ne recevez pas des e-mails que vous attendiez.

• Votre compte Yahoo Mail envoie des spams

Ce que vous devez faire

Bloquer l'envoi de spam depuis votre compte

Recevoir des spams est une chose. Recevoir des rapports de spam provenant de votre compte en est une autre. Si votre compte a été piraté de sorte qu'il envoie des spams, vous pouvez résoudre ce problème ! Le moyen le plus rapide de bloquer l'envoi de spams depuis votre compte consiste à sécuriser votre compte en créant un nouveau mot de passe fiable ou activer la clé de compte.

Signaler un mail falsifié (usurpé)

Les messages falsifiés sont des mails qui semblent avoir été envoyés depuis votre adresse mail, mais qui en réalité ont été envoyés depuis un compte de messagerie complètement différent. Si votre Yahoo Mail est sécurisé, mais que vos contacts reçoivent toujours des spams qui semblent provenir de votre adresse, il s'agit probablement d'un mail falsifié ou « usurpé ».

1. Affichez l'en-tête complet du mail en question.

2. Dans la dernière ligne Reçu de l'en-tête complet, notez l'adresse IP d'où provient le mail.

– Cela correspond au fournisseur d'accès Internet (FAI) de l'expéditeur.

3. Effectuez une recherche par adresse IP sur un site tel que WhoIs.net pour déterminer le fournisseur d'accès Internet de l'expéditeur.

4. Contactez le fournisseur d'accès Internet de l'expéditeur pour demander que l'action appropriée soit entreprise.

Les fournisseurs de messagerie ne peuvent pas empêcher ces contrefaçons, mais si la fraude est identifiée, il est possible d'entreprendre une action.

Examinez les paramètres Yahoo Mail

• Supprimez les contacts mail inconnus.

• Supprimez les comptes Mail liés que vous ne reconnaissez ou ne contrôlez pas.

• Changer votre mot de passe sur les comptes liés que vous contrôlez.

• Vérifiez que votre réponse automatique de congés est désactivée.

• Découvrez si une autre personne a accédé à votre compte.

Autres paramètres de compte Yahoo Mail habituellement modifiés :

• Signature

• Nom d'expéditeur

• Adresse de réponse

• Transfert de mails

• Filtres

• Adresses interdites

Restaurer les mails, messages instantanés et contacts manquants

Si des mails, des messages instantanés ou des contacts sont manquants, vous pouvez restaurer les mails ou messages instantanés perdus ou supprimés. Vous pouvez également récupérer les contacts perdus.

Empêchez d'autres personnes d'accéder à nouveau à votre compte, même après avoir modifié votre mot de passe. Assurez-vous que votre compte reste protégé.

Recherchez la présence de logiciel malveillant sur votre ordinateur

Les logiciels malveillants peuvent corrompre votre système et collecter des informations sensibles, telles que des mots de passe et des coordonnées bancaires. Plusieurs programmes anti-logiciel malveillant sont disponibles sur Internet et permettent de détecter et de supprimer les logiciels malveillants sur les Mac et PC.

Réagissez à cet article

Original de l'article mis en page : Signes indiquant qu'un

compte a été piraté et procédure à suivre | Yahoo Aide – SLN2090

L’Agence mondiale anti-dopage victime de piratage

	L’Agence mondiale anti-dopage victime de piratage

L'Agence mondiale anti-dopage (AMA ou WADA en anglais) a été victime d'un piratage. Un groupe de hackers a pu subtiliser les dossiers médicaux de quatre athlètes américaines et dévoiler des informations confidentielles. Surprise : les pirates sont russes !

Les Russes l'auraient-ils mauvaise suite à la disqualification de la quasi-totalité de leurs athlètes lors des Jeux Olympiques de Rio ? Ce vaste « nettoyage » opéré par les fédérations sportives internationales faisait suite au scandale sur le dopage d'Etat généralisé en Russie. Toujours est-il que le groupe russe Tsar Team (APT28), Fancy Bear pour les intimes, a piraté une base de données de l'AMA.
La date exacte de l'attaque n'est pas connue. Les hackers ont vraisemblablement obtenu l'accès aux serveurs de l'Agence en obtenant par phishing des mots de passe ADAMS (pour Anti-Doping Administration and Management System, le SI de l'AMA), via un compte du Comité International Olympique créé à l'occasion des JO de Rio. Ils ont ainsi pu dérober les données relatives à quatre athlètes américaines, notamment leurs dossiers médicaux détaillés.

Simone Biles, quadruple championne olympique en athlétisme

Sur les réseaux sociaux, Fancy Bear a divulgué une partie de ces informations, pointant du doigt des « *analyses anormales* » dans les dossiers des joueuses de tennis Venus et Serena Williams, de la basketteuse Elena Delle Donne et de la gymnaste Simone Biles. L'AMA a pris la défense des athlètes mises en cause, expliquant qu'elles bénéficient d'exemptions thérapeutiques. Dans le cas de Simone Biles, par exemple, il s'agit d'un traitement pour trouble du déficit de l'attention, dont il avait déjà été question lors des JO. Mais les hackers promettent bien d'autres révélations.

« Miner le système anti-dopage mondial ».

Le CIO a condamné cette attaque, « *destinée à salir la réputation d'athlètes propres* ». L'AMA elle aussi condamne, et y voit une tentative de « *miner le système anti-dopage mondial* »…[lire la suite]

Réagissez à cet article

Original de l'article mis en page : Des hackers russes derrière le piratage de l'Agence mondiale anti-dopage

Comment se prémunir de la cybercriminalité, ce risque sur Internet pour les particuliers et les professionnels ?

Comment se prémunir de la cybercriminalité, ce risque sur Internet pour les particuliers et les professionnels ?

En pleine recrudescence, de nombreuses attaques ciblent les particuliers mais aussi les entreprises et les administrations. Elles visent à obtenir des informations personnelles afin de les exploiter ou de les revendre (données bancaires, identifiants de connexion à des sites marchands, etc.). Hameçonnage (phishing) et «Rançongiciel» (ransomware) sont des exemples connus d'actes malveillants portant préjudices aux internautes. Pour s'en prémunir, des réflexes simples existent.

QUELS SONT LES DIFFÉRENTS TYPES D'ATTAQUES ?

Attaque par hameçonnage (phishing)

L'hameçonnage, phishing ou filoutage est une technique malveillante très courante sur Internet. L'objectif : opérer une usurpation d'identité afin d'obtenir des renseignements personnels et des identifiants bancaires pour en faire un usage criminel.

1. Le cybercriminel se « déguise » en un tiers de confiance (banques, administrations, fournisseurs d'accès à Internet…) et diffuse un mail frauduleux, ou contenant une pièce jointe piégée, à une large liste de contacts. Le mail invite les destinataires à mettre à jour leurs informations personnelles (et souvent bancaires) sur un site internet falsifié vers lequel ils sont redirigés.
2. La liste comprend un nombre si important de contacts et augmente les chances que l'un des destinataires se sente concerné par le message diffusé.
3. En un clic, il est redirigé vers le site falsifié qui va recueillir l'ensemble des informations qu'il renseigne.
4. Ces informations sont alors mises à disposition du cybercriminel qui n'a plus qu'à faire usage des identifiants, mots de passe ou données bancaires récupérées.

Voir la vidéo de la Hackacademy sur le phishing (CIGREF – partenariat ANSSI)

Pour s'en prémunir :

- N'ayez pas une confiance aveugle dans le nom de l'expéditeur de l'email. Au moindre doute, n'hésitez pas à contacter l'expéditeur par un autre biais.
- Méfiez-vous des pièces jointes, elles pourraient être contaminées. Au moindre doute, n'hésitez pas à contacter l'expéditeur pour en connaître la teneur.
- Ne répondez jamais à une demande d'informations confidentielles par mail.
- Passez votre souris au-dessus des liens, faites attention aux caractères accentués dans le texte ainsi qu'à la qualité du français ou de la langue pratiquée par votre interlocuteur (ex : orthographe).

Pour aller plus loin, n'hésitez pas à consulter la page sur les conseils aux usagers qui reprend les bonnes pratiques à mettre en place pour sécuriser ses équipements et ses données.

Attaque par «Rançongiciel» (ransomware)

Les rançongiciels sont des programmes informatiques malveillants de plus en plus répandus (ex : Locky, TeslaCrypt, Cryptolocker, etc.). L'objectif : chiffrer des données puis demander à leur propriétaire d'envoyer de l'argent en échange de la clé qui permettra de les déchiffrer.

1. Le cybercriminel diffuse un mail qui contient des pièces jointes et / ou des liens piégés. Le corps du message contient un message correctement rédigé, parfois en français, qui demande de payer rapidement une facture par exemple.
2. En un clic, le logiciel est téléchargé sur l'ordinateur et commence à chiffrer les données personnelles : les documents bureautiques (.doc, .xls, .odf…etc), les photos, la musique, les vidéos…etc.
3. Les fichiers devenus inaccessibles, un message s'affiche pour réclamer le versement d'une rançon, payable en bitcoin ou via une carte prépayée, en échange de la clé de déchiffrement. Attention, rien n'indique que le déchiffreur en question soit efficace !

Pour s'en prémunir :

- N'ayez pas une confiance aveugle dans le nom de l'expéditeur de l'email. Au moindre doute, n'hésitez pas à contacter l'expéditeur par un autre biais.
- Méfiez-vous des pièces jointes et des liens dans les messages dont la provenance est douteuse. Au moindre doute, n'hésitez pas à contacter l'expéditeur pour en connaître la teneur.
- Effectuez des sauvegardes régulièrement sur des périphériques externes.
- Mettez à jour régulièrement tous vos principaux logiciels en privilégiant leur mise à jour automatique.

Pour aller plus loin, n'hésitez pas à consulter la page sur les conseils aux usagers qui reprend les bonnes pratiques à mettre en place pour sécuriser ses équipements et ses données.

VOUS ÊTES VICTIME D'UN RANSOMWARE OU DE FISHING ?

Suite à une escroquerie ou une cyberattaque, déposez plainte auprès d'un service de **Police nationale** ou de **Gendarmerie nationale** ou bien adressez un courrier au Procureur de la République auprès du Tribunal de Grande Instance compétent.

Munissez-vous de tous les renseignements suivants :

- Références du (ou des) transfert(s) d'argent effectué(s)
- Références de la (ou des) personne(s) contactée(s): adresse de messagerie ou adresse postale, pseudos utilisés, numéros de téléphone, fax, copie des courriels ou courriers échangés…
- Numéro complet de votre carte bancaire ayant servi au paiement, référence de votre banque et de votre compte, et copie du relevé de compte bancaire où apparaît le débit frauduleux
- Tout autre renseignement pouvant aider à l'identification de l'escroc

Vous pouvez également signaler les faits dont vous avez été victime via la plateforme de signalement « Pharos » ou le numéro dédié : 0811 02 02 17

Des services spécialisés se chargent ensuite de l'enquête :

- **Police nationale** : l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC) qui dépend de la Sous-direction de lutte contre la cybercriminalité (SDLC) : 01 47 44 97 55
- **Gendarmerie nationale** : le centre de lutte contre les criminalités numériques (C3N) du Service Central du Renseignement Criminel (SCRC) :cyber@gendarmerie.interieur.gouv.fr
- **Préfecture de police** : la Préfecture de police de Paris, de la Direction centrale du renseignement intérieur (DCRI) et ses équipes de la Brigade d'enquêtes sur les fraudes aux technologies de l'information (BEFTI) compétente uniquement pour Paris et petite couronne (75, 92, 93 et 94) : 01 40 79 67 50

Article original de gouvernement.fr

Réagissez à cet article

Original de l'article mis en page : Cybercriminalité | Gouvernement.fr

---

Et si Gmail vous protégeait contre les expéditeurs potentiellement malveillants ?

Et si Gmail vous protégeait contre les expéditeurs potentiellement malveillants ?

Gmail renforce ses outils de filtrage contre les expéditeurs non authentifiés et les liens vers des sites frauduleux ou indésirables.

Google ajoute de nouvelles fonctionnalités à Gmail pour protéger toujours plus ses utilisateurs des dangers du Net. Dans les prochaines semaines, le webmail se verra doté d'un système alertant son utilisateur quand il reçoit un e-mail en provenance d'un expéditeur non authentifié. Un point d'interrogation s'affichera alors en lieu et place de l'image correspondant au profil de l'expéditeur, à côté de son nom (voir l'image ci-dessous), indique le service de mise à jour des applications de l'entreprise de Mountain View.

Une façon d'inviter le destinataire à la plus grande prudence face à un e-mail douteux, surtout si le message contient des pièces jointes. Même si tous les expéditeurs non authentifiés ne sont pas nécessairement des pourvoyeurs de spam ou d'autres contenus à caractères frauduleux. *« Il peut arriver que l'authentification ne fonctionne pas lorsqu'une organisation envoie des messages à de grands groupes d'utilisateurs, via des listes de diffusion, par exemple »*, rappelle Google dans l'aide de Gmail.

Pour authentifier les expéditeurs, Google s'appuie sur les protocoles SPF et DKIM. Le premier (Sender Policy Framework) se charge de vérifier le nom de domaine de l'expéditeur d'un courriel. Ce protocole est normalisé dans la RFC 7208 dans l'objectif de réduire les envois de spams. Le second, DomainKeys Identified Mail, permet à l'expéditeur de signer électroniquement son message afin de garantir à la fois l'authenticité du domaine ainsi que l'intégrité du contenu.

Deuxième niveau d'alerte

Au cas où un expéditeur malintentionné aurait réussi à contourner (ou exploiter) ces normes d'authentification, Gmail s'enrichit d'un deuxième niveau de protection. Lorsque l'utilisateur cliquera sur un lien considéré comme frauduleux (pointant vers un site de phishing, pourvoyeur de malwares, voire de logiciels indésirables), il sera averti par le système des risques qu'il encourt à poursuivre sa navigation. Une fonction héritée du Safe Browsing, un système lancé en 2006 chargé de référencer les sites frauduleux, et qui équipe le navigateur Chrome mais aussi Firefox et Safari (via une API).

Signalons que Safe Browsing est en évolution constante, notamment grâce à la participation des internautes. Le mois dernier, Google a annoncé renforcer cette protection. *« Dans les prochaines semaines, ces améliorations de détection deviendront plus visibles dans Chrome : les utilisateurs verront plus d'avertissements que jamais sur les logiciels indésirables »*, indiquait alors l'éditeur.

Article original de Christophe Lagane

Réagissez à cet article

Original de l’article mis en page : Gmail va pointer les expéditeurs potentiellement malveillants

---

Attention aux versions piégées de Pokémon GO

Attention aux versions piégées de Pokémon GO

L’application Pokémon Go fait un carton dans les smartphones. Prudence, non encore officiel en Europe, installer le jeu via des boutiques hors de contrôle des auteurs met en danger votre vie privée.

Pas de doute, le phénomène Pokémon GO débarque en force en cet été 2016. L’application tirée du jeu éponyme de Nintendo permet de s’éclater à trouver des Pokemons un peu partout dans le monde. De la réalité virtuelle bien venue pour l’été.

Édité par Niantic, le créateur de Pokémon GO ne propose son appli qu’aux États-Unis, en Australie et en Nouvelle-Zélande. Un pré lancement pour tester les serveurs, très sollicités, et la stabilité du jeu. Bref, normalement, il n’est pas possible d’y jouer en Europe, et donc en France. Sauf qu’il y a toujours des possibilités, comme celle d’installer Pokémon GO vient l’APK (le programme) proposé par de nombreux sites Internet non officiels.

Attention ! des sites qui ne sont pas maîtrisés et contrôlés par les auteurs. Des espaces de téléchargements qui sont des limites du Play Store de Google et de l’App Store d’Apple. Bref, à vos risques et périls.

J’ai déjà pu repérer des APK piégés (ransomwares, cheval de Troie, …) proposés, je l’avoue, dans des lieux peu recommandables. Prenez l’avertissement très au sérieux. Pokemon GO ne vous demandera JAMAIS d’accéder à vos messages [SMS, MMS], à vos appels téléphoniques. Si l’APK que vous avez téléchargez vous propose ces « autorisations », ne l’installez surtout pas. Attendez la version officielle.

Je ne me voile pas la face, le phénomène attire beaucoup d’internautes, jeunes et moins jeunes. Et avec les vacances, une bonne occasion de sauter sur le jeu pour smartphone de l’été. Des milliers de Français l’ont fait. J’en croise beaucoup, dans la rue, comme le montre ma photographie, prise ce 13 juillet dans les rues de Paris. Je rentre de New York, l’engouement est… pire !

A noter que plusieurs éditeurs d’antivirus ont mis la main sur une version « malveillante » de Pokémon GO. Bitdefender, par exemple, parle de DroidJack. Ce cheval de Troie ouvre une backdoor et donne l’accès aux données des appareils mobiles infectés, permettant ainsi leur prise de contrôle à distance par les pirates. Ce malware disponible pour seulement 200 dollars sur certains sites Web, offre au pirate une interface de contrôle facile à utiliser lui permettant par exemple de surveiller l’activité des appareils corrompus, de passer des appels, d’envoyer des SMS, de localiser l’appareil, d’utiliser l’appareil photo ou le microphone ou même d’accéder aux dossiers.

La version iPhone malmenée par la version officielle

Autre mise en garde pour les joueurs de Pokémon GO : sur iOS, l’application semble demander plus d’autorisations que nécessaire. L’accès à l’application via un compte Google semble conférer au développeur Niantic (ex Start-up de Google), un accès complet aux comptes des utilisateurs. Ce problème est en cours de résolution et n’est pas présent dans les versions Android.

Article original de Damien Bancal

Réagissez à cet article

Original de l’article mis en page : ZATAZ Pokémon GO, prudence aux fichiers vérolés – ZATAZ

Sensibilisation au Phishing

Sensibilisation au Phishing

Vous feriez confiance à cet homme ? Sur Internet aussi, soyez vigilants: il arrive que des acheteurs ou vendeurs malhonnêtes essaient de vous arnaquer. Découvrez les bons réflexes sécurité avec PayPal. Acheter et vendre en ligne est simple et sécurisé avec PayPal, 7 millions de Français nous utilisent déjà.

https://www.youtube.com/watch?v=00Nr59TlDas

Campagne Paypal France 2016

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

Euro 2016 et sécurité informatique, quelques conseils face à quelques risques…

Euro 2016 et sécurité informatique, quelques conseils face à quelques risques…

Euro 2016 – Les événements sportifs mondiaux ont toujours constitué un terrain de chasse idéal pour les cybercriminels. L'Euro 2016, qui débute le 10 juin prochain, ne devrait pas déroger à la règle.

Euro 2016 – Voici quelques éléments clés à retenir, amateur de football, de l'Euros 2016 ou non. Se méfier du spam et autre fausses « bonnes affaires » (places pour assister aux matchs à des prix défiant toute concurrence, par exemple). Ces mails peuvent contenir une pièce jointe infectée contenant un malware accédant au PC et interceptant les données bancaires des internautes lorsqu'ils font des achats en ligne. Ils peuvent également contenir un ransomware, qui verrouille et chiffre les données contenues dans le PC et invite les victimes à verser une rançon pour les récupérer.
Détecter les tentatives de phishing (vente de tickets à prix cassés voire gratuits, offres attractives de goodies en lien avec l'évènement,…) en vérifiant l'URL des pages auxquelles le mail propose de se connecter et en ne communiquant aucune information confidentielle (logins/mots de passe, identifiants bancaires, etc.) sans avoir préalablement vérifié l'identité de l'expéditeur.
Être prudent vis à vis du Wi-Fi public pour éviter tout risque de fuite de données, par exemple en désactivant l'option de connexion automatique aux réseaux Wi-Fi. Les données stockées sur les smartphones circulent en effet librement sur le routeur ou le point d'accès sans fil (et vice-versa), et sont ainsi facilement accessibles.
Redoubler de vigilance vis-à-vis des mails invitant à télécharger un fichier permettant d'accéder à la retransmission des matchs en temps réel. Il s'agit en réalité de logiciels malveillants qui, une fois exécutés, permettent d'accéder aux données personnelles stockées dans le PC (mots de passe, numéro de CB, etc.) ou utilisent ce dernier pour lancer des procédures automatiques comme l'envoi de mails massifs. (TrendMicro).
Auteur : Damien Bancal

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

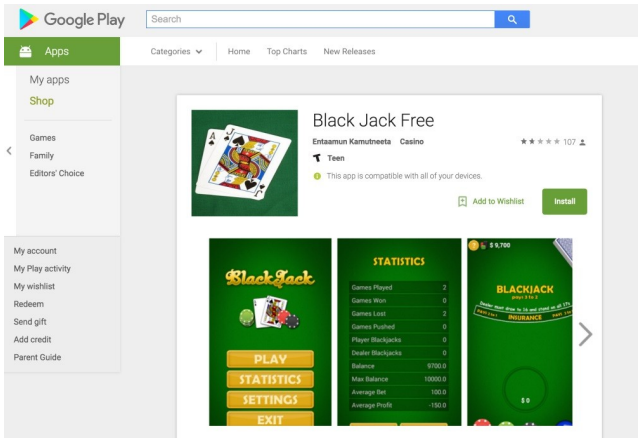
Original de l'article mis en page : Football : Euro 2016 et sécurité informatique – Data Security BreachData Security Breach

---

Alerte : Un Trojan détecté sur Google Play

Alerte : Un Trojan détecté sur Google Play

Lookout, spécialiste dans la sécurité mobile a détecté « Black Jack Free », un jeu gratuit sur Google Play qui appartient à la famille du Trojan Acecard.



S'il est de bon augure de se méfier des jeux d'argents, il faut les craindre d'autant plus lorsqu'ils sont sur internet. L'application Black Jack Free qui était en fait un Trojan a été téléchargée plus de 5000 fois avant d'être retirée du Google Play Store quatre jours plus tard. A première vue, il n'y avait rien à craindre de ce jeu de cartes qui permettait de jouer gratuitement tout en utilisant de l'argent fictif. Sauf que, dans l'arrière boutique l'application dérobait des données, mais aussi de l'argent sur les comptes en banque des utilisateurs. «Black Jack Free n'était pas directement le problème. Mais il installait une deuxième application, Play Store Update qui repérait les applications actives sur internet et imitait les pages d'accueil» explique Arnaud Simon, responsable technique Europe du sud chez Lookout.
Par ce stratagème, l'application superposait des fenêtres sur les applications bancaires, ou sur les réseaux sociaux comme Facebook ou Skype par exemple. Ensuite, les utilisateurs entraient leurs codes et identifiants sans se douter que des pirates les récupéraient. Play Store Update pouvait aussi intercepter des SMS, les envoyer vers un serveur malicieux, transférer des appels, verrouiller l'écran et effacer les données d'un terminal.

Un risque plus ou moins écarté

Il est donc fortement conseillé aux utilisateurs ayant téléchargé Black Jack Free de supprimer l'application de leurs terminaux Android et de se débarrasser de Play Store Update également. Ensuite, pour éviter les mauvaises surprises, Lookout invite les personnes concernées à modifier leurs codes d'accès.
A noter que « l'application était disponible sur Google Play car les pirates disposaient d'un accès potentiel à de nombreux terminaux. Mais les hackers ne se sont pas contentés de diffuser Black Jack Free sur cette seule et unique plateforme, elle est disponible ailleurs sur le web», ajoute Arnaud Simon. Comprendre que le Trojan court toujours et que la méfiance reste de mise.
Article original de Victor Mayet

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

Source : *Un Trojan détecté sur Google Play*

Forte hausse des applications Android malveillantes

Forte hausse des applications Android malveillantes

Les applications Android malveillantes et les ransomwares dominent le paysage des menaces au 1er trimestre 2016.

La société Proofpoint a publie son Rapport trimestriel sur les menaces, qui analyse les menaces, les tendances et les transformations observées au sein de notre clientèle et sur le marché de la sécurité dans son ensemble au cours des trois derniers mois. Chaque jour, plus d'un milliard de courriels sont analysés, des centaines de millions de publications sur les réseaux sociaux et plus de 150 millions d'échantillons de malwares afin de protéger les utilisateurs, les données et les marques contre les menaces avancées. On apprend, entre autres, que 98 % des applications mobiles malveillantes examinées au 1er trimestre 2016 ont ciblé des appareils Android. Cela demeure vrai en dépit de la découverte médiatisée d'un cheval de Troie pour iOS et de la présence persistante d'applications iOS ou officieuses dangereuses. Les applications Android malveillantes sont de plus en plus nombreuses.

75 % des attaques de phishing véhiculées par des e-mails imposteurs comportent une adresse «répondre à » usurpée afin de faire croire aux destinataires que l'expéditeur est une personne représentant une autorité. Ce type de menaces est de plus en plus mature et spécialisé, et c'est l'un des principaux ciblant les entreprises aujourd'hui, qui leur auraient coûté 2,6 milliards de dollars au cours des deux dernièresannées selon les estimations.

Applications Android malveillantes

Les ransomwares se sont hissés aux premiers rangs des malwares privilégiés par les cybercriminels. Au 1er trimestre, 24 % des attaques par e-mail reposant sur des pièces jointes contenaient le nouveau ransomware Locky. Seul le malware Dridex a été plus fréquent.

L'e-mail reste le principal vecteur de menaces : le volume de messages malveillants a fortement augmenté au 1er trimestre 2016, de 66 % par rapport au 4ème trimestre 2015 et de plus de 800 % comparé au 1er trimestre 2015. Dridex représente 74 % des pièces jointes malveillantes.

Chaque grande marque analysée a augmenté ses publications sur les réseaux sociaux d'au moins 30 %. L'accroissement du volume des contenus générés par les marques et leurs fans va de pair une accentuation des risques. Les entreprises sont constamment confrontées au défi de protéger la réputation de leurs marques et d'empêcher le spam, la pornographie et un langage grossier de polluer leur message.

Les failles de Java et Flash Player continuent de rapporter gros aux cybercriminels. Angler est le kit d'exploitation de vulnérabilités le plus utilisé, représentant 60 % du trafic total imputable à ce type d'outil. Les kits Neutrino et RIG sont également en progression, respectivement de 86 % et 136 %. (ProofPoint)… [Lire la suite]

Article de Damien BANCAL

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

Source : *Forte hausse des applications Android malveillantes – Data Security BreachData Security Breach*