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

---

Les logiciels indésirables sont 3 fois plus répandus que les malwares

Les logiciels indésirables sont 3 fois plus répandus que les malwares

---

Google génère 60 millions d'alertes aux logiciels indésirables chaque semaine. Les injecteurs de publicités et autres scarewares se cachent, le plus souvent, dans les offres groupées de logiciels.

Disponible pour Google Chrome, Mozilla Firefox et Apple Safari, la fonction Navigation sécurisée de Google analyse des milliards d'URL. Chaque semaine, elle génère plus de 60 millions d'alertes aux logiciels indésirables, selon Google. C'est trois fois plus que le nombre d'avertissements concernant des programmes malveillants (malwares), tels que les virus, les vers et les chevaux de Troie.

Paiement à l'installation (PPI)

La plupart des alertes aux logiciels non sollicités apparaissent lorsque les utilisateurs téléchargent involontairement un pack de logiciels (*software bundles*) bardé d'applications additionnelles. Ce modèle peut rapporter au diffuseur jusqu'à 1,50 dollar par installation effective (*pay-per-install*, PPI).

Outre la cible (les internautes), de nombreux acteurs sont impliqués : annonceurs, réseaux d'affiliation, développeurs, éditeurs et distributeurs des logiciels. Toutes les offres groupées de logiciels ne cachent pas une tentative d'installation de programmes non sollicités. Mais il suffit d'un acteur peu scrupuleux dans la chaîne de distribution pour inverser la tendance.

Injecteurs de publicités

Une étude menée par des chercheurs de Google, de NYU et de l'ICSI de Berkeley, montre que les réseaux PPI fleurissent (une cinquantaine a été analysée). Quatre des réseaux les plus étendus distribuaient régulièrement des injecteurs de publicités, des détourneurs de navigateur et des rogues ou scarewares. Ces derniers sont de faux logiciels de sécurité. Ils prennent la forme de fenêtres d'alerte et prétendent que les fichiers du système utilisé par l'internaute sont infectés…

Par ailleurs, 59 % des offres des réseaux d'affiliation PPI ont été signalées comme étant indésirables par au moins un antivirus. Pour détecter la présence de ces antivirus, les programmes indésirables vont le plus souvent marquer d'une empreinte (*fingerprinting*) la machine de l'utilisateur. Ils ont aussi recours à d'autres techniques pour contourner les mesures de protection.

Autorégulation

« Ces packs de logiciels sont promus à travers de fausses mises à jour, des contenus bidons et du détournement de marques », explique Google dans un billet de blog. *« Ces techniques sont ouvertement présentées sur des forums souterrains comme des moyens destinés à tromper les utilisateurs pour qu'ils téléchargent involontairement des logiciels et acceptent les termes d'installation proposés »*.

« Ce modèle décentralisé incite les annonceurs à se concentrer uniquement sur la monétisation, et les éditeurs à maximiser la conversion sans tenir compte de l'expérience utilisateur final », regrettent les chercheurs de Google Kurt Thomas et Juan Elices Crespo.

L'industrie travaille à l'encadrement de ces pratiques. C'est l'objectif affiché de la Clean Software Alliance, regroupement d'acteurs de la distribution de logiciels et d'éditeurs d'antivirus. Impliqué, Google détaillera ses plans cette semaine lors du USENIX Security Symposium d'Austin, Texas.

Article original de Ariane Beky

Réagissez à cet article

Original de l'article mis en page : Logiciels indésirables : 3 fois plus répandus que les malwares

Usages et attentes des Français à l’égard du digital en matière d’information sur leur santé

6

Usages et attentes des Français à l’égard du digital en matière d’information sur leur santé

Dans un monde de santé de plus en plus connecté et digitalisé, 4 français sur 10 restent insatisfaits des informations santé qu'ils trouvent sur internet. A la veille du lancement par le laboratoire pharmaceutique MSD d'une nouvelle plateforme digitale d'information médicale, le groupe et Ipsos se sont intéressés aux usages et attentes des Français à l'égard des informations médicales trouvées sur internet.

Article original de Ipsos

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.

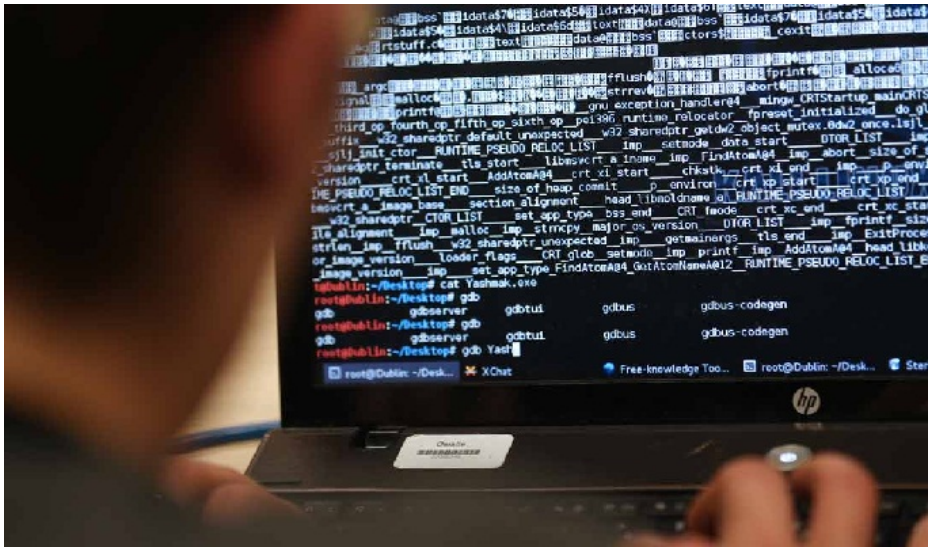
Le Net Expert
INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Original de l’article mis en page : Usages et attentes des Français à l’égard du digital en matière d’information sur leur santé

Cyberattaques terroristes déjouées au Maroc



Cyberattaques terroristes déjouées au Maroc

Des cyberattaques de sites étatiques planifiées par des individus soupçonnés d'avoir des penchants extrémistes et des relations avec Daech ont été déjouées dans le Royaume du Maroc grâce à une vaste opération antiterroriste qui a abouti à l'arrestation et la garde à vue de 52 personnes.

Selon un communiqué du ministère de l'Intérieur cité par des médias locaux, dont le Matin.ma, ainsi que le quotidien ivoirien Fraternité Matin, cette opération antiterroriste a été menée sous la houlette du parquet général et visait 343 individus.

Outre des projets terroristes ciblant des centres de loisir, des festivals, des établissements sécuritaires du Royaume, des cyberattaques à un niveau de préparation bien avancée devaient être dirigées contre les institutions marocaines. Objectif? Bloquer le fonctionnement des structures étatiques et paralyser l'économie.

D'autres personnes arrêtées par les forces de police marocaine sont soupçonnées de recruter des combattants mineurs via les réseaux sociaux.

Article original de Alselme AKEKO

Réagissez à cet article

Original de l’article mis en page : Terrorisme : des cyberattaques déjouées au Maroc | CIO MAG

Quelques domaines d’application du Big Data dans les Comment les données améliorent les services communaux | L’Atelier : Accelerating Innovation

Quelques domaines d’application du Big Data

Original de l’article mis en page : Comment les données améliorent les services communaux | L’Atelier : Accelerating Innovation

---

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

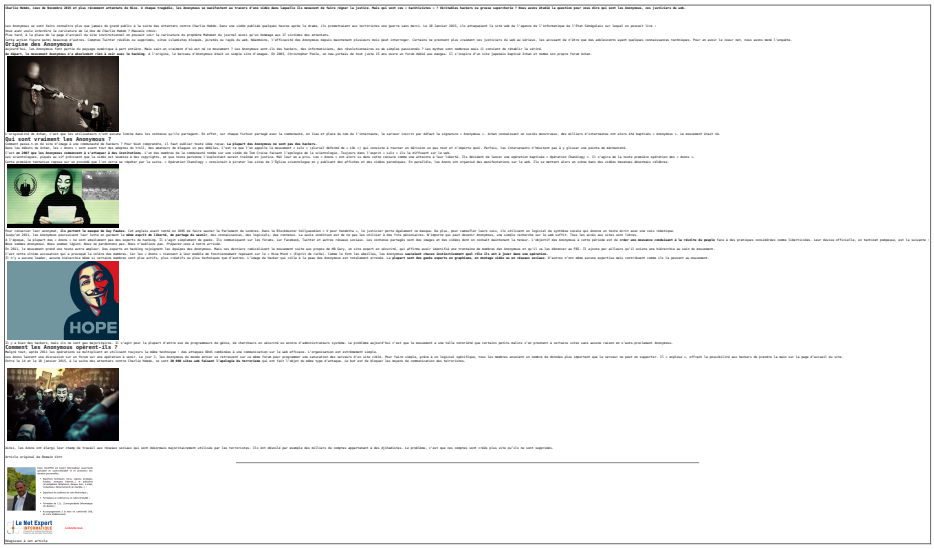
Réagissez à cet article

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

de mots de passe nuisent à la sécurité

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