Michelin victime de « l'arnaque au président », Banque – Assurances

Michelin victime de « l'arnaque au président »

Le fabricant de pneumatiques s'est fait dérober 1,6 million d'euros au moyen de l'arnaque dite « du président ».

L'arnaque est désormais bien rodée, et Michelin en est la dernière victime. Le fabricant de pneumatiques s'est fait dérober 1,6 million d'euros via une escroquerie reposant sur de faux ordres de virement, a-t-il indiqué lundi à l'AFP, confirmant une information du journal « Le Parisien ». La méthode employée est celle de « l'arnaque au président », qui sévit de plus en plus dans les entreprises.

Modus operandi

Un individu se fait généralement passer pour le président ou l'un des directeurs d'une société ou d'un groupe, et appelle un comptable de niveau assez bas dans hiérarchie, à qui il demande, dans le cadre d'une opération soi-disant très confidentielle, un virement urgent vers un pays étranger. Bien souvent, il s'agit de la Chine, ou de Chypre, mais cette fois, le pseudo directeur financier a réclamé que les règlements soient effectués sur le compte d'une banque en République tchèque. « Cet homme connaissait parfaitement la procédure à suivre et la personne à contacter au sein du groupe Michelin pour pouvoir effectuer cette modification en toute discrétion », a rapporté une source proche de l'affaire. Une enquête a été ouverte et confiée à la police judiciaire de Clermont-Ferrand.

Michelin n'est pas le premier groupe à être victime d'une telle escroquerie, « la plus redoutable » et qui requiert « une autorité naturelle, un certain aplomb et […] un don pour la comédie », expliquait récemment aux « Echos » le SRPJ de Clermont-Ferrand. Pour le service régional de police judiciaire, ces arnaques sont de trois types : outre « l'arnaque au président », on trouve l'escroquerie « à la nigériane » ou encore le détournement de la nouvelle norme Sepa , l'espace de paiement unique européen.

La fédération française bancaire a récemment mis en ligne une vidéo afin de prévenir les escroqueries aux ordres de virement :

Selon l'Office central pour la répression de la grande délinquance, quelque 700 faits ou tentatives ont ainsi été recensés entre 2010 et 2014. Le montant des préjudices atteignait, en août dernier, plus de 250 millions d'euros. Le cabinet KPMG (audits et expertises comptables) avait révélé cette année en avoir été victime, pour un préjudice de 7,6 millions d'euros.

Denis JACOPINI et son équipe vous propose des formations pour sensibiliser les salariées à ce type de pratiques cybercriminelles.

N'hésitez pas à me contacter pour organiser une session de formation. (Denis JACOPINI)

Source :

http://www.lesechos.fr/finance-marches/banque-assurances/0203910698411-michelin-victime-de-larnaque-au-president-1060501.php

Outlook Web App ciblé par des attaques de phishing sophistiquées – Le Monde Informatique

Outlook Web App ciblé par des attaques de phishing sophistiquées

Selon les chercheurs de Trend Micro, un groupe de pirates sévit à l'encontre d'agences militaires, ambassades et d'entreprises liées à la défense nationale et des médias internationaux utilisant Outlook Web App d'Office 365.

Afin de voler les identifiants de messagerie des employés de nombreuses organisations publiques, parapubliques mais également privées, un groupe d'espions a mis en place des techniques de phishing avancées.
Selon des chercheurs de l'entreprise de sécurité Trend Micro, qui ont baptisé cette campagne Operation Pawn Storm dans un document publié la semaine dernière, le groupe à l'origine de ces attaques opèrerait depuis au moins 2007. Au cours de ces années, ils ont utilisé différentes techniques pour atteindre leurs objectifs, notamment des campagnes de phishing pour propager des malwares sous forme de pièces jointes Microsoft Office malveillantes, l'installation de backdoors type SEDNIT ou Sofacy, ou des exploits plus sélectifs pour infecter des sites légitimes.

Dans ses dernières attaques de phishing, le groupe a utilisé une technique particulièrement intéressante, ciblant les organisations qui utilisent Outlook Web App (OWA), une composante du service Office 365 proposé par Microsoft. Pour chaque attaque, le groupe a créé deux faux domaines : un premier, qui reproduit un site Web tiers connu des victimes – par exemple le site d'une conférence dans un secteur de l'industrie qui les intéresse – et un second, similaire au domaine utilisé pour le déploiement d'Outlook Web App par l'organisation visée. Les attaquants ont ensuite créé des courriels contenant un lien vers le faux site tiers sur lequel ils hébergeaient un code JavaScript non malveillant dont le but était double : ouvrir le site légitime dans un nouvel onglet et rediriger l'onglet déjà ouvert du navigateur Outlook Web App vers une page de phishing. « Le code JavaScript faisait croire aux victimes que leur session OWA était close, et la page malveillante leur demandait de se reconnecter en tapant à nouveau leurs identifiants », ont écrit les chercheurs de Trend Micro dans leur document.
« Les attaquants ont réussi à rediriger les victimes vers de fausses pages Outlook Web App en agissant sur les propriétés d'ouverture des pages de leurs navigateurs ».

Une technique de phishing multi-navigateurs
Selon les chercheurs, cette technique n'exploite aucune vulnérabilité et fonctionne avec tous les navigateurs courants dont Internet Explorer, Mozilla Firefox, Google Chrome et Safari d'Apple. Cependant, il faut deux conditions pour que ce mode opératoire fonctionne : « Les victimes doivent utiliser OWA et ils doivent cliquer sur les liens intégrés au volet de prévisualisation OWA », ont-ils expliqué. L'attaque est redoutable parce que l'onglet du navigateur ne permet pas aux victimes de voir que leur session OWA est illégitime et ils ont peu de chance de se rendre compte que l'URL a été usurpée avant de rentrer leurs identifiants. « De plus, les attaquants ont pris soin d'utiliser des noms de domaine très similaires à ceux choisis par les organisations ciblées pour leurs pages de log in OWA, et dans certains cas, ils ont même acheté des certificats SSL légitimes, de sorte que les navigateurs des victimes affichent aussi les indicateurs de connexion sécurisée HTTPS pour les sites de phishing », ont encore ajouté les chercheurs de Trend Micro.

Parmi les personnes visées, on trouve des employés de l'entreprise militaire privée américaine Academi, anciennement connue sous le nom de Blackwater ; l'Organisation pour la sécurité et la coopération en Europe (OSCE) ; le Département d'État des États-Unis ; le fournisseur du gouvernement américain Science Applications International Corporation (SAIC) ; une société multinationale basée en Allemagne ; l'ambassade du Vatican en Irak ; des médias de radiodiffusions de plusieurs pays ; les ministères de la Défense de la France et de la Hongrie ; des responsables militaires pakistanais ; des employés du gouvernement polonais et des attachés militaires de différents pays. Parmi les appâts utilisés par les assaillants, les chercheurs ont identifié des événements et des conférences bien-connus pour lesquels les victimes pouvaient avoir un intérêt.
« Mais, ce n'est pas tout : les assaillants ont combiné leur tactique de phishing à diverses attaques éprouvées afin de compromettre les systèmes et entrer dans les réseaux pour y voler des données », ont déclaré les chercheurs de Trend Micro.
« Les variantes de SEDNIT utilisées ont été semble-t-il très efficaces car elles ont permis aux pirates de voler des informations sensibles sur les ordinateurs des victimes en évitant de se faire repérer ».

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Source :
http://www.lemondeinformatique.fr/actualites/lire-outlook-web-app-cible-par-des-attaques-de-phishing-sophistiquees-59081.html

---

Après JP Morgan, 9 autres banques auraient été piratées

Après JP Morgan, 9 autres banques auraient été piratées

Le groupe responsable du piratage de JP Morgan cet été aurait mené des attaques sur 9 autres établissements financiers. Comme la loi américaine n'oblige pas les banques à communiquer sur ce genre d'incident, l'ampleur exacte de la fuite potentielle de données reste inconnue.

JP Morgan serait loin d'être la seule banque à avoir été attaquée par ce groupe de pirates. Il s'agirait en réalité d'une vague d'intrusions, dont l'ampleur exacte reste inconnue.

Elle aurait permis aux assaillants « d'infiltrer environ 9 autres établissements financiers », explique le New York Times en s'appuyant sur des sources proches de l'enquête.

De nombreux points à éclaircir
Peu de détails ont été révélés par les canaux officiels. D'ailleurs, le journal américain n'a pas pu obtenir les noms des établissements infiltrés et ignore toujours ce à quoi les pirates ont pu accéder.
JP Morgan, seule banque à avoir communiqué sur le sujet, affirme que les responsables n'ont pu accéder qu'aux noms des clients et à d'autres informations non-financières. Le personnel chargé de la sécurité de la banque aurait repéré l'attaque avant que les assaillants n'accèdent aux données sensibles. Ceci étant dit, l'intrusion n'aurait pas été entièrement arrêtée avant la mi-août alors qu'elle avait débuté en juillet.
Pour ce qui est de l'identité des pirates, les autorités en charge de l'enquête pencheraient pour un groupe opérant depuis la Russie. Ils auraient une « vague connexion » avec des membres du gouvernement de Moscou.
Les motivations des pirates restent, elles aussi, inconnues. Cependant, ces attaques pourraient avoir été menées en représailles aux sanctions visant la Russie dans le cadre de la crise ukrainienne, présument les services de renseignement américains.

Une brèche dans les systèmes mais aussi dans la loi ?
Outre l'aspect sécuritaire, l'attaque met en évidence une potentielle lacune dans la loi américaine. On apprend aujourd'hui que l'incident a bien plus d'ampleur qu'il n'y parait. Peut être qu'une meilleure information aurait permis de limiter l'intrusion ou d'aider à faire avancer l'enquête. Seulement, les banques en ligne ne sont pas obligées de communiquer sur les événements ayant pu compromettre les données des clients à moins qu'ils leur aient fait perdre de l'argent.

Dans certains Etats américains, les banques peuvent attendre jusqu'à un mois avant d'informer les autorités et les clients de ce type d'incident. La loi californienne, par exemple, impose simplement un délai « raisonnable », une définition sujette à interprétations. Il est alors difficile, dans un tel contexte, de lutter efficacement contre ce type de piratage.

La France n'est pas mieux lotie : les banques ne sont pas tenues d'informer les clients lors d'une fuite de données. Pour l'instant, seuls les fournisseurs d'accès et opérateurs ont l'obligation de notifier la CNIL ou les clients. Cependant, le régulateur français et ses équivalents européens cherchent à étendre ces exigences à l'ensemble des services en ligne.

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Source :
http://pro.clubic.com/it-business/securite-et-donnees/actualite-731231-jp-morgan-9-banques-attaquees-pirates.html

500 000 PC infectés à cause d’une faille Windows XP

500 000 PC infectés à cause d’une faille Windows XP

Selon les chercheurs en sécurité de Proofpoint, 52% des PC infectés par le botnet Qbot font tourner Windows XP. Exploitant une faille de Windows XP mais également de Seven et Vista, un groupe de cybercriminels russe a réussi à activer le botnet Qbot fort 500 000 PC zombies, essentiellement localisés aux Etats-Unis. Son objectif : Aspirer les identifiants bancaires des utilisateurs de ces PC corrompus.

Des pirates russes à l’origine du botnet Qbot ont construit une impressionnante armée de 500 000 PC zombies en exploitant des failles non corrigées dans des ordinateurs tournant sous Windows XP mais également Windows 7 et Vista. Des PC localisés principalement aux Etats-Unis, a fait savoir la société Proofpoint. Ces derniers temps, les hackers russes ont fait monter la pression avec des incursions sérieuses telle que l’attaque qui a visé la banque américaine JPMorgan Chase. Avec ce botnet, baptisé Qbot, les chercheurs de Proofpoint ont fait ressortir que le groupe qui est à l’origine de sa création l’a élaboré de façon méticuleuse à travers le temps, sans faire de vague, au point de rester sous les radars des sociétés de sécurité et donc de ne pas avoir attiré leur attention.

Selon Proofpoint, 75% des 500 000 PC infectés par le botnet Qbot sont situés aux Etats-Unis, sachant que parmi eux, 52% font tourner Windows XP, 39% Windows 7 et 7% Windows Vista. En Grande-Bretagne, la proportion de PC infectés est bien moindre, 15 000 postes environ. « Avec 500 000 clients infectés volant les identifiants des comptes bancaires en ligne des utilisateurs, le groupe de cybercriminels a le potentiel pour réaliser des bénéfices vertigineux », ont indiqué les chercheurs de la société de conseil en sécurité. Mais le botnet Qbot ne s’attaque pas seulement aux comptes bancaires, il compromet également les sites WordPress, soit en infectant le site lui-même ou bien en injectant des contenus corrompus dans leurs newsletters.
Article de Dominique Filippone

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Source :
http://www.lemondeinformatique.fr/actualites/lire-500-000-pc-infectes-a-cause-d-une-faille-windows-xp-58878.html

JP Morgan piraté : les données de 83 millions de clients exposées

JP Morgan piraté : les données de 83 millions de clients exposées

Cet été, JP Morgan a été victime d'une attaque informatique de grande envergure. La banque américaine admet que les données de 83 millions de clients ont pu être exposées. Toutefois, il ne s'agirait pas d'informations sensibles pour la porte-parole de la société.

76 millions de foyers et 7 millions de PME seraient concernés par ce qui pourrait être l'une des plus grandes fuites de données de l'histoire. Cet été, les systèmes informatiques de la banque JP Morgan ont été compromis par une attaque ayant permis aux pirates d'accéder aux noms, adresses, numéros de téléphone, et adresses e-mail de 83 millions de clients, annonce JP Morgan dans un document transmis à la SEC, le gendarme américain de la bourse.

La banque ajoute qu'il n'y a « pas de preuve » que des données sensibles comme les numéros de comptes, mots de passe, identifiants, dates de naissance ou numéros de sécurité sociale aient été compromises. Les responsables de l'attaque n'auraient pas eu accès à ce type de données sensibles, pense Patricia Wexler, porte-parole de JP Morgan. Il ne serait donc pas nécessaire que les clients changent leurs mots de passe.

Pour le moment, la banque n'aurait pas constaté de fraude relative à cet incident.
Mais l'attaque, très sophistiquée, aurait tout de même permis aux pirates d'accéder « au plus haut niveau des droits administrateurs » selon le New York Times qui s'appuie sur des sources proches du dossier. Puis, les informations exposées restent potentiellement utiles aux cyber criminels : « ils pourraient littéralement utiliser l'identité de ces 83 millions de personnes et entreprises », affirme Tal Klein, de la société de sécurité informatique Adallom, à l'agence Reuters.
La banque avait annoncé en août qu'elle enquêtait avec les autorités sur une attaque informatique. Le FBI soupçonnait des pirates russes en raison de la crise ukrainienne et des sanctions économiques à l'encontre du régime de Moscou. Le New York Times affirmait que JP Morgan n'était pas la seule banque concernée mais qu'en tout, cinq banques auraient été visées le même mois.

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Source :
http://pro.clubic.com/it-business/securite-et-donnees/actualite-730905-clients-jp-morgan-pirates.html

Home Depot : finalement 56 millions de cartes bancaires piratées

Home Depot : finalement 56 millions de cartes bancaires piratées

Début septembre, l'enseignement américaine Home Depot révélait avoir observé une activité inhabituelle concernant les données de paiement de ses clients avant de reconnaître une intrusion informatique.

Home Depot expliquait ainsi que tout client ayant utilisé, depuis le mois d'avril, une carte bancaire pour régler un achat dans l'un de ses magasins aux Etats-Unis et au Canada est potentiellement concerné par le vol de ces données de paiement.
Le groupe ne chiffrait pas le nombre de clients affectés ni le détail exact des données personnelles compromises. Le New York Times évoquait le nombre de 60 millions de cartes de paiement compromises.

EMV
Bingo, Home Depot indique aujourd'hui que ce sont 56 millions de cartes bancaires ont été « mises en péril ». De quoi constituer un nouveau triste record en la matière, jusqu'ici détenu par Target (40 millions de cartes de paiement compromises).
D'ailleurs, comme pour Target, il semble que les pirates aient exploité une variante du programme malveillant BlackPOS installé dans le système de paiement de l'entreprise.
Seule bonne nouvelle, Home Depot estime qu'à ce stade de l'enquête aucune preuve ne permet d'établir que les codes PIN des cartes bancaires compromises figurent également parmi les données dérobées. Mais cette protection est assez peu utilisée aux Etats-Unis…
A la suite de cette intrusion informatique, dont l'ampleur doit encore être précisée, Home Depot a fait savoir qu'il déploierait sur l'ensemble de ses magasins, d'ici à octobre 2015, la technologie EMV de paiement pour cartes à puce. Ce standard international, en vigueur notamment en France, apporte en principe une sécurité accrue des transactions et contribue donc à réduire la fraude.

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Source :
http://www.zdnet.fr/actualites/home-depot-finalement-56-millions-de-cartes-bancaires-piratees-39806615.htm

---

Le site internet de la région

PACA victime d’un piratage

Le site internet de la région PACA victime d’un piratage

Le site internet de la Région Provence-Alpes-Côte d’Azur (http://www.regionpaca.fr) a été victime d’un piratage informatique le mercredi 10 septembre. Après avoir été mis hors-ligne, le site est à nouveau accessible.

Les internautes ont vu s’afficher sur leur écran une page sans aucun lien avec l’Institution régionale. Le site a été rapidement mis hors ligne afin de stopper la diffusion de cette page. Les services de la Région procèdent actuellement aux analyses techniques afin de déterminer les conditions de cette attaque et travaillent au rétablissement de l’accès au site institutionnel.
La Région a également saisi la division cybercriminalité de la Police judiciaire et informé l’Agence Nationale pour la Sécurité des Systèmes d’Information. L’Institution entend porter plainte afin qu’une enquête soit menée et que des poursuites soient engagées à l’encontre des auteurs de ce piratage.

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Source :
http://www.nicematin.com/derniere-minute/le-site-internet-de-la-region-paca-victime-dun-piratage.1899236.html

---

Soyez vigilants: Usurpation d’identité, « Escroquerie au Président » ou « Escroquerie au dirigeant » ça n’arrive

pas qu’aux autres…

« Escroquerie au dirigeant » ou « Escroquerie au Président » ça n’arrive pas qu’aux autres…

Il me semblait important de vous informer d'un type d'utilisation des données personnelles que l'on vole aux opérateurs, entreprises, particuliers…Méthode redoutable basée sur l'usurpation d'identité, aucun système de sécurité informatique ne peut l'empêcher
Denis JACOPINI
L'Escroquerie au Président : faux dirigeants et véritable escroquerie !
L'imagination humaine étant rarement à court d'idée ; une vague d'escroqueries est en recrudescence ces derniers temps : l'« Escroquerie au Président ».

Media Participations : 987000 euros (tentative)
Areva, Scor, Quick, Nestle, CMA CGM, Michelin : Montant inconnus (Tentatives)
Elysée : 2 millions d'euros (tentative)
Valrhona : 400000 euros (tentative)
Le groupe Terrena : 489 872 euros puis 3,4 millions d'euros (tentative)
Brittany Ferries : 1 million d'euros (réussite)
Vinci : Montant non divulgué (réussite)
Robertet, l'un des leaders mondiaux des parfums implanté à Grasse : 900000 euros (réussite)
Société spécialisée dans l'optique dans le Pas-de-Calais : 497 000 euros (réussite) et 800 000 euros gelé au dernier moment par la police…
Michel (le transporteur) : 7000 euros (réussite)
KPMG : 7,6 millions d'euros (réussite)
Pour arriver à leurs fins, les aigrefins ont recours à des méthodes très pointues. Dans l'arnaque aux faux virements, ils commencent par mener une enquête fouillée sur leurs cibles. « Pendant un mois, une équipe se renseigne sur la société et ses filiales à l'étranger, témoigne Bernard Petit, sous-directeur à la lutte contre la criminalité organisée, l'un des pontes de la police. Elle collecte les PV d'assemblées générales et de conseils d'administration, et s'imprègne de la culture maison en étudiant les messages des dirigeants aux salariés ou les newsletters internes aux directeurs. » Les filous vont même jusqu'à enquêter sur la vie privée des cadres de l'entreprise. « Grâce aux réseaux sociaux, Facebook ou Twitter, ils peuvent savoir le prénom des enfants ou la date d'anniversaire de la secrétaire », relève Michèle Bruno, chef de la brigade de répression de la délinquance astucieuse.

En quelques années, les as de "l'escroquerie au Président", comme l'appellent maintenant les spécialistes, ont prélevé environ 100 millions d'euros aux sociétés françaises et à leurs banques, selon le commissaire Souvira, patron de l'Office central de lutte contre la grande délinquance financière (OCLGDF) en Janvier 2013. « Jusqu'à deux tentatives par jour enregistrées dans les grands groupes français et pas moins de 700 faits ou tentatives recensés entre 2010 et 2014.=
.Mi 2014, 250 millions d'euros ont été extorqués par ce biais aux entreprises françaises depuis 2010.

Ce type de filouterie bénéficie d'un mode opératoire très simple :
– Le fraudeur contacte, par téléphone ou par écrit, les services comptables de la société cible en se faisant passer pour son Président. Ces prises de contact ont fréquemment lieu en période de vacances, lorsque les dirigeants sont absents.
– Il invoque alors une opération confidentielle en cours (facture urgente à régler, acquisition, contrôle fiscal…) nécessitant un virement conséquent et urgent à destination d'un pays étranger.
– Devant l'urgence de la situation, la force de persuasion de l'interlocuteur (imitation de la voix, connaissance de l'organigramme de l'entreprise…) et l'intimidation dont il fait preuve (menace de licenciement) le comptable sollicité s'exécute.
Les opérations demandées sont généralement réalisés en dehors du processus habituel via une procédure de virement manuel, en raison de leur sécurisation moindre. Les sommes en jeu peuvent être considérables : entre 100.000 euros et plusieurs millions d'euros.

Afin de vous prémunir contre ce type d'escroquerie, plusieurs actions sont à réaliser en amont :
– Informer vos salariés de ces manœuvres et mettre en place un processus de sécurisation ;
– Rappeler aux services comptables et financiers de s'en tenir strictement aux procédures habituelles appliquées en matière de paiement et de signaler à la DAF toute demande inhabituelle ;
– Ré-examiner les procédures de virements manuels pour s'assurer qu'elles sont correctement sécurisées, notamment prévoir un double contrôle pour tout virement important ;
– Examiner la sécurité des accès au système d'information de l'entreprise pour vérifier son intégrité et rappeler aux salariés l'importance de ne pas livrer sur les réseaux sociaux des informations qui pourraient être utilisées aux dépens de l'entreprise…. Tels que les données personnelles des dirigeants, leurs coordonnées, leur planning, tout acte présentant la signature d'un membre de la direction, le cachet de l'entreprise …

Si vous êtes victime d'une telle escroquerie, en premier lieu :
– Portez plainte dans les plus brefs délais, même si l'escroquerie a été déjouée ! Souvent cette démarche est accompagnée d'une usurpation de l'identité du Président ou de membres de la direction ;
– Prenez contact avec un avocat spécialisé pour vous aider à mettre en place la stratégie nécessaire à la défense des intérêts de votre société mais également des intérêts des personnes physiques dont l'identité aura été usurpée.

Ce type d'escroquerie se démultiplie ces derniers temps, nous accompagnons nombre de nos clients qui sont victimes de tentative de cette nature depuis ces 24 derniers mois : Les modes opératoires de ce type de fraude varient et continueront à se perfectionner.

Il faut rester vigilant et surtout réagir très vite lorsque vous avez connaissance d'une telle fraude ou tentative de fraude.
Claudia WEBER, Avocat Associée, et Arthur DUCHESNE, Elève Avocat

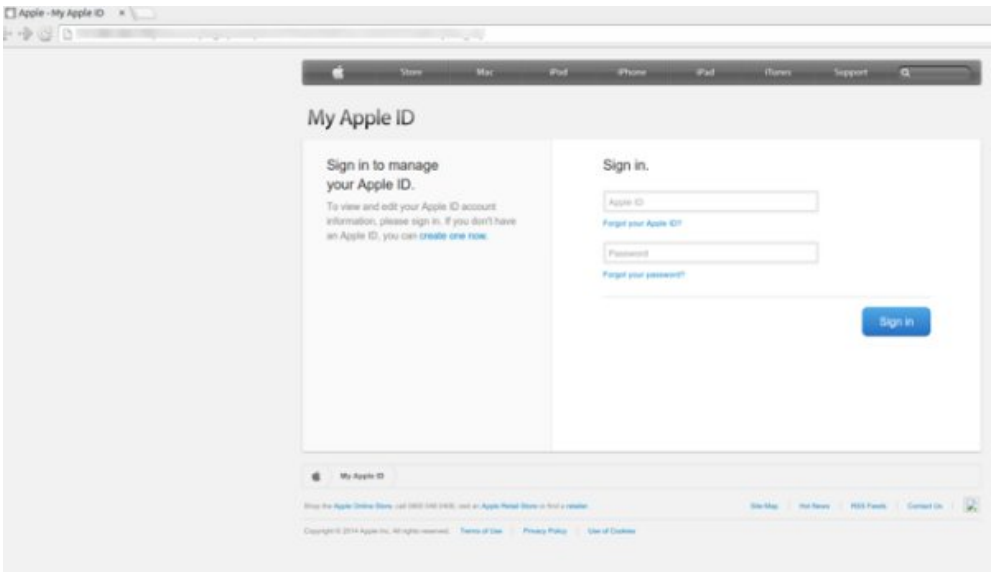
---

Au travers de conférences ou de formations, Denis JACOPINI sensibilise des directeurs, des cadres et des salariés aux risques induits par les nouveaux usages de l'informatique en entreprise et dans les collectivités, ainsi que leurs responsabilités pénales.
Contactez-nous

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Source :
http://www.itlaw.fr/fr/index.php/articles/287-l-escroquerie-au-president-faux-dirigeants-et-veritables-escroqueries
http://www.challenges.fr/entreprise/20120516.CHA6506/menace-sur-le-cac-40-les-nouveaux-escrocs-pechent-au-gros.html
http://business.lesechos.fr/directions-generales/partenaire/attention-a-l-escroquerie-au-president-4416.php
http://www.egaliteetreconciliation.fr/Alerte-sur-une-gigantesque-arnaque-israelienne-aux-faux-virements-26662.html

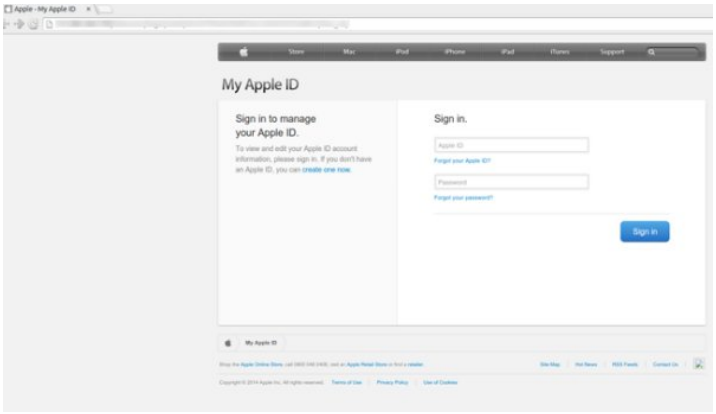
Alerte iCloud : une campagne de phishing tente de dérober des Apple ID



Alerte iCloud : une campagne de phishing tente de dérober des Apple ID

Le hack des photos de célébrités nues a-t-il donné des idées à des pirates ? Symantec signale en tout cas le lancement d'une campagne de phishing visant à dérober identifiants Apple et mots de passe.

Comme en politique, un évènement chasse l'autre. Une bonne chose pour Apple qui, grâce au lancement imminent de l'iPhone 6, a visiblement réussi à faire oublier la fuite sur Internet des photos de nombreuses vedettes américaines et les faiblesses de la sécurité de son service iCloud.
Souvent opportunistes, les cybercriminels voient au contraire dans cette récente actualité une bonne occasion de parvenir à leurs fins. Symantec signale ainsi le lancement d'une campagne de phishing visant justement à moissonner Apple ID et mots de passe auprès des utilisateurs d'Apple.



Attention, achat illicite sur votre compte ! Cliquez, vite !
La recette reste invariablement la même : des emails sont envoyés aux internautes et se présentent comme légitimes, ici envoyés par Apple. Le destinataire est ainsi informé d'un risque de compromission de son compte, un achat ayant été réalisé par son intermédiaire, depuis une IP en Russie.
Sans plus de surprise, l'internaute est prié de se rendre sur un site, reproduction d'un formulaire d'authentification d'Apple, afin de se connecter à son compte en saisissant pour cela son identifiant ainsi que son mot de passe. L'utilisateur abusé transmettra alors ses données d'accès aux pirates.

Et c'est peut-être notamment par le biais de mail de phishing que certaines des célébrités, utilisatrices d'iCloud, ont pu être abusées récemment et des photos intimes dérobées. Car selon Apple, ces informations ont été obtenues seulement par l'intermédiaire d'attaques ciblées et non grâce à une intrusion dans ses serveurs.

Néanmoins, dans une interview, Tim Cook s'est engagé à renforcer la sécurité de son service en ligne : authentification à deux facteurs, alerte mail lors de tentatives de modification du mot de passe, de la restauration des données iCloud sur de nouveaux terminaux ou de l'authentification depuis un terminal Apple encore non-enregistré.

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Source :
http://www.zdnet.fr/actualites/icloud-une-campagne-de-phishing-tente-de-derober-des-apple-id-39806035.htm

---

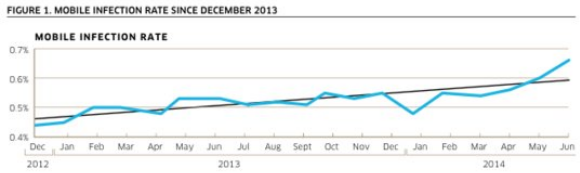
15 millions de terminaux

mobiles seraient infectés d’un malware

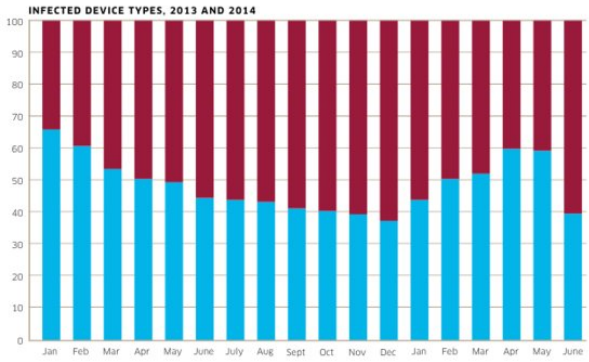
	15 millions de terminaux mobiles seraient infectés d’un malware

Le nombre de terminaux infectés d'un malware continue d'augmenter et l'on estime désormais que 15 millions d'entre eux sont actuellement en circulation, la plupart étant équipés d'Android.

Le cabinet Kindsight Security Labs du groupe Alcatel Lucent, a publié son rapport semestriel sur la sécurité des terminaux mobiles (smartphones et PC portables). Parmi les principaux malwares identifiés, le nombre de spywares augmenterait, certains allant jusqu'à récupérer des informations personnelles. D'autres effectuent des appels ou envoient des SMS vers des numéros surtaxés.



D'après les analystes entre janvier et juin 2014, le nombre d'infections touchant les terminaux mobiles a progressé de 17%. A titre de comparaison, sur l'année 2013 complète ce chiffre était de 20%. Sur l'ensemble des appareils en circulation l'on estime que 0,65% d'entre eux sont infectés d'un malware, soit 15 millions d'appareils à travers le monde.
Les smartphones équipés d'Android comptent 60% des équipements mobiles infectés contre 40% pour les PC portables équipés de Windows. De leur côté, les iPhone, les BlackBerry, les téléphones sous Symbian et sous Windows Phone totaliseraient moins de 1%.



Rouge: Android – Bleu : Windows

Le cheval de Troie Android.Trojan.Coogos.A!tr représenterait 35,69% des attaques ciblant Android. Ce dernier vérifie si le smartphone de la victime est rooté et télécharge automatiquement un fichier. Ce malware récupère en outre les numéros IMEI et IMSI pour les envoyer vers un serveur en Chine. A ses débuts Coogos.A!tr se présentait sous la forme d'un fond d'écran dynamique à installer. ll est aujourd'hui distribué au sein d'un jeu.
Retrouvez l'étude dans son intégralité. (PDF)

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Source
: http://pro.clubic.com/it-business/securite-et-donnees/actualite-725971-etude-15-smartphones-infectes-malware.html