Piratage du site de l'US Army par l'armée électronique syrienne | Le Net Expert Informatique

Piratage du site de l'US Army par l'armée électronique syrienne

L'armée de terre américaine a annoncé lundi avoir temporairement fermé son site internet grand public, après un piratage revendiqué sur Twitter par l'armée électronique syrienne (SEA). Cette dernière soutient le président Bachar al-Assad.

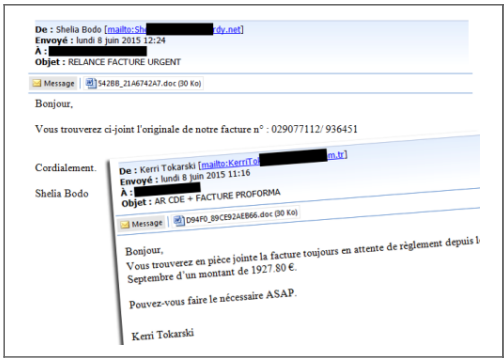
Après avoir constaté qu'un contenu de son site avait été « compromis », l'armée de terre « a pris les mesures préventives appropriées pour s'assurer qu'il n'y avait pas de vol de données de l'armée, en fermant son site internet temporairement », a-t-elle déclaré dans un communiqué de presse. Le site (www.army.mil) n'était toujours pas accessible à 21h30 GMT (23h30 suisses) lundi.
L'attaque a été revendiquée par un compte Twitter s'identifiant comme un compte de l'Armée électronique syrienne. Cette dernière soutient le président Bachar al-Assad et a déjà mené des attaques contre les sites internet de presse dans le monde entier, dont ceux du New York Times ou du Washington Post.
Le compte Twitter du service photo de l'AFP et les réseaux sociaux de la BBC, d'Al Jazeera, du Financial Times ou du Guardian en ont aussi fait les frais.

Message confus
Selon ce compte, @official_SEA16, les pirates avaient notamment laissé sur le site de l'US Army un message en anglais alambiqué dénonçant apparemment le programme de formation de rebelles syriens modérés par le gouvernement américain. « Vos responsables admettent qu'ils entraînent ceux contre qui ils vous envoient mourir au combat », littéralement, selon ce message.
En janvier, les comptes Twitter et YouTube du commandement de l'armée américaine au Moyen-Orient avait déjà été temporairement fermés, après avoir été piratés par des messages faisant la promotion du groupe Etat islamique. Les responsables militaires américains avaient qualifié ce piratage de « cybervandalisme », répétant qu'aucune donnée sensible n'avait été touchée.

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : http://www.bluewin.ch/fr/infos/international/2015/6/9/piratage-du-site-de-l-us-army-par-l-armee-electron.html

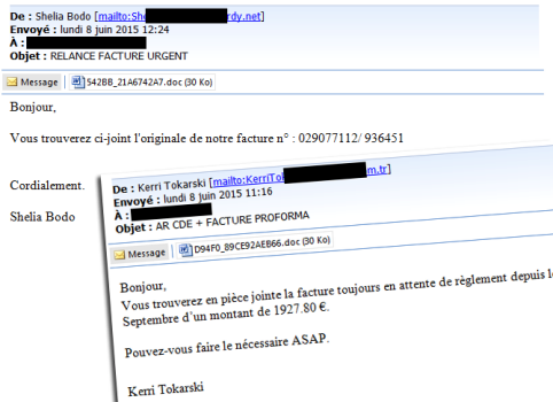
Alerte au Malware caché dans une pièce jointe Microsoft Office – Relayez l'info ! | Le Net Expert Informatique



Alerte au Malware caché dans une pièce jointe Microsoft Office – Relayez l'info !

En ce début de semaine, de nombreuses entreprises ont reçu un e-mail alarmant les informant qu'une facture impayée était à régler rapidement. Attention ! Le document Microsoft Office en pièce jointe dissimule un code d'attaque.

Vous trouverez ci-joint l'originale de notre facture », « vous trouverez en pièce jointe la facture toujours en attente de règlement », « un montant de 1927,80€ », etc.
Les e-mails, écrits dans un français très correct, sans faute d'orthographe, se ressemblent tous et contiennent un document Microsoft Word en pièce jointe. La notion d'urgence dans le ton employé incite à l'ouverture du document.
Une fois exécuté, le document Word téléchargera via un script en Visual Basic un code malveillant-relai Drixed.



Sa présence en mémoire compromet la sécurité du poste et de ses transactions, celui-ci pourra en effet évoluer de diverses manières : trojan bancaire, logiciel espion ou encore un cryptoware.
Vous l'aurez compris, il ne faut surtout pas ouvrir la pièce jointe de cet e-mail, même s'il semble en tout point réaliste. Le fait que vous ne connaissez pas l'expéditeur devrait suffire à vous mettre en garde.
En cas d'ouverture, n'éteignez pas votre ordinateur, déconnectez-le d'Internet et appelez votre département informatique.
Bitdefender détecte le malware en tant que Trojan.Downloader.Drixed.C.

Source : http://www.globalsecuritymag.fr/Le-trojan-Drixed-revient-en-force,20150609,53337.html

Les Etats-Unis victimes d’une nouvelle cyber-attaque | Le Net Expert Informatique

Les Etats-Unis victimes d’une nouvelle cyber-attaque

Des pirates chinois seraient à l’origine d’une nouvelle cyber-attaque visant les données de fonctionnaires américains © Reuters/Pichi Chuang

Les données de millions de fonctionnaires américains ont été piratées ces derniers mois, aux Etats-Unis. Des cyber-pirates chinois seraient à l’origine de l’attaque, ils ont réussi selon des officiels américains à s’introduire dans les serveurs de l’Office of Personal Management, qui stocke notamment les profils des employés fédéraux.
Une nouvelle cyber-attaque d’envergure aux Etats-Unis. Les données personnelles de fonctionnaires ont été piratées depuis décembre 2014. Des hackers, apparement chinois, ont réussi à s’introduire dans les serveurs de l’Office of Personal Management (OPM), une agence qui vérifie notamment les profils des employés fédéraux pour le compte de la sécurité nationale.

4 millions de victimes, peut-être plus
Pas moins de quatre millions d’agents fédéraux, en activité ou à la retraite, ont été victimes de cette cyber-attaque. Ils vont devoir s’assurer auprès de leur banque que leurs données privées n’ont pas été utilisés par les pirates. D’autres éléments, comme les numéros de sécurité sociale et autres identifiants personnels sont également tombées aux mains des hackers.
Dans son communiqué, l’OPM n’exclut pas que d’autres personnes aient pu être victimes de cette attaque en ligne, menée au moment même où l’agence se dotait d’un nouveau système de sécurité. Vol de données ou espionnage, l’objectif des pirates reste en revanche incertain.
Le FBI, qui enquête sur l’affaire, dit « prendre au sérieux toutes les attaques potentielles contre les systèmes du secteur public et privé ».

Vulnérabilité du réseau informatique américain
L’attaque a été découverte en avril, mais la pêche aux informations aurait débuté dès la fin 2014. Une affaire de plus qui confirme la vulnérabilité du réseau informatique de l’administration américaine, fragilité dénoncée par le Government Accountability Office (GAO), l’équivalent de la Cour des comptes française.
Il y a quelques jours encore, on apprenait qu’une cybermafia avait réussi à récupérer les déclarations fiscales de plus de 100.000 contribuables. L’an dernier, le Département d’Etat et la Maison Blanche faisaient les frais d’intrusions attribuées à des Russes. A l’époque les courriels du président Barack Obama avaient été compromis.

Source : http://www.franceinfo.fr/vie-quotidienne/high-tech/article/les-etats-unis-victimes-d-une-nouvelle-cyber-attaque-des-hackers-chinois-soupconnes-688588
par Arnaud Racapé

Alerte : Des millions de routeurs domestiques peuvent être attaqués à distance | Le Net Expert Informatique

Une faille dans le driver NetUSB permet à un pirate de prendre le contrôle total de l'équipement et d'y installer, par exemple, des malwares. Pour l'instant, seul TP-Link a fourni un correctif.

Netgear, TP-Link, Trendnet, Zyxel… Si vous possédez un routeur domestique de l'une de ces marques, il est probable que vous ayez un problème de sécurité. La plupart de ces routeurs disposent en effet d'une fonctionnalité théoriquement assez pratique, à savoir le partage en réseau d'une connexion USB. Concrètement, vous connectez un équipement en USB sur votre routeur – un disque dur par exemple – et celui-ci devient alors accessible à distance au travers du réseau. Beaucoup de ces routeurs s'appuient pour cela sur un module logiciel nommé « NetUSB », développé par le fournisseur taiwanais KCodes.
Le problème, c'est qu'il existe dans ce module une faille qui permet à une personne mal intentionnée de faire crasher le routeur ou d'y exécuter n'importe quel code. Et donc d'en prendre possession pour, par exemple, y installer des malwares. Cette vulnérabilité a été découverte par les chercheurs en sécurité de la société autrichienne SEC Consult. Elle repose sur une erreur de codage : quand le nom de l'ordinateur qui souhaite se connecter à distance est supérieur à 64 caractères, le module NetUSB génère un dépassement de mémoire tampon et le fait planter. Pire : comme ce module est exécuté au niveau du noyau Linux du routeur, cette faille permet d'accéder au plus haut niveau de privilège. Plutôt pratique pour un pirate.

Exemple de routeur vulnérable.

Attaque par Internet
Certains d'entre vous se diront que ce n'est pas si grave que cela, car il faut déjà pouvoir rentrer dans le réseau domestique pour réaliser cette attaque. Mais cela n'est pas toujours vrai. Les chercheurs de SEC Consult ont trouvé que pour un certain nombre de routeurs, les connexions NetUSB étaient accessibles par Internet, peut-être en raison d'une mauvaise configuration. Par ailleurs, il s'avère que la procédure d'authentification utilisée pour initier une connexion avec NetUSB est totalement inutile : « les clés AES sont statiques et peuvent être trouvées dans le driver », expliquent les chercheurs. En d'autres termes, lorsque le routeur expose sa fonctionnalité NetUSB sur le web, un pirate pourra s'y introduire sans problème.
Une rapide recherche a montré qu'au moins 26 fabricants de routeurs utilisent le logiciel de KCodes dans au moins 92 produits. Ce qui représente certainement plusieurs millions de clients dans le monde. Contacté par les SEC Consult, KCodes n'a fait aucun commentaire. Que faut-il faire pour se protéger ? Seul TP-Link a développé, à ce jour, un correctif qu'il diffusera progressivement dans ses différents modèles. Dans certains équipements, il est possible, par ailleurs, de désactiver le partage de connexion USB. Les clients de Netgear, en revanche, ne pourront rien faire. Le fabricant a indiqué d'emblée ne pas pouvoir produire de patch, et qu'il était impossible de désactiver la fonction de partage. Il ne reste alors qu'une seule solution : la prière.

Source : http://www.01net.com/editorial/655187/des-millions-de-routeurs-domestiques-peuvent-etre-attaques-a-distance/

Réunion de crise de 8 banques à cause d’attaques de hackers | Le Net Expert Informatique

Réunion de crise de 8 banques à cause d’attaques de hackers

De nos jours les attaques par des hackers font partie du quotidien. Souvent on reçoit des mails par des expéditeurs inconnus qui ont pour but de parvenir aux données personnelles des clients. Les banques sont souvent ciblées lors de tels envois: le système « multiline » offert par 8 banques du Grand-Duché est actuellement dans la ligne de mire.

Attention! N'ouvrez aucun fichier ou document émis par l'adresse email suivante: helpdesk@multiline.lu !
Ceci est un message obtenu directement lorsque qu'on se rend sur le site Multiline.

Multiline est un service dit « e-banking » pour professionnels et entreprises (pour leur gestion financière) proposé depuis 1992.
Bien que ce système paraisse assez sécurisé (collaboration avec Luxtrut et Cetrel) il a quand même fait l'objet de cyberattaques.
Les dégâts ont été tels que 8 banques utilisant ce système (BCEE, Banque de Luxembourg, Raiffeisen, BIL, Poste, BGL BNP Paribas, ING et Société Générale) se sont réunies en cellule de crise.
Il n'y a pas encore d'informations disponibles émanant de l'ABBL, de la Cetrel ou de Multiline.
Le situation serait sous contrôle, un communiqué officiel est attendu pour le mardi de pentecôte.

Source : http://5minutes.rtl.lu/fr/actualite/alaune/634917.html

Le Bundestag se montre incapable de surmonter une cyber-attaque | Le Net Expert Informatique

Le Bundestag se montre incapable de surmonter une cyber-attaque

Depuis quelques semaines le parlement allemand est victime d'attaques informatiques à répétition. Un phénomène qui inquiéte certains députés.

Le Bundestag est vulnérable. Depuis le début du mois de mai, les services informatiques du parlement allemand sont la cible de cyber-attaques répétées. Les députés ne sont plus en mesure de sécuriser leurs communications. Des données ont été piratées, sans qu'il soit possible d'en connaître la nature. Impossible pour l'heure de savoir si des documents confidentiels ont été volés. «Et ce n'est pas terminé», a déclaré un porte-parole, selon des propos rapportés par les médias allemands, comme Der Spiegel ou Die Zeit, qui ont notamment révélé l'affaire. Le «cheval de Troie» utilisé par les hackers n'a pas encore été neutralisé. Selon le quotidienSüddeutsche Zeitung, le BSI, chargé de la sécurité fédérale informatique, aurait même demandé une aide extérieure pour en venir à bout.
L'exaspération et l'inquiétude commencent à se répandre au Bundestag, principalement dans les rangs de l'opposition. Les députés Verts et Die Linke semblent davantage touchés par l'attaque. Mais la cible exacte des hackers reste encore inconnue. «L'incertitude demeure sur l'intensité de l'attaque et son ampleur», a expliqué le député Vert Konstantin von Notz, spécialiste des questions informatiques. «Il n'y avait encore jamais une telle attaque pendant plusieurs jours», a déploré la vice-présidente Petra Pau (Die linke). «Il y a une attente évidente pour que la protection des communications soient rétablies», a observé le responsable SPD Lars Klingbeil. Le Bundestag envisage la possibilité de devoir réinstaller totalement l'infrastructure du réseau, pour purger la menace. Toute l'activité informatique du Bundestag en serait interrompue. L'opération pourrait avoir lieu au moment des vacances parlementaires, en juillet.

20 tentatives d'intrusion par jour en 2014
Qui se cache derrière l'assaut? Pour l'instant, la seule piste connue mène vers Europe de l'Est, où sont situés des serveurs qui auraient infiltré au moins deux ordinateurs du Bundestag. Mais l'enquête de la Sécurité intérieure est toujours en cours. Toutefois, à écouter les experts, la complexité de l'attaque témoigne d'une capacité technologique dont seuls des services secrets peuvent disposer.
Il ne s'agit pas de la première attaque informatique dont est victime l'administration allemande, loin de là. Selon le BSI, les services internes du gouvernement auraient subi en moyenne 20 tentatives d'intrusion par jour l'année dernière. Des services de renseignement étrangers seraient à l'origine d'au moins une attaque quotidienne. Pour renforcer la sécurité informatique de l'Allemagne et notamment de ses entreprises, le gouvernement élabore un nouveau projet de loi. «Avec cette loi, une amélioration significative de la sécurité des communications informatiques devra être atteinte», promet le texte en préparation. Le Bundestag sera amené à en débattre.

Source : http://www.lefigaro.fr/international/2015/05/22/01003-20150522ARTFIG00173-le-bundestag-se-montre-incapable-de-surmonter-une-cyber-attaque.php

---

Alerte: Nouveaux courriels de phishing au nom d'Apple

(iTunes) | Le Net Expert Informatique

Des fraudeurs envoient des courriels au nom d'Apple (iTunes) afin de s'emparer des données d'accès à votre compte.
Par ces courriels, les destinataires sont informés que leur compte n'a pas pu être validé et que celui-ci a été bloqué. Les escrocs demandent de suivre un lien et de fournir des données personnelles (nom d'utilisateur et mot de passe) sous prétexte de pouvoir réactiver leur compte.

Le SCOCI conseille :
1. Effacez le courriel !
2. Si vous soupçonnez quelqu'un d'être en possession de vos données d'accès à votre compte, veuillez immédiatement prendre contact avec le support d'Apple.
3. Soyez prudents avec tous les courriels qui vous demandent de cliquer sur un lien Internet pour contrôler vos données personnelles. En règle générale, ceci est l'œuvre de fraudeurs.
4. Contrôlez toujours l'adresse Internet (URL) sur laquelle vous êtes redirigés (cf. rectangle rouge sur l'image). De manière générale, si vous devez vous connecter à un compte en ligne, inscrivez l'URL vous même dans votre navigateur plutôt que de cliquer sur un lien qui vous est transmis par courriel.
5. Signalez ces cas au SCOCI par le biais de son formulaire d'annonce en ligne afin que nous puissions analyser ces courriels et faire fermer au plus vite les sites frauduleux.

En cas de doute sur une usurpation d'identité ou de doute sur une arnaque, n'hésitez pas à contacter Denis JACOPINI expert informatique assermenté.

Source : https://www.cybercrime.admin.ch/kobik/fr/home/warnmeldungen/2015/2015-05-15.html

---

Des pirates informatiques

volent 5 millions de dollars à Ryanair | Le Net Expert Informatique

Des pirates informatiques volent 5 millions de dollars à Ryanair

Un peu moins de 5 millions de dollars (4,5 millions d'euros) ont été dérobés d'un des comptes de la compagnie aérienne à bas coûts Ryanair. Selon la société irlandaise, des pirates informatiques se seraient emparés de la somme par « un transfert électronique frauduleux passé via une banque chinoise ».

La compagnie travaille actuellement avec ses établissements bancaires et les autorités compétentes afin de récupérer ces fonds. Elle annonce dans un communiqué, publié mercredi 29 avril, que ceux-ci ont été « bloqués » et que des mesures ont été prises pour sécuriser les comptes de Ryanair. L'identité des pirates est encore inconnue.

Facture de kérosène

La société, dont le siège est à Dublin, assure des liaisons principalement en Europe. La plupart de ses transactions sont effectuées en euros, mais elle dispose aussi de comptes en dollars. D'après The Irish Times, les fonds en dollars ciblés par les pirates informatiques étaient destinés à payer ses factures de kérosène.

Le quotidien ajoute que l'agence judiciaire chargée du dossier en Irlande, le Criminal Assets Bureau (« bureau des biens d'origine criminelle ») de Dublin, avait pu identifier où la somme subtilisée avait été transférée grâce à un système de coopération internationale avec des agences jumelles en Asie.

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure sécurité des systèmes informatiques et améliorer la protection juridique du chef d'entreprise.
Contactez-nous

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.lemonde.fr/pixels/article/2015/04/29/des-pirates-informatiques-volent-5-millions-de-dollars-a-ryanair_4625234_4408996.html#Zc4r8duqZpt2kWJo.99

La Maison Blanche victime d'une cyberattaque « préoccupante » | Le Net Expert Informatique

La Maison Blanche victime d'une cyberattaque « préoccupante »

Des e-mails non classés secrets adressés au président des Etats-Unis, Barack Obama, et envoyés par lui ont été lus l'année dernière par des hackeurs russes qui ont pénétré une partie du système informatique de la Maison Blanche, a affirmé samedi 25 avril le New York Times.

Au début du mois d'avril des responsables américains avaient reconnu qu'il y avait eu un « événement » relatif à la sécurité à la fin de l'année dernière, mais avaient refusé de confirmer les informations selon lesquelles des Russes seraient derrière ces cyberattaques. Selon le quotidien américain, qui cite des responsables ayant été informés de l'enquête sur ces faits, l'attaque a été « beaucoup plus intrusive et préoccupante » que cela n'a été officiellement reconnu. Les personnes cités laissent entendre que les hackeurs étaient liés au pouvoir russe.

« Aucun réseau classé secret atteint »

Les pirates ont réussi à accéder aux archives des e-mails de personnes employées à la Maison Blanche et avec lesquelles M. Obama communiquait régulièrement, écrit le New York Times. C'est dans ces archives que les hackeurs ont pu voir des e-mails que le président avait envoyés et reçus, selon les sources citées par le quotidien. Son compte mail lui-même ne semble pas avoir été piraté. Les hackeurs auraient par ailleurs également pénétré le système non secret du département d'Etat américain.

Les pirates ne semblent en revanche pas avoir pénétré les serveurs qui contrôlent le trafic de messages du BlackBerry de Barack Obama, et la Maison Blanche a assuré qu'aucun réseau classé secret n'avait vu sa sécurité compromise. « Mais des responsables ont reconnu que le système non classé secret contient régulièrement beaucoup d'informations considérées comme hautement sensibles : horaires, échanges d'e-mails avec des ambassadeurs et des diplomates (…) et, inévitablement, débats politiques », écrit le quotidien.

On ignore combien de courriels du président ont été lus par les pirates. « Néanmoins, le fait que les communications de M. Obama étaient parmi celles qui ont été ciblées par les hackeurs – qui sont suspectés d'être liés au pouvoir politique russe, voire de travailler pour lui – a été l'une des conclusions de l'enquête les plus étroitement protégées », selon le New York Times.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.lemonde.fr/ameriques/article/2015/04/26/la-maison-blanche-victime-d-une-cyberattaque-preocucupante_4622869_3222.html

Lufthansa victime d'une cyberattaque | Le Net Expert Informatique

Lufthansa victime d'une cyberattaque

Le site de la compagnie aérienne allemande Lufthansa a été victime d'une attaque informatique, a indiqué vendredi 10 avril l'hebdomadaire Der Spiegel. Des individus ont réussi à se procurer les données personnelles d'utilisateurs du site LH.com.

L'attaque a été menée via un « botnet » (machine zombie), une série de noms d'utilisateurs et de mots de passe ont été automatiquement testés jusqu'à l'aboutissement du méfait, selon Der Spiegel.
Lufthansa a indiqué avoir immédiatement pris les mesures nécessaires, « mais celles-ci n'ont pas pu empêcher l'accès illicite aux données personnelles de certains utilisateurs ».

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source :
http://www.7sur7.be/7s7/fr/4134/Internet/article/detail/2282639/2015/04/10/Lufthansa-victime-d-une-cyberattaque.dhtml