Cyber-attaques, vigilance rouge pour les maires et les administrations

Cyber-attaques, vigilance rouge pour les maires et les administrations

Les cyber-attaques sont aussi une arme utilisée par les terroristes. Les maires et les administrations les craignent à juste titre. Conseils de l'ANSSI.

Dans un entretien publié dans le journal Le Monde du 10 novembre, le directeur de l'ANSSI (Agence nationale de sécurité des systèmes d'information) alerte sur une autre facette du terrorisme, les cyber-attaques.
Cela inquiète d'ailleurs de nombreux maires ruraux et les administrations qui ont encore en mémoire la cyber-attaque contre TV5 Monde, ce début d'année et les nombreux « défaçage » de sites administratifs. Celui-ci consiste à remplacer leurs pages d'accueil par des slogans faisant l'apologie du terrorisme ou en les sabotant.

D'où les conseils suivants de l'ANSSI :
1.- contacter le prestataire informatique qui a réalisé le site web ou l'hébergeur du site,
2.- vérifiez avec eux que toutes les mises à jour ont bien été réalisées surtout celles des pare-feux,
3.- créer des copies de sauvegarde des fichiers corrompus afin de les remettre aux enquêteurs,
4.- porter plainte auprès de la police ou de la gendarmerie puisque ces actes peuvent tomber sous le coup de la circulaire 2015/0213/A13 du 12 janvier 2015 du ministère de la justice (voir lien ci-dessous)

Pour se prémunir et éviter que cela se produise, l'ANSSI conseille :
1.- utiliser des mots de passe robustes d'au moins 12 caractères alternant majuscules, minuscules, chiffres et symboles,
2.- éviter un même mot de passe pour des accès différents,
3.- ne pas configurer les logiciels pour qu'ils retiennent les mots de passe,
4.- faire les mises à jour depuis le poste informatique, en aucun cas à distance depuis un ordinateur extérieur, une tablette ou un Smartphone,
5.- mettre à jour tous les logiciels afin de corriger les failles,
6.- réaliser une surveillance du compte ou des publications en prévoyant des sauvegardes. Attention aux courriels et leurs pièces jointes- toujours vérifier la cohérence entre l'expéditeur et le contenu du message,- ne pas ouvrir les pièces jointes provenant de destinataires inconnus ou douteux,- passer la souris sur les liens avant de cliquer afin que l'adresse complète s'affiche,- ne jamais répondre par courriel à une demande d'informations personnelles ou confidentielles.

Bien évidemment, ces mesures ne font pas écran total contre les cyber-attaque mais permettent quand même un minimum de prévention.
Elles permettent aussi aux maires (responsables de l'état-civil par exemple) et aux administrations qui détiennent de nombreux fichiers de clients et les comptes bancaires de se « couvrir » pour garantir la sécurité des données à caractère personnel que contiennent leurs sites Internet.

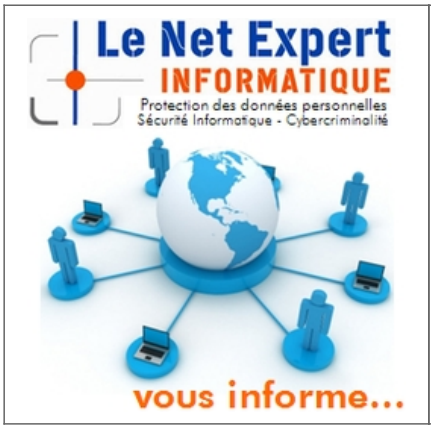
Liens :
– site de l'ANSSI :
http://www.ssi.gouv.fr

– circulaire du ministère de la justice :
http://www.justice.gouv.fr/publication/circ_20150113_infractions_commises_suite_attentats201510002055.pdf
– signaler : www.internet-signalement.gouv.frwww.signal-spam.fr

---

Source : http://www.humanite.fr/cyber-attaques-vigilance-rouge-pour-les-maires-et-les-administrations-589915

Des injection MySQL pour générer des attaques DDOS | Le Net Expert Informatique



Des injection MySQL pour générer des attaques DDOS

MySQL transformé en plate-forme DDoS. Des hackers utilisent des techniques d'injection SQL pour infecter la base de données MySQL et la transformer en plate-forme d'attaques par déni de service.

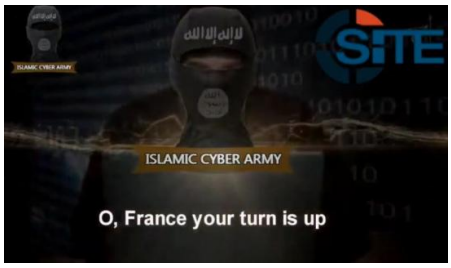
Selon l'éditeur Symantec, qui détaille l'attaque dans un billet de blog, les pirates s'appuient sur un malware appelé Chikdos, qui possède des variantes pour Windows et Linux. Connue depuis 2013, cette souche infectieuse serait ici mise en place via l'injection de code UDF (user-defined function), une fonction de MySQL servant à en étendre les capacités. Pour les pirates, cibler des serveurs MySQL plutôt que des PC lambda leur permet d'accéder à des bandes passantes bien plus larges, renforçant la portée des attaques DDoS.

Source :
http://www.silicon.fr/europe-vote-snowden-mysql-ddos-open-source-apple-stonesoft-130344.html

---

Cyberjihadisme : trois sites de ministères français piratés | Le Net Expert

Informatique



Cyberjihadisme : trois sites de ministères français piratés

Après TV5 Monde, les sites gouvernementaux. Les portails web du ministère français de la Défense, des Affaires étrangères, de la Culture, mais aussi les sites du Sénat, de l'Organisation de l'aviation civile internationale et de la préfecture maritime de la Manche ont été piratés vendredi.

Les attaques ont été revendiquées dimanche soir, captures d'écran et données personnelles à l'appui, par un groupe intitulé «The Islamic Cyber Army» («Hackers de l'État islamique», NDLR). Ce sont ces mêmes pirates qui avaient revendiqué l'attaque de la chaîne de télévision francophone en avril dernier.
Des listes de noms d'agents publics, leurs coordonnées ou encore leurs adresses mails ont été dévoilées sur les réseaux sociaux tout le long du week-end. L'attaque, qui a commencé vendredi, a été confirmée au Figaro.fr par une source gouvernementale. Selon cette source, «à ce stade aucun serveur des trois ministères n'a été compromis et il n'y a pas eu d'exfiltration de données».

Attaque annoncée

L'opération, baptisée «France under Hacks», avait été repérée dès jeudi dernier par le Centre américain de surveillance des sites djihadistes. Le groupe avait en effet, sur Twitter, menacé «la France» d'un piratage imminent. Le Centre français d'analyse de lutte informatique défensive (Calid), chargé de la cyberdéfense auprès du ministère de la Défense, et l'Agence nationale de la sécurité des systèmes d'information (Anssi) sont toujours en train d'étudier les données volées diffusées sur le web. Il s'agirait d'une attaque bénigne et «plutôt fantaisiste». «Il est très simple de deviner les mails d'un service à partir d'un modèle-type», minimise une source ministérielle.

Source :
http://www.leparisien.fr/faits-divers/cyberjihadisme-trois-sites-de-ministeres-francais-pirates-26-10-2015-5220325.php

Des chercheurs découvrent un navigateur malveillant, il se présente comme une imitation de Chrome afin de tromper les utilisateurs | Le Net Expert Informatique

Des chercheurs découvrent un navigateur malveillant, il se présente comme une imitation de Chrome afin de tromper les utilisateurs

Face à la diversité des outils de détection de malwares, les pirates informatiques n'hésitent pas à faire preuve d'inventivité pour atteindre leurs objectifs. En effet, une société du nom de Claralabsoftware a mis en œuvre un navigateur du nom d'eFast. Ce navigateur est censé améliorer l'expérience de navigation en fournissant des résultats de recherche les plus pertinents, en affichant des réductions et bonnes affaires disponibles sur la toile, et en fournissant des outils de protection contre les phishings et divers malwares. Il est basé sur Chromium, le navigateur open source sur le lequel sont fondés plusieurs autres navigateurs dont Chrome, Opera, Vivaldi, etc.

Les utilisateurs voyant donc les caractéristiques d'eFast pourraient croire à une application dénuée de tout code malveillant, mais tant s'en faut. Selon le rapport de Malwarebytes, l'entreprise de sécurité informatique, lorsque vous installez eFast, ce dernier essaie automatiquement de prendre le contrôle du terminal sur lequel il est installé en cherchant à devenir le navigateur par défaut.

En plus de cette action, eFast s'associe par défaut avec les extensions de fichiers suivantes : gif, htm, html, jpeg, jpg, pdf, png, shtml, webp, xht, xhtml. La même association est effectuée pour les schémas, protocoles, et autres objets URL suivants : ftp, http, https, irc, mailto, mms, news, nntp, sms, smsto, tel, urn, webcal.

Lorsque ces extensions sont associées par défaut à eFast, pour toute tentative d'ouverture de fichier, d'appel d'un protocole ou toute action utilisant les objets listés plus haut, c'est le navigateur eFast qui exécutera l'action souhaitée.

En plus de cela, eFast redirigeraient les internautes vers des pages publicitaires ou d'autres pages web qui pourraient héberger des malwares. En outre, PCrisk rapporte qu'eFast est un aspirateur de données de navigation. Ces informations une fois collectées pourraient être partagées avec d'autres personnes et utilisées à mauvais escient afin de gâcher la vie d'un internaute.

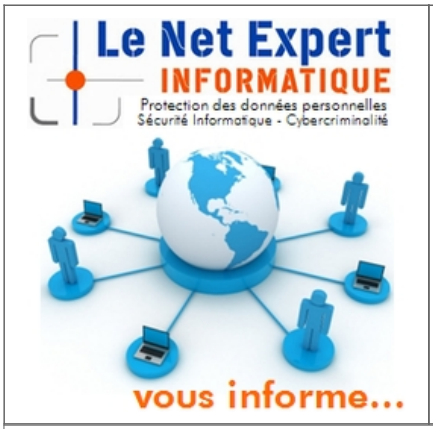
Selon PCrisk, ce programme pourrait s'installer lors de l'installation de certains programmes. En effet, les développeurs pourraient cacher l'option d'installation de ce programme dans les paramètres personnalisés. C'est pourquoi il est recommandé de ne pas installer les applications en utilisant les paramètres de recommandation, mais plutôt les paramètres personnalisés.

Une des choses à ne pas négliger par ailleurs est que lors de l'installation d'eFast, celui-ci se charge de supprimer les raccourcis de Chrome sur le bureau et la barre des tâches et installe par la même occasion des raccourcis de YouTube, Amazon, Facebook, Wikipedia et Hotmail sur le bureau. Il faut noter qu'il est très similaire à Chrome aussi dans la présentation générale que dans les couleurs de l'icône.

Enfin, nous précisons qu'en voulant nous rendre sur le site de l'éditeur clara-labs afin d'effectuer des recherches supplémentaires, Chrome nous a envoyé une alerte afin de signaler que le site que nous voulons ouvrir contient des programmes dangereux. Ce n'est donc pas uniquement le produit de l'entreprise qui est étiqueté comme dangereux, mais même le site l'est également.

Source :
http://www.developpez.com/actu/91354/Des-chercheurs-decouvrent-un-navigateur-malveillant-base-sur-Chromium-il-se-presente-comme-une-imitation-de-Chrome-afin-de-tromper-les-utilisateurs/
par Olivier Famien

Le site Web des universités de Montpellier piraté par un groupe pro-palestinien | Le Net Expert Informatique



Le site Web des universités de Montpellier piraté par un groupe pro-palestinien

L'attaque s'est déroulée pendant quelques heures ce samedi. Des hackers se revendiquant de l'opération « Save Gaza » ont pris en main le site des Universités de Montpellier comme l'a repéré le site H24.Dans un message écrit à la fois en anglais et en français, ils dénoncent l'aide américaine au gouvernement d'Israël, accusé de « contrôler le monde, l'armée, l'économie et les cerveaux ».

« Save Gaza »

Dans un long paragraphe, les auteurs du piratage accusent les deux « gouvernements monsters » d'être « à l'origine de l'hypnose dont souffre la race humaine ». Le texte se conclut sur une adresse aux français: « Si être un vrai « Français », comme vous le dites, c'est d'être soumis, alors personne n'a à le cacher, nous ne sommes pas français, et bien heureux et vous nous considériez différents de vous ».

Le groupe affiche en conclusion son objectif: « The Intruders Will Transform The World », traduit en français par « Les Intruders changeront le monde ».

Source :

http://www.bfmtv.com/societe/le-site-web-des-universites-de-montpellier-pirate-par-un-groupe-pro-palestinien-919637.html

Les sites Web du gouvernement thaïlandais attaqués | Le Net Expert Informatique

Les sites Web du gouvernement thaïlandais attaqués

Plusieurs sites gouvernementaux thaïlandais ont été la cible, dans la nuit de mercredi 30 septembre à jeudi 1er octobre, d'attaques dites de « déni de service », qui les ont rendus inaccessibles pendant plusieurs heures. Ce type d'attaque, appelée DDoS, consiste à multiplier les requêtes inutiles sur un site afin de le saturer. Parmi les sites visés, celui du gouvernement, du ministère de l'information et du ministère de la défense. Certains étaient encore difficiles d'accès jeudi matin.

Ces attaques sont généralement automatisées, mais mercredi, des appels à surcharger ces sites ont été relayés sur les réseaux sociaux, incitant les internautes à s'y connecter et à rafraîchir les pages au maximum. Objectif : dénoncer les projets du gouvernement sur l'avenir d'Internet.

« Grande muraille »

Les Thaïlandais s'inquiètent en effet de la censure grandissante exercée par la junte militaire au pouvoir sur Internet, qui a amplifié sa politique de censure, et multiplié les poursuites contre les internautes ayant émis des critiques sur la famille royale.

L'inquiétude est montée d'un cran la semaine dernière, après l'annonce discrète, sur un site gouvernemental, d'un projet de mise en place d'une gateway (« passerelle ») unique. Une gateway est une sorte de porte d'entrée permettant à un pays de se connecter au réseau mondial. La Thaïlande en possède actuellement une dizaine, gérées par des opérateurs publics ou privés. Se limiter à une seule gateway, opérée par la junte, pourrait faciliter la surveillance et la censure, dénoncent les détracteurs du projet.

Ceux-ci ont réussi à réunir plus de 130 000 signatures sur une pétition en ligne contre ce projet surnommé « Great firewall of Thaïlande », en référence au Great firewall of China, cette « Grande Muraille » de l'Internet érigée en Chine.

Source :

http://www.lemonde.fr/pixels/article/2015/10/01/les-sites-web-du-gouvernement-thailandais-attaques-pour-protester-contre-la-censure_4779521_4408996.html

---

Facebook de nouveau en panne

mondialement, pendant un heure | Programmez! | Le Net Expert Informatique

Facebook de nouveau en panne mondialement, pendant un heure

Facebook connaît de temps en temps une panne mondiale, qui empêche les utilisateurs de se connecter au réseau social. La dernière grande panne mondiale date du début de l'année. A l'époque, les Lizard Quad avaient prétendus avoir lancé une attaque DDoS sur Facebook ce qui avait provoqué le problème. Facebook avait alors démenti l'attaque DDoS, et indiqué que des modifications techniques avaient été responsables du problème, sans plus d'informations.

Hier soir rebelote. Facebook a été en panne mondialement, ou dans nombreuses régions du monde, dont l'Europe, pour être plus précis. Toujours pas d'attaque DDoS des Lizard Squad, mais un problème technique. Facebook a ainsi indiqué que son API Graph a été temporairement indisponible. Ce qui veut tout dire et rien dire. Pas d'API Graph = pas de réseau social certes, mais cela n'explique rien quand au pourquoi. C'est d'ailleurs la ligne de conduite habituelle de Facebook d'être plus que sibyllin dans ce genre de situation.

Que fait-on quand un réseau social est en panne ? On en utilise un autre pour se plaindre du premier C'est ainsi que l'incident a fait les choux gras de Twitter, avec un hashtag #facebookdown qui est monté dans le Top 10 des hashtags Twitter.

Source :
http://www.programmez.com/actualites/facebook-de-nouveau-en-panne-mondialement-pendant-un-heure-23249

Russie: la Commission électorale attaquée par des hackers US | Le Net Expert Informatique

Russie: la Commission électorale attaquée par des hackers US

Le site officiel de la Commission électorale centrale (CEC) de Russie a repoussé une attaque informatique provenant d'une compagnie basée à San Francisco, annoncent les médias russes. Des élections de différent niveau se sont tenues dimanche 13 septembre en Russie.

Piratage massif: sanctions US imminentes contre des compagnies chinoises

La tentative de piratage a été enregistrée samedi soir, selon le chef de la CEC, Vladimir Tchourov. « Quelqu'un a essayé de pirater notre site et de substituer son contenu, avec un intensité de 50.000 requêtes par minute », a-t-il déclaré. Selon lui, cette tentative aurait rapidement été neutralisée.

La CEC a demandé aux organes compétents des Etats-Unis d'identifier et de punir les coupables.

Des élections régionales et locales se sont tenues dimanche 13 septembre en Russie. Près de la moitié des électeurs étaient appelés aux urnes. Les chefs de 24 régions russes, les députés de 11 parlements régionaux et 25 conseils municipaux ont notamment été élus.

Source : http://fr.sputniknews.com/russie/20150914/1016708817.html

Alerte : L'éditeur de Firefox victime d'un piratage | Le Net Expert Informatique

Alerte : L'éditeur de Firefox victime d'un piratage

La Fondation Mozilla, qui édite notamment le navigateur Firefox, a annoncé vendredi 4 septembre qu'elle avait été victime d'un piratage touchant Bugzilla, son outil de notification de bugs. « Quelqu'un est parvenu à voler des informations sensibles touchant à la sécurité [de Firefox]. Nous pensons que ces informations ont été utilisées pour mener des attaques informatiques contre des utilisateurs de Firefox », est-il écrit sur le site de la fondation.

Les informations volées contenaient entre autres des détails sur une vulnérabilité présente dans une précédente version de Firefox, qui a été corrigée le 27 août dans la dernière mise à jour du logiciel.
Mozilla a également annoncé avoir renforcé la sécurité de Bugzilla, et a transmis les informations collectées lors de son enquête interne aux autorités. « L'ouverture, la transparence et la sécurité sont au cœur de notre mission, écrit la fondation. Et c'est pourquoi nous rendons publics les bugs que nous détectons une fois qu'ils ne sont plus dangereux, et que nous le disons publiquement lorsqu'il y a un accès non autorisé à nos infrastructures. »

Denis JACOPINI est Expert Judiciaire en Informatique, consultant, formateur et chargé de cours.
Nos domaines de compétence :
• **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
• **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
• **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.
Contactez-nous

Source :
http://www.lemonde.fr/pixels/article/2015/09/07/l-editeur-de-firefox-victime-d-un-piratage_4747961_4408996.html

---

Les publicités piégées au ransomware se multiplient |

Le Net Expert Informatique

ransomwa

	Les publicités piégées au ransomware se multiplient

Une nouvelle campagne d'infection via des annonces publicitaires falsifiées sévit sur plusieurs sites populaires comme Weather.com ou Drudgereport.com, prévient KnowBe4.

Une nouvelle campagne de « malvertizing » sévit sur Internet. Weather.com, Drudgereport.com, wunderground.com, des sites qui génèrent plusieurs millions de visites mensuelles, en seraient victimes. L'infection serait en train de s'étendre à Ebay.com et AOL.com, indique Stu Sjouwerman, le CEO de KnowBe4, une société spécialisée dans le conseil en sécurité qu'il a créée avec Kevin Mitnick, l'un des hackers les plus médiatiques des années 90. Rappelons que ce dernier avait accédé aux systèmes de grandes entreprises américaines, ce qui lui a valu 5 ans d'emprisonnement en 1995.
Selon KnowBe4 la campagne infectieuse diffuserait des ransomware de type CryptoWall. Une fois installée dans le système, généralement des PC sous Windows, cette bestiole crypte les fichiers locaux. Pour pouvoir les déchiffrer et y accéder de nouveau, ses auteurs réclament une rançon de 500 dollars (montant généralement constaté aujourd'hui), généralement en Bitcoin, à la victime. Un récent rapport de Proopoint estimait que les attaques par CryptoWall généraient jusqu'à 25 000 dollars par jour de revenus pour les pirates. Selon des chercheurs de Dell SecureWorks, plus de 830 000 personnes dans le monde avaient été victimes d'un ransomware fin 2014.

Adspirit.de, le propagateur
Ce ne pas les sites eux-mêmes qui sont infectés, mais la plate-forme de diffusion des annonces publicitaires qui, indirectement, contribue à la propagation infectieuse en distribuant les fichiers publicitaires malveillants. Dans le cas présent, le réseau Adspirit.de serait à l'origine de la contamination. L'entreprise sert en effet d'intermédiaire entre les annonceurs et les sites « afficheurs ». Quand les annonceurs sont des pirates, les choses se compliquent. Les publicités infectieuses ne se distinguant pas en apparence des réclames légitimes, il est facile de tomber dans le panneau. Un simple clic sur ces pubs déclenche le processus d'infection.
Pire : dans de nombreux cas, leur simple affichage suffit à enclencher le mécanisme de contamination par exploitation d'une faille système (particulièrement celle du player Flash, ou encore de Java, d'où l'importance d'appliquer régulièrement ses mises à jour de sécurité) sans aucune intervention de l'utilisateur. Pour s'en prémunir, KnowBe4 préconise d'utiliser le mode « clic-to-play » qui impose une intervention manuelle pour dérouler un contenu publicitaire en Flash, voire de supprimer le plugin d'Adobe de son navigateur. Ou encore d'installer un bloqueur de publicités comme Ad-Blocker, utilisé par 200 millions de personnes dans le monde et honni par la presse en ligne qui l'accuse d'un manque à gagner de 45 millions de dollars rien qu'aux Etats-Unis.
Si KnowBe4 nomme bien Adspirit.de comme étant la source de cette campagne infectieuse dans son communiqué, le nom du diffuseur n'apparaît pas dans le billet de blog de la société de conseils en sécurité. Aucune alerte n'a cependant été émise du côté du réseau allemand. Quelques semaines auparavant, c'est Yahoo qui avait exposé ses visiteurs à une campagne d'attaques par publicités déguisées.

Source : http://www.silicon.fr/nouvelle-vague-publicites-piegees-ransomware-124341.html
Par Christophe Lagane