Alerte : Vulnérabilité zero-day qui affecte des millions de systèmes Linux et Android

Alerte : Vulnérabilité zero-day affecte des millions de systèmes Linux et Android

Le fournisseur en sécurité Perception Point a découvert une vulnérabilité zero-day présente dans le code source de Linux depuis 2012. Touchant des dizaines de millions de postes de travail et serveurs Linux 3 et 64-bit, mais également tous les terminaux Android 4.4 ou supérieurs, cette vulnérabilité sera corrigée sous peu.

Une nouvelle vulnérabilité zero-day a été découverte permettant à des applications Android ou Linux d'escalader des privilèges et d'avoir un accès root, d'après un rapport publié ce matin par le fournisseur de solutions de sécurité Perception Point. « Elle affecte tous les téléphones Android sous KitKat (4.4) ou supérieurs », a fait savoir Yevgeny Pats, co-fondateur et CEO de Perception Point.

Toutes les machines dotées d'un noyau Linux 3.8 (ou supérieur) sont vulnérables, incluant des dizaines de millions de PC et serveurs Linux, aussi bien 32 que 64 bits. En tirant parti de cette vulnérabilité, des attaquants sont en mesure de supprimer des fichiers, accéder à des informations personnelles, et installer divers programmes.

Des correctifs disponibles via des mises à jour automatiques

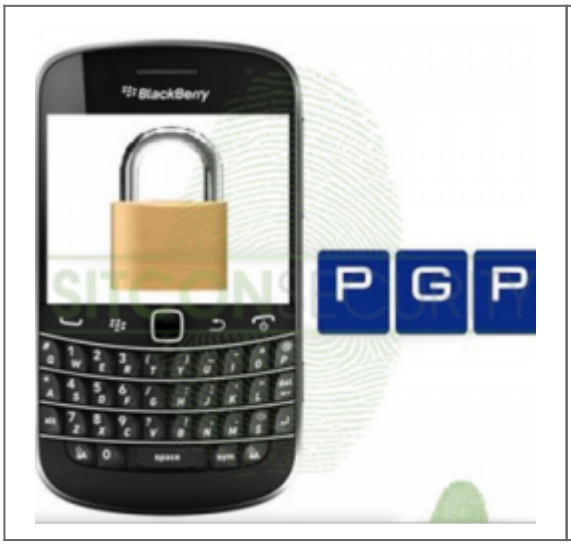
Cette vulnérabilité, présente dans le code source de Linux depuis 2012 mais découverte seulement maintenant par Perception Point, n'a pour l'heure pas été exploitée. L'équipe Linux a été prévenue et des correctifs devraient être disponibles sous peu et seront installés via des mises à jour automatiques. Selon Yevgeny Pats, cette vulnérabilité zero-day (CVE-2016-0728) concerne le service keyrings facility permettant aux drivers de sauvegarder dans le noyau de l'OS des données de sécurité ainsi que des clés d'authentification et de chiffrement.

Réagissez à cet article

Source : *Une vulnérabilité zero-day affecte des millions de systèmes Linux et Android – Le Monde Informatique*

Article de Dominique Filippone avec IDG News Service

Les Blackberry PGP déchiffrés par la Police hollandaise



Les Blackberry PGP déchiffrés par la Police hollandaise

Commercialisés par de nombreux vendeurs en ligne, les smartphones Blackberry embarquant en surcouche le standard de chiffrement de messagerie PGP seraient loin d'assurer un échange confidentiel des données. Tout du moins pour la Police hollandaise qui a confirmé être en mesure de les déchiffrer.

Les oreilles des défenseurs de la vie privée vont encore siffler. Des enquêteurs de la Police hollandaise ont en effet confirmé à Motherboard être en mesure d'accéder aux messages chiffrés envoyés depuis un terminal Blackberry sur lesquel le standard de chiffrement PGP est intégré en surcouche. « Nous sommes capables d'obtenir des données chiffrées depuis les terminaux Blackberry PGP », a fait savoir Tuscha Essed, responsable presse du Netherlands Forensic Institute (NFI), qui assiste la Police dans la recherche de preuves pour ses enquêtes en Hollande. L'information était parue initialement en décembre sur le blog misdaadnieuws.com où plusieurs documents sourcés NFI ont été publiés.

Le fait que les emails chiffrés puissent être lus et les messages effacés retrouvés, ne semble en tout cas pas perturber outre mesure les fournisseurs de Blackberry PGP. « Nous n'avons pas été affecté. Nos services sont complètement sécurisés et nous n'avons jamais été compromis », a indiqué un porte-parole de GhostPGP dans un mail à Motherboard. « Nous utilisons le dernier chiffrement PGP du moment qui est aussi impossible à déchiffrer. Nos clients sont très satisfaits du niveau de sécurité fourni », a quant à lui indiqué un représentant de TopPGP.com.

Réagissez à cet article

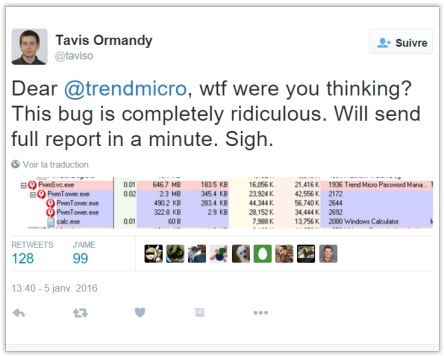
Source : *Les Blackberry PGP déchiffrés par la Police hollandaise – Le Monde Informatique*

Le coffre-fort à mots de passe de Trend Micro pas si fort

Le coffre-fort à mots de passe de Trend Micro pas si fort

L'éditeur de solutions de sécurité Trend Micro a lancé un correctif pour patcher une faille dans son logiciel Password Manager permettant à un attaquant distant de voler les mots de passe utilisateur.

Un chercheur en sécurité de Google, Tavis Ormandy, a tiré la sonnette d'alarme après avoir trouvé plusieurs failles dans le gestionnaire de mots de passe de Trend Micro, Password Manager. Ces dernières peuvent permettre à un personne malintentionnée d'exécuter du code à distance et de voler les mots de passe des utilisateurs stockés dans ce logiciel. L'éditeur japonais a confirmé ces problèmes et propose une mise à jour automatique pour les résoudre.



Ce n'est pas la première fois que Tavis Ormandy alerte l'éditeur sur l'existence de telles failles de sécurité. Se sentant frustré par un temps de réaction trop long de Trend Micro, le chercheur de Google a d'ailleurs pris la décision de poster les derniers échanges qu'il a eus avec la société. « Alors cela signifie que n'importe quel internaute peut voler tous les mots de passe en silence, autant qu'exécuter du code arbitraire sans aucune interaction utilisateur », s'est indigné Tavis Ormandy. « J'espère vraiment que vous prenez conscience de la gravité de la situation car je suis très étonné de tout cela. »

Des mots de passe utilisateurs trouvés en 30 secondes

Les utilisateurs des solutions antivirus de Trend Micro peuvent choisir d'utiliser le gestionnaire de mots de passe Password Manager afin pour exporter dedans l'ensemble de leurs mots de passe et de n'avoir plus qu'un mot de passe maître à retenir et utiliser. Les concurrents Dashlane ou LastPass proposent des services similaires. Ce gestionnaire est écrit en Javascript avec node.js et ouvre de multiples ports HTTP RPC pour des requêtes API, a précisé Tavis Ormandy. En 30 secondes, le chercheur indique avoir trouvé une requête API permettant d'accepter du code distant et également qu'une autre lui a permis d'accéder aux mots de passe stockés dans le gestionnaire. Cerise sur le gâteau, M. Ormandy a trouvé plus de 70 API de Trend Micro étaient exposées et a recommandé – non sans humour – à l'éditeur de recruter un constant externe pour auditer son code.

Les logiciels antivirus tournent avec un haut niveau de privilège sur les systèmes d'exploitation, ce qui signifie que l'exploitation d'une vulnérabilité peut donner à un attaquant un accès profond à un ordinateur. Des dizaines de sévères vulnérabilités ont été trouvé sur les 7 derniers mois dans les logiciels antivirus incluant ceux de Kaspersky Lab, Eset, Avast, AVG Technologies, Intel Security et Malwarebytes.

Réagissez à cet article

Source : *Le coffre-fort à mots de passe de Trend Micro transformé en passoire – Le Monde Informatique*

Les 5 dangers pour vos ordinateurs, smartphones et données en 2016

Les 5 dangers pour vos ordinateurs, smartphones et données en 2016

Les 5 tendances qui motiveront leurs actions envers votre ordinateur, votre smartphone, vos données…

Ecartelée entre la démocratisation de l'Internet des objets (thermostat intelligent, balance connectée…), la prise de pouvoir du stockage dans le « cloud » et l'émergence des nouveaux smartphones vedettes, la sphère des nouvelles technologies subira en 2016 les assauts des virus virulents, des arnaques en ligne, des cybercriminels.
Comme un caméléon virtuel, la cybercriminalité s'adaptera plus que jamais à l'air du temps pour exploiter les nouveaux territoires en friche.
Entre prudence et clairvoyance, voici les 5 tendances cybercriminelles qui se développeront ces 12 prochains mois, selon les experts de l'éditeur de solution de sécurité BullGuard.

1. La montée en puissance du « ransomware »
Impitoyable méthode d'extorsion, le « ransomware » bloque votre ordinateur, crypte vos fichiers personnels et vous réclame un paiement en ligne pour les libérer.
La menace brandie en cas de refus de payer la rançon : l'extermination de vos données (photos, vidéos, documents…).
Alors que les virus à l'ancienne et les chevaux de Troie accusent une certaine perte de vitesse, le « ransomware » est appelé à les dribbler.
Ces logiciels malveillants s'attrapent en visitant un site préalablement « hacké » (piraté) ou un obscur site volontairement malveillant, en téléchargeant des fichiers vérolés, notamment sur les plateformes d'échange de fichiers illégaux…

2. Le smartphone, cette cible indiscrète
Connecté à Internet 7 jours sur 7, 24 heures sur 24 dans le scénario le plus extrême, le smartphone concentre une myriade de données personnelles, des adresses email de vos contacts au numéro de votre carte de crédit.
Le téléphone est par conséquent une cible de choix pour les cybercriminels, qui rivalisent d'ingéniosité pour contourner les nouvelles barrières de sécurité régulièrement déployées par Apple pour ses iPhone et Google pour son système d'exploitation mobile Google Play.
Après avoir concentré leurs efforts sur la Chine et l'Extrême-Orient, les cybercriminels devraient viser tout particulièrement l'Europe en 2016.
Certes, nos smartphones étaient déjà menacés par le virus et les logiciels malveillants. Hélas, le niveau d'alerte devrait grimper de quelques degrés.

3. L'Eldorado inquiétant de l'Internet des objets
Nouvelle marotte des constructeurs, l'Internet des objets entend envahir notre quotidien pour évaluer et prédire nos besoins, mesurer notre activité, adapter l'éclairage et le chauffage de notre habitation en fonction de nos usages…
Qu'il s'agisse d'un pèse-personne connecté ou d'un thermostat intelligent, ces appareils vulnérables de par leur connexion constante à Internet récoltent au kilo les données personnelles.
Imaginons le cas d'une caméra de sécurité connectée. Elle pourrait simplement être détournée par un cybercriminel pour détecter les moments où vous quittez votre maison.
Toujours en quête d'un standard, notamment pour la sécurité, la galaxie de l'Internet des objets, tout juste née de son Big Bang historique, ne manquera pas de révéler en 2016 ses failles et ses vulnérabilités.

4. Des nuages dans le ciel du « cloud »
Inexorable lame de fond qui modifiera à jamais le monde du stockage, le « cloud » éparpille données et fichiers dans un nuage de serveurs (ordinateurs) répartis dans d'immenses « data center » aux quatre coins du monde.
Ces « fermes » informatiques dédiées au stockage et au traitement des données présentent un double intérêt pour les cybercriminels.
Leur puissance peut être détournée à d'autres fins, tandis que les données stockées constituent un sérieux trésor de guerre au cœur duquel il est tentant de piocher.
Objet de toutes les attentions des esprits mal intentionnés, la vulnérabilité du « cloud » risque d'être régulièrement soulignée ces prochains mois.

5. Les gangs sous les projecteurs
Les cybercriminels se structurent en gangs d'une efficacité redoutable, souligne BullGuard.
« Ils passent des semaines, voire des mois, à effectuer des missions de reconnaissance avant d'attaquer des organisations », témoignent les experts de l'éditeur. « Ces entreprises ont été conçues dès le départ pour se spécialiser dans les crimes informatiques et ont des hiérarchies cloisonnées qui incorporent des programmeurs spécialisés dans le piratage, de vendeurs de données et des gestionnaires, tous supervisés par un cadre supérieur. Ces équipes de cybercriminels occuperont le devant de la scène en 2016. »

Réagissez à cet article

Source : *Virus, arnaques en ligne, cybercriminalité : les 5 dangers de l'année 2016 – L'Avenir Mobile*

Google corrige 5 failles critiques d’Android

Google corrige 5 failles critiques d’Android

Pratiquement tous les terminaux tournant sous une version récente d'Android sont affectés par au moins une des cinq failles critiques corrigées par Google dans l'OS mobile.

Google a remédié à une douzaine de vulnérabilités d'Android, dont cinq sont qualifiées de « critiques ».
Parmi les failles critiques identifiées et corrigées dans cette nouvelle série de correctifs, la firme de Mountain View signale qu'une des vulnérabilités pourrait permettre à un attaquant d'exécuter du code distant – comme un malware – en exploitant la manière dont Android traite certains fichiers médias.

Nexus, puis smartphones Samsung, LG et BlackBerry

Google précise par ailleurs qu'Android 5.0 et les versions ultérieures – dont « Marshmallow » 6.0 – sont affectées par ces différentes vulnérabilités.
Et si la nature de ces failles vous évoque quelque chose, ce n'est pas une coïncidence. Mois après mois, le service « mediaserver » reste le composant le plus problématique d'Android. Au point que Google a copié-collé le même message dans ses bulletins de sécurité à chaque fois que le composant a été affecté.
La vulnérabilité critique porte sur une partie centrale du logiciel Android et qui dispose de permissions auxquelles les applications tierces n'ont normalement pas accès. D'autres failles se situent elles dans la gestion du Bluetooth et du Wi-Fi, ou encore au niveau du kernel.
Les terminaux Nexus sont les premiers appareils Android à recevoir les correctifs de sécurité. D'autres fabricants, parmi lesquels Samsung, LG et BlackBerry, déploieront des mises à jour dans les prochains jours.

Réagissez à cet article

Source : *Google corrige 5 failles critiques d'Android*

50 attaques informatiques qui ont marqué le web Français en 2015

50 attaques informatiques qui ont marqué le web Français en 2015

Pendant qu'il est possible de lire un peu partout sur le web le « top 5 », le « top 7 » des attaques informatiques dans le monde, ZATAZ préfère regarder du côté de VOS ordinateurs avec le top 50 des attaques informatiques qui ont touché la France et les internautes francophones. Des cas traités par ZATAZ.

Madison, Hacking Team, Hôtels Trump, Madisson, Vtech… les cas de piratage et de fuites de par le monde ont été pléthoriques, encore une fois, cette année. Revenir sur ces cas, pourquoi pas, mais il suffit d'en parler aux internautes francophones croisés sur la toile pour se rendre compte qu'ils ne se sentent pas concernés, et considères ces actes comme « drôles », ou « insignifiants » pour leur vie 2.0. Bilan, sur 1 475 personnes interrogées par ZATAZ (Âgés de 18 à 55 ans – entre le 22 décembre et le 30 décembre – 71% d'hommes – 43% évoluant dans le monde de l'informatique) seules 96 personnes interrogées avaient pris soins de modifier leurs mots de passe, car utilisés plusieurs fois dans des comptes différents (webmails, forums, …). 27 des interviewés confirmaient qu'ils regardaient plus souvent leur compte en banque. 339 avaient décidé, cette année, de faire un backup mensuel de leurs données (Je vous conseille fortement de pratiquer une sauvegarde, chaque jour, ndr).

Opération Anti Charlie

Janvier 2015, les attentats contre la rédaction de Charlie Hebdo et une supérette parisienne met en émoi le monde et le web. Les Anonymous décident de s'attaquer aux sites de djihadistes. Les participants s'attaquent à tout et n'importe quoi, dont des commerces de produits Hallal. En réponse, de jeunes internautes musulmans et plus d'une centaine de pirates du Maghreb et d'Asie lancent l'Opération Anti Charlie. Plus de 20 000 sites en .fr sont modifiés et/ou infiltrés. A noter que certains sites piratés, mais aussi infiltrés sans que la moindre trace du piratage n'apparaisse publiquement, ne sont toujours corrigés 11 mois plus tard. Une attaque informatique qui, sous l'excuse d'une cyber manifestation, était surtout menée et manipulée par des commerçants officiant dans le blackmarket. Dans la liste des espaces touchés : plusieurs centaines de sites du CNRS et des Restaurants du cœur, ainsi que 167 établissements scolaires d'Aquitaine ou encore de vieux espaces du Ministère de l'Intérieur et de la Défense.

TV5 Monde

Avril, le piratage de TV5 Monde fait grand bruit dans un contexte politique tendu. Au début du mois d'avril, la chaîne fait face à une cyberattaque d'ampleur. Ses différents comptes de réseaux sociaux sont piratés et diffusent de la propagande de la secte de Daesh. La diffusion des émissions de la chaîne sont coupées de l'antenne par la direction. Trend Micro évoque l'implication possible d'un groupe d'APT d'origine russe, Pawn Storm. Les autorités restent discrètes sur les différents éléments de l'affaire, si bien qu'encore aujourd'hui, on peine à se faire une idée de ce qu'il s'est vraiment passé dans le SI de France TV5 Monde. C'est surtout l'impact médiatique de cette attaque que l'on retiendra. Cinq mois après l'attaque, ZATAZ alertera l'ANSSI et TV5 Monde pour corriger d'autres failles informatiques découvertes sur les serveurs de la chaîne. A noter qu'un internaute est arrêté au mois d'août en Bulgarie. Des documents retrouvés dans son ordinateur son signé CyberCaliphate, le pseudonyme utilisé lors de l'attaque de TV5 Monde.
Un piratage qui fait ressortir que les media Français sont totalement dépassés par les potentialités malveillantes qui planent au-dessus de leurs claviers. Pour preuves, les différentes fuites de données et autres failles remontées par ZATAZ auprès de France Télévision [Fuite de données de téléspectateurs] ; du journal telecablesat.fr et 13 833 comptes clients volés.

Infiltrations

Les banques, les grands groupes Français sont visés, chaque jour, par des tentatives de piratage. Des attaques réussies ou non. Les clients ne sont jamais informés. Pendant ce temps, des millions d'informations appartenant aux Français sont pillés, copiés, revendues sur la toile. Par exemples, avec trois espaces de filiales de la BNP Paribas. Des sites retrouvés dans un espace pirate. Les malveillants s'échangeant les failles donnant accès à des bases de données. ; le pétrolier Total, et sa boutique, attaquée et pillée en janvier 2015. 29.657 clients d'un espace commercial grand public du pétrolier. Les pirates m'avouaient avoir vendu pour 500€ des informations de Français collectés dans cette BDD. Des fuites de données accessibles directement, ou via des tiers commerciaux, comme ce fût le cas pour TF1 et 1,9 millions de clients Français, abonnés à des journaux papiers ; Le site Internet La Boutique Officielle, spécialisé dans la vente de vêtements « Urban », visité par des pirates informatiques. Données des clients volées. L'entreprise ferme son espace numérique plusieurs jours ; de son côté, la CNIL contrôle 13 sites de rencontres français, 8 sont mis en demeure de mieux contrôler les informations de leurs « clients » ; En Mars, une faille informatique permettait à un pirate informatique de mettre la main sur les données d'un espace Orange Business.
Juin 2015, le portail Associations Sportives, qui répertorie plus de 240.000 clubs et associations françaises est infiltré. Le pirate diffuse un extrait de la base de données. Même sanction pour l'enseigne King jouet qui corrigera une fuite de données visant ses clients. Quinze ans de factures disponibles sur le web d'un simple clic de souris ; Un pirate informatique annonçait, en septembre, le vol des données appartenant au laboratoire Santé Beauté. Le groupe Santé Beauté regroupe des marques telles que « Barbara Gould », « Linéance », « Email diamant », « Batiste », « Nair », « Poupina » et « Femfresh ».
En octobre, le piratage de plusieurs espaces de la marque de lingerie ETAM était annoncé. Le jeune pirate diffusait plusieurs captures écrans qui ne laissent rien présager de bon pour la marque de textile.

Ransomwares

La grande mode des logiciels dédiés au chantage 2.0 (blocage de disque dur, chiffrement de données, NDR) aura frappé très fort en cette année 2015. ZATAZ a reçu pas moins de 3.022 mails de personnes et de PME piégés par ce genre d'attaque informatique. J'ai pu référencer plusieurs dizaines de mairies ou entités publiques malmenées par un ransomware, comme GDF Suez.

Arnaques et autres fraudes

Des arnaques au ransomware qui oblige les « pirates » à payer pour récupérer leurs informations prises en otage. Des arnaques qui existent aussi sous d'autres formes, comme la fraude au président. KPMG, Michelin, le Printemps, LVMH, Vinci, Total, Brevini, Areva, le cabinet d'avocats Baker & McKenzie, Finder France, SAM, Abuba, Vallourec, Sonia Ryckiel, Dargaud, Seretram… quelques exemples d'entreprises qui ont versé de l'argent à des professionnels du social engineering. Des pirates qui avaient collecté un grand nombre d'informations sur l'entreprise. Des données qui vont permettre de convaincre les services comptables de verser des millions d'euros aux pirates. Ces derniers se faisant passer pour le patron, un client, un fournisseur. Les premières arrestations ont eu lieu en février 2015. Elles concernaient les pirates ayant jeté leurs dévolus sur le club de football de l'Olympique de Marseille (OM). Deux hommes (50 et 34 ans) seront été arrêtés à Tel-Aviv.
Autre chantage, autre arnaque, celle mise en place par Rex Mundi. Plus de 15 000 identités de patients d'un laboratoire de santé français diffusées par le pirate. Le maître chanteur réclamait 20.000€ contre son silence. Le laboratoire n'a pas payé. Les informations sensibles et privées des patients seront diffusées.
Des pirates informatiques qui se spécialisent, même dans les prénoms à l'image de cet arnaqueur qui ne visait que les « Jacquelines« . Un prénom que l'escroc considère comme étant celui de personnes âgées.
Le chômage et la « crise » économique profitent aux pirates. Comme avec le site Internet Crédit Financement Fiable qui cachait une escroquerie numérique ; ou encore avec plusieurs cas d'arnaques téléphoniques. Le pirate se faisant passer pour la FNAC, Conforama ou encore Darty ; Les hôteliers, les chambres d'hôtes ne sont malheureusement pas oubliés avec une vague massive de fausses réservations de séjours.

Universités et écoles

Piratage, spams massifs, infiltration par des pirates présumés Chinois et maintenant, la diffusion d'une base de données d'élèves. L'informatique de l'université de Lyon 3 était-elle devenue complétement folle en février 2015 ? Quelques mois plus tard, rebelote, avec de nouvelles fuites de données. D'autres grandes écoles seront visées par des fuites, comme l'extranet du groupe éducatif ESG fermé à la suite d'un piratage informatique ; ou encore le cas de milliers de documents privés, et pour certains sensibles, d'étudiants de l'EPITECH. Plus de 47 000 dossiers pour quatre ans de fuite.

Fuite de données d'adresses postales

En Mars 2015, via le site Internet Degrouptest, il était possible de trouver l'adresse postale collée à un numéro de téléphone. Même une ligne téléphonique sur liste rouge pouvait être démasquée ; Neuf mois plus tard, le même type de fuite touchait un site Bouygues Telecom. Ici aussi, il suffisait de rentrer un numéro de téléphone pour accéder aux adresses postales. Liste rouge comprise.
Des fuites de données que connaitra aussi la société Somfy (spécialiste de la domotique). Zataz.com a pu constater que l'un de ses espaces web, il était dédié au personnel de l'entreprise, avait été infiltré par de nombreux pirates informatiques. Des pirates qui s'étaient empressés d'installer des backdoors, des portes cachées, leur permettant de jouer, à loisir, avec le serveur et son contenu.
Fuite de données sous forme de CV aussi, comme ce fût le cas pour un site d'Ametix. Des milliers de CV sauvegardés directement dans un dossier du WordPress d'un site dédié à une opération marketing.

Viagra et baskets dans votre site web

Le Black Seo, l'utilisation malveillante du référencement de liens et pages pirates via un site légitime, aura permis à des escrocs d'installer de fausses pharmacies et autres boutiques de contrefaçons dans des centaines de sites Français. Des Mairies, des boutiques, des sites étatiques ; Sans parler des sites propres sur eux, capable d'attirer dans leurs filets des milliers de Français, comme la fausse boutique officielle Nike RBFIRM.
En juin, le site Internet officiel de la chambre des Huissiers de Justice de Paris est (le site diffuse toujours des liens malveillants, ndr) piraté et exploité par des vendeurs de viagra ; des attaques que zataz révélera aussi en août 2015 à l'encontre du site de la Haute Autorité de la Santé ; ou encore en septembre pour la Fédération nationale des associations d'accueil et de réinsertion sociale, pour le portail dédié à une étude médicale en France et l'Établissement de Préparation et de Réponse aux Urgences Sanitaires (APRUS).

DDoS

Bloquer un site Internet, un serveur, un streamer (joueur en ligne) … la grande mode des petits pirates, en 2015. Des attaques qui ont eu pour mission de bloquer un site, d'empêcher son bon fonctionnement. Cette année, le groupe de presse belge Rossel (Le soir, La Voix du Nord, …), mais aussi NRJ, BFM, l'Académie de Grenoble ou encore l'UMP ont été attaqués de la sorte.
Des attaques faciles à mettre en place pour le premier idiot qui passe. Les boutiques vendant du DDoS poussent comme les champignons à l'automne. A noter que durant ce mois de décembre 2015, de très nombreux amateurs de jeux en ligne, des streamers, se sont retrouvés menacer par un maître chanteur demandant de l'argent pour stopper ses blocages.

Cartes Bancaires

La fraude à la carte bancaire se porte bien ! La police de Toulouse, et plus précisément la SRPJ, a mis la main sur trois cinéphiles pas comme les autres au mois d'avril 2015. Les individus avaient piégé un distributeur de billets installé dans le cinéma Gaumont Wilson ; En Juin, la banque postale déposé plainte après que des distributeurs de billets soient piégés par des skimmeur, du matériel pirate capable d'intercepter les données inscrites sur une carte bancaires ; Des cartes bancaires qui sont devenues causantes, en mode sans fil. Bilan, même le CNRS a tiré la sonnette d'alerte en indiquant que les cartes de paiement sans contact comportent de graves lacunes de sécurité ; du sans fil qui attire, en novembre, les Frotteurs 2.0 dans le bus, le métro et autres lieux publiques ; du matériel pirate que l'on a retrouvé, entre autre, au mois d'août 2015, dans un parking proche de la gare Montparnasse (Paris). Et les arrestations se succèdent, comme à Tours, et de la prison ferme (7 mois) pour l'un de ces pirates.

Objets connectés

En Mai, je vous expliquais que pour moins de 40 euros, des voleurs de voiture s'invitaient dans les véhicules que les propriétaires pensaient avoir fermé. Même le Ministère de l'Intérieur Français s'en inquiètera quelques jours plus tard ; des panneaux d'affichage seront attaqués, modifiés (Lille, Paris…). De la geek security attitude qui démontre aussi et surtout la faiblesse des villes connectées. La partie immergée d'un problème qui pourrait être bien plus dramatique.

Swatting

Le swatting, une mode venue des Etats-Unis. L'idée du pirate, envoyer les forces de l'ordre au domicile d'un joueur en ligne. En juillet, un second cas de swatting touchait la France. Domingo est un jeune Youtuber/Streamer. Un de ces jeunes professionnels du jeu en ligne qui diffuse ses parties, en direct. Il s'est retrouvé nez-à-nez avec la police après ce genre de mauvaise blague ; Le premier cas, en février 2015, BibixHD. L'action de la police, à son domicile, sera diffusé en directe alors qu'il était en train de jouer au jeu DayZ. Un inquiétant jeu qui amuse des adolescents en mal de repères. Certains vendant des possibilités de swatting pour quelques euros comme je le révélais au moins d'août !

Phreaking

Le piratage téléphonique, le phreaking, un acte numérique qui ne connait pas la crise. Mission du pirate, mettre la main sur une ligne téléphonique qu'il pourra commercialiser, surtout les minutes disponibles d'appels. Par exemples, en juillet, 5.288€ de détournement téléphonique pour la Maison de la Jeunesse de Nancy. En novembre, 43 000€ d'appels téléphoniques détournés pour le département des Deux-Sèvres.

Heartbleed

En juillet, la faille Heartbleed refaisait surface dans mes recherches. Une vulnérabilité datant d'avril 2014. Plusieurs centaines d'importants serveurs Français étaient toujours faillibles, 16 mois plus tard.

Scientologie

Des Anonymous se sont attaqués à plusieurs sites Français de la secte de la scientologie. Les manifestants 2.0 ont voulu rappeler l'affaire de Gloria Lopez, une ancienne scientologue retrouvée morte en 2006.

Box

Cette année, nous aurons connu chez ZATAZ cinq cas, dont deux considérés comme sérieux. Numéricâble, et Bouygues. Ce dernier avait son option Playin'TV particulièrement sensible. Plusieurs problèmes qui auraient pu servir à des actions malveillantes.

Réagissez à cet article

Source : *ZATAZ Magazine » Les 50 attaques informatiques qui ont marqué le web Français en 2015*

Paralyser une voiture pour 90 euros | Data Security Breach

Paralyser une voiture pour 90 euros | Data Security Breach

---

la prise USB d'une Toyota Corolla, un chercheur en informatique, bloque la voiture à coup de DDoS.

Le monde du « sans connexion » envahi nos vies. La marche de l'IoT est lancée et rien ne l'arrêtera vue les enjeux économiques. L'important, que le client achète, on verra ensuite pour sa sécurité. **Du moins si le client est encore vivant.**

Inoue Hiroyuki, professeur en informatique à la Graduate School of Information Sciences de l'université d'Hiroshima a expliqué comment il avait « planté » une Toyota Corolla avec 90€.
Une clé USB trafiquée et un DDoS via le port USB de la voiture « Le pilote était incapable de bouger la voiture en appuyant sur l'accélérateur » explique-t-il dans le Japan Times. L'agrégé en informatique a indiqué avoir aussi été capable d'ouvrir et fermer les fenêtres de la voiture, afficher une lecture de compteur de vitesse incorrecte et geler l'accélérateur. Toyota a annonçait qu'il allait continuer « à faire des efforts » pour améliorer la sécurité de ses véhicules.

Il serait peut-être temps d'arrêter de nous prendre pour des idiots ?
En juillet 2015, une Jeep Cherokee, et un mois plus tard, une Corvette étaient elles aussi malmenées. Le piratage des voitures ne fait que débuter ! Pour le moment, il ne se déroule officiellement que dans des laboratoires.

Réagissez à cet article

Source : *Paralyser une voiture pour 90 euros | Data Security Breach*

Hello Kitty : les données de millions de fans compromises

Hello Kitty : les données de millions de fans compromises

Les données personnelles de millions fans d'Hello Kitty étaient facilement accessibles. C'est un chercheur en sécurité Chris Vickery qui a donné l'alerte. Il a découvert une base contenant les informations de plus de trois millions d'utilisateurs, tels que nom, prénom, pays d'origine, emails, mots de passe. La société japonaise Sanrio qui gère la licence Hello Kitty assure avoir comblé la faille de vulnérabilité.

Et pour l'heure, l'entreprise assure aussi n'avoir détecté aucun vol de données. Une mauvaise configuration serait à l'origine du problème.
A quelques jours de Noël, la nouvelle passe mal. Le mois dernier déjà, c'est le fabricant de jouets hongkongais VTech qui était sur la sellette après le piratage de centaines de milliers de comptes et de profils d'enfants.

Réagissez à cet article

Source : *Hello Kitty : les données de millions de fans*

compromises | euronews, monde

Juniper : une faille de sécurité permettait de surveiller le trafic VPN

	**Une faille de sécurité permettait de surveiller le trafic VPN**

La firme indique avoir découvert des portes dérobées dans ScreenOS, présent dans ses pare feux et services VPN. Par mesure de sécurité, Juniper a mis à jour son système d'exploitation.

Juniper indique qu'un morceau de code informatique non-autorisé était présent dans son système d'exploitation maison. Ce dernier est utilisé pour une partie de ses solutions de sécurité tels que les firewall et les services de VPN. La société a donc émis un bulletin de sécurité au sujet de ce code-espion.
Ce dernier aurait été initialement publié en 2008, de quoi laisser le temps aux éventuels attaquants d'utiliser cette porte dérobée pour utiliser des informations transitant par le biais de ces équipements. Un correctif est donc actuellement déployé par Juniper, en particulier pour les équipements de la gamme NetScreen.
Malgré ces mises à jour de sécurité, Juniper n'a pas identifié la provenance de ce code aux effets malfaisants. Si la thèse des services de renseignement n'est pas à exclure, il pourrait également s'agir de hackers ou même de développeurs présents en interne (voire des sous-traitants).

La porte dérobée doit en principe permettre à un attaquant d'accéder à distance en mode administration à un équipement sous ScreenOS. Quant à la seconde vulnérabilité mise au jour par Juniper, elle autorise un pirate à surveiller un trafic au sein d'un VPN.
Malgré l'ampleur du problème, la direction se veut rassurante. Elle précise : « pour le moment, aucun rapport n'indique que ces vulnérabilités ont été exploitées. Nous recommandons vivement aux clients de mettre à jour leurs systèmes et d'appliquer les versions corrigées sans délai ».

Réagissez à cet article

Source : *Juniper : une faille de sécurité permettait de surveiller le trafic VPN*

Un malware qui reste lors d’une réinstallation du système d’exploitation

Un malware qui reste lors d’une réinstallation du système d’exploitation

---

Conçu en particulier pour dérober des données bancaires, l’écosystème Nemesis comporte un logiciel malveillant qui s’installe à très bas niveau sur le disque dur.

Les équipes de Mandiant (FireEye) ont découvert, en septembre dernier, un logiciel malveillant employant des méthodes de persistance peu communes : il s’immisce dans le processus d’initialisation de l’ordinateur infecté, avant même le chargement du système d’exploitation, afin de pouvoir compromettre celui-ci à coup sûr et, surtout, résister à une tentative de nettoyage de la machine par réinstallation de son système d’exploitation – « un moyen largement considéré comme le plus efficace pour éradiquer un logiciel malveillant », soulignent les chercheurs de FireEye dans un billet de blog.

Analyse comportementale : la clé de la sécurité ?

E-handbook : L’analyse comportementale joue un rôle non négligeable dans la sécurité de votre entreprise.

Ce logiciel malveillant fait partie de Nemesis, un ensemble d’outils malicieux utilisé par le groupe FIN1, qui semble « localisé en Russie, ou un pays russophone », spécialisé dans le vol de données de cartes bancaires et, plus généralement, d’informations « aisément monétisables en provenance d’organisations telles que banques, organismes de crédit, opérations de DAB », etc.

Comme le rappellent les chercheurs de FireEye, le secteur d’amorçage des disques durs, le fameux MBR (Master Boot Record), ne contient pas que des données inertes relatives aux partitions définies : il recèle également quelques éléments de code utilisés durant le processus de démarrage ; « ce code cherche la partition active principale et passe ensuite le contrôle au VBR (Volume Boot Record) de cette partition ». Ce dernier contient également du code exécutable « spécifique au système d’exploitation présent sur cette partition », et lui permettant de lancer son démarrage.

Baptisé Bootrash, le logiciel malveillant découvert par les équipes de Mandiant, pirate ce processus en remplaçant le code d’amorçage du VBR par son propre code malicieux chargé d’appeler le bootkit Nemesis. Celui-ci « intercepte certaines fonctions du processus de démarrage et injecte les composants Nemesis dans le noyau de Windows ».

Les chercheurs de FireEye soulignent que ce n’est pas une première, mais que l’utilisation d’un bootkit MBR ou VBR n’est pas courant. Une chance, peut-être, car la détection peut s’avérer particulièrement difficile : ces logiciels malveillants peuvent « être installés et s’exécuter presque complètement en dehors du système d’exploitation Windows », passant au travers des mécanismes de vérification de son intégrité ou encore des anti-virus – à moins d’examiner méticuleusement la mémoire vive.

Réagissez à cet article

Source : http://www.lemagit.fr/actualites/4500260472/Un-malware-qui-reste-lors-dune-reinstallation-du-systeme-dexploitation