Piratage de 1,6 million de comptes Clash of King

Piratage de 1,6 million de comptes Clash of King

Pour ne pas avoir corrigé une faille vieille de 3 ans, le jeu Clash of King se retrouve avec 1,6 million de comptes de joueurs dans la nature.

vBulletin, un framework (un outil Internet NDR) de forum très utilisé sur le réseau des réseau a subi à plusieurs reprises des failles de sécurité. Des « bugs » que s'empressent d'utiliser les pirates informatique. La dernière campagne malveillante officielle visant ce forum concerne la société Elex qui produit le jeu sur mobile « Clash of Kings ». Ce jeu est utilisé par des millions de joueurs sur les plateformes mobiles. Ces joueurs s'enregistrent sur le forum afin d'échanger avec d'autres utilisateurs.
Le pirate a profité d'une faille vBulletin connue pourtant depuis 2013. Comme le rappel Matthieu Dierick, de chez F5 Networks, les failles ne sont pas nouvelles et l'ANSSI avait déjà alerté les autorités au sujet de vBulletin. Bref, si vous ne patchez pas, il ne faut pas pleurer ! vBulletin n'est pas responsable du fait que les entreprises ne programment pas leur mise à jour.
Pour détecter si un serveur est vulnérable, il suffit de lancer une requête HTTP sur une liste de serveurs et d'attendre un code retour. Voici un exemple de requête utilisée pour détecter la vulnérabilité d'un serveur : *http://[l'url du site]/ajax/api/hook/decodeArguments?arguments=O:12: »vB_dB_Result »:2{s:5: »*db »;O:11: »vB_Database »:1:{s:9: »functions »;a:1{s:11: »free_result »;s:6: »assert »;}}s:12: »*recordset »;s:20: »print_r(md5(92829)) »;}*.
Si le code retour contenait le hash 92829, alors l'espace numérique est vulnérable. C'est l'action qu'a orchestré le pirate de Clash of King. C'est la recherche qu'aurait du faire les équipes de Clash of King pour se protéger et sécuriser les utilisateurs.
Nous ne connaissons pas encore la vulnérabilité exploitée mais lors des dernières campagnes de piratage sur vBulletin, les pirates ont réussi à envoyer leur SHELL (Outil installé dans le serveur qui permet au pirate d'être maître de l'espace infiltré, NDR) sur le serveur et a exécuter des requêtes SQL en mode « root ». Pour cela, ils passaient par des fonctions PHP, par exemple la fonction system() qui permet l'exécution de commande shell.

Mot de passe hashé ? la belle affaire !
Les données volées concernent les identifiants avec mot de passe hashé, l'adresse mail, l'adresse IP et les tokens liés aux réseaux sociaux. Par hashé, comprenez que le mot de passe ne se lit plus directement (ZATAZ se transforme en hashé md5 par *79e35664717c21b96225d8d6ed4f0b16*). Les utilisateurs du forum doivent donc changer leur mot de passe même si ceux-ci étaient rendus illisibles au niveau de la base de données. Le hash MD5 ne sertb à rien si un mot de passe trop simple a été enregistré. Reprenons mon exemple avec *79e35664717c21b96225d8d6ed4f0b16*. Allez sur le site crackstation.net et rentrez *79e35664717c21b96225d8d6ed4f0b16*. En quelques millièmes de secondes, le mot de passe hashé n'est plus illisible. Pour une meilleure sécurité, dirigez-vous plutôt vers bcrypt !
« ***Toute infrastructure de données doit être protégée par des mécanismes d'analyse de niveau 7 tels que les Firewall Applicatifs ou Web Application Firewall.*** Indique Matthieu Dierick (Il commercialise ce genre d'outil, NDR). ***Cela peut empêcher un pirate de lancer des commandes sur un serveur même si celui-ci est concerné par une faille de sécurité***« . La politique de WAF empêche l'exécution de scripts, de commandes shell et de commandes PHP non autorisées.
En attendant, les 1,6 millions de clients impactés de Clash of King sont invités à changer leur mot de passe… surtout si ce dernier est aussi utilisé sur d'autres espaces web !

0Day vBulletin dans la nature ?
A noter que la société Trillian a alerté ses utilisateurs de l'utilisation d'un 0day vBulletin qui a touché l'un de ses services. La société ne sait pas vraiement quand a eu lieu l'attaque [on parle de décembre 2015, NDR] mais a fermé le site et le serveur contenant les forums impactés par la fuite de données. Dans les informations prises en main par le pirate : les données du blog de la société [sous WordPress] et « une poignée d'autres bases de données marketing qui contenait les noms d'utilisateurs Trillian et leurs adresses mail ». Les mots de passe étaient, eux aussi, en Md5. Le plus inquiétant à mon sens est que Trillian indique que les données « volées » étaient âgées de 3 à … 14 ans !
Article original de

Original de l'article mis en page : ZATAZ Piratage de 1,6 million de comptes Clash of King – ZATAZ

L’arnaqueur Chinaper Chinapa roi de l’escroquerie sur Internet enfin arrêté

L’arnaqueur Chinaper Chinapa roi de l’escroquerie sur Internet enfin arrêté

Il se nomme Chinaper Chinapa, un arnaqueur de Côte d'Ivoire qui vient d'être arrêté. Il arnaquait des hommes et des femmes sur Internet.

Les scammeurs, les brouteurs, bref les escrocs qui s'attaquent aux internautes sont légions sur la toile. Ils usent de multiples arnaques pour soutirer de l'argent à leurs victimes. Ils jouent ensuite les « rois » dans leur quartier. Parmi les pièges usités : l'arnaque à l'amour, le wash-wash, la création de billets, le faux mail d'inquiétude d'un proche perdu, la fausse location ou loterie… Pour Chinaper Chinapa, chaussures et portes feuilles magiques en bonus ! Je possède une liste d'une quarantaine d'arnaques possibles mises en place par les brouteurs.

Chinaper Chinapa le chenapant !

L'un des « rois » des brouteurs se nommait Chinape Chinapa. L'amateur de casquettes et baskets « bling-bling » se faisait passer pour un « magicien ». Il affirmait être capable de faire sortir des billets de chaussures, de boite magique. Il avait aussi mis en place des arnaques amoureuses, se faisant passer pour des hommes et des femmes à la recherche de l'âme sœur. Il volait les photos sur Facebook et « chassait », ensuite, sur des sites de rencontres.

J'ai pu croiser cet escroc de Chinaper Chinapa, il y a quelques mois, dans son pays (il se baladait aussi beaucoup au Bénin). Ce « roi » des boites de nuit qui sortait les billets de banque plus vite que 007 son Walther PPK.

Mi juin 2016, l'homme avait été tabassé par des personnes qu'il avait escroquées. Quinze jours plus tard, la police lui mettait la main dessus pour une série d'escroqueries. Arrêté par la police début juillet, détail confirmé par le journal Koaci. Le flambeur s'est retrouvé les menottes aux poignets dans son appartement de Cocody. Il est accusé d'activités cybercriminelles et de multiples escroqueries. Pas évident que sa « magie » fonctionne dans la prison d'Abidjan.

Un ami a besoin de vous

15h, un courrier signé d'un de vos amis arrive dans votre boîte mail. Pas de doute, il s'agit bien de lui. C'est son adresse électronique. Sauf que derrière ce message, il y a de forte chance qu'un brouteur a pris la main sur son webmail. Les courriels « piégés » arrivent toujours avec ce type de contenu « ***Je ne veux pas t'importuner. Tu vas bien j'espère, puis-je te demander un service ?***« . Le brouteur, par ce message, accroche sa cible. En cas de réponse de votre part, l'interlocuteur vous sortira plusieurs possibilités liées à sa missive « ***J'ai perdu ma carte bancaire. Je suis coincé en Afrique, peux-tu m'envoyer de l'argent que je te rembourserai à mon retour*** » ; « ***Je voudrais urgemment recharger ma carte afin de pouvoir régler mes frais de déplacement et assurer mon retour. J'aimerais s'il te plaît, que tu me viennes en aide en m'achetant juste 4 coupons de rechargement PCS MASTER CARD de 250 € puis transmets moi les codes RECH de chaque coupon de rechargement, je te rembourserais dès mon retour***« . Je possède plus d'une centaine de variantes d'excuses.

Bien entendu, ne répondez pas, ne versez encore moins d'argent. Attention, selon les brouteurs, des recherches poussées sur leurs victimes peuvent être mises en place. J'ai dernièrement traité le cas d'un brouteur qui connaissait le lieu de résidence du propriétaire du compte webmail que le voyou utilisait. De quoi faire baisser les craintes des amis contactés.

A noter que le scammeur indiquera toujours un besoin de confidentialité dans sa demande : « ***Je souhaite également que tu gardes ce mail pour toi uniquement. Je ne veux pas inquiéter mon entourage. Y'a t'il un buraliste ou un supermarché non loin de toi ?***« .

Remboursement de l'argent volé

Une autre arnaque de brouteurs est intéressante à expliquer. Elle est baptisée « *remboursement*« . Le voleur écrit aux internautes se plaignant, dans les forums par exemple, d'avoir été escroqués. L'idée de l'arnaque est simple : le voleur indique qu'il a été remboursé grâce à un policier spécialisé dans les brouteurs. Le voyou fournit alors une adresse électronique.

Suivre

ZATAZ.COM Officiel @zataz

Prudence à l'adresse « interpol.police.antiarnaque@gmail(.)com » qui n'est pas celle d' #interpol *! L'escroc cherche des personnes escroquées.*

23:12 – 14 Mai 2015

•

•

1111 Retweets

•

55 j'aime

Derrière cette fausse adresse de policier, un autre brouteur. Il va tenter d'escroquer le pigeon déjà pigeonné. Sa mission, se faire envoyer de l'argent via Western Union, MoneyGram. Certains brouteurs sont à la solde de petits commandants locaux qui imposent un quota d'argent à collecter. En 2013, la cyber police de Côté d'Ivoire estimait que les brouteurs avaient pu voler pas moins de ***21 millions d'euros****. N'hésitez pas à me contacter si vous avez croisé la route d'arnaques.*

Article original de Damien Bancal

Réagissez à cet article

Original de l’article mis en page : ZATAZ Brouteur : Chinaper Chinapa roi de l’escroquerie 2.0 – ZATAZ

Les claviers sans fil pourraient aussi servir à espionner !

Les claviers sans fil pourraient aussi servir à espionner !

Avec un simple dongle USB, une antenne et quelques lignes de code, un pirate peut capter toutes les frappes d'un clavier sans fil, selon la start-up Bastille.

Après les souris (MouseJack), les claviers sans fil… Avec une simple antenne et un dongle USB, plus quelques lignes de code écrites en Python, un pirate peut enregistrer *« toutes »* les frappes réalisées par l'utilisateur d'un clavier sans fil bon marché ou générer ses propres frappes, selon la start-up américaine Bastille. Et ce dans un rayon de plusieurs dizaines de mètres autour de la cible.

Claviers sans fil vulnérables

« Lorsque nous achetons un clavier sans fil, nous nous attendons à ce que le fabricant ait conçu et intégré la sécurité nécessaire au coeur du produit », a déclaré Marc Newlin, ingénieur et chercheur chez Bastille. *« Nous avons testé les claviers de 12 fabricants et nous avons constaté, malheureusement, que 8 d'entre eux (soit les deux tiers) sont vulnérables à une attaque [que l'on nomme] KeySniffer »*.

Ces claviers sans fil utilisent le plus souvent des protocoles radio propriétaires peu testés et non sécurisés pour se connecter à un PC, à la différence du standard de communication Bluetooth. Ils sont d'autant plus faciles à détecter car leur signal est toujours actif… Les fabricants concernés (dont HP, Toshiba et Kensington) ont tous été alertés. Selon Bastille, la plupart, voire tous les claviers exposés à KeySniffer ne peuvent pas être mis à jour et devront être remplacés.

Absence de chiffrement

En 2010 déjà, les développeurs de Dreamlab Technologies ont exposé une faille dans un clavier sans fil Microsoft. Le *« renifleur »* et programme Open Source KeyKeriki a capté le signal et déchiffrer les données transmises à un ordinateur… Mais la découverte de Bastille, KeySniffer, est différente. Elle montre que des fabricants produisent et vendent encore des claviers *wireless* sans chiffrement.

La start-up recommande aux internautes d'utiliser un clavier filaire pour se protéger.

Article original de Ariane Beky

Réagissez à cet article

Original de l'article mis en page : Les claviers sans fil, des espions en puissance

Privacy Shield : 1 an de sursis donné par les CNIL européennes

Privacy Shield : 1 an de sursis donné par les CNIL européennes

Les CNIL européennes ne sont pas satisfaites du Privacy Shield, mais prennent date en 2017 pour s'inviter dans la révision de l'accord.

Le verdict était attendu. Les CNIL européennes du groupe de l'article 29 (G29) ont rendu leur décision définitive sur le Privacy Shield. Cet accord encadre le transfert des données entre les Etats-Unis et l'Union européenne Il est le successeur du Safe Harbor, invalidé par la Cour de Justice de l'Union européenne. Dans un communiqué de presse, le G29 souligne ses réserves sur le Privacy Shield. Il considère néanmoins que l'accord a été voté et il donne rendez-vous au 1 an de l'accord lors de sa révision pour un examen plus approfondi de certaines dispositions.

En avril dernier, le groupe avait émis différentes critiques sur le Privacy Shield. Il avait souligné *« un manque de clarté général »*, une *« complexité »*, et parfois une *« incohérence »*, des documents et annexes qui composent le Privacy Shield. C'est notamment le cas pour les voies de recours que pourront emprunter les citoyens européens contestant l'exploitation de leurs données outre-Atlantique, indique le groupe dans son avis consultatif.

Quant à l'accès des agences de renseignement aux données transférées dans le cadre du Privacy Shield (volet sécurité nationale), il soulève de *« fortes préoccupations »*. Le risque d'une collecte *« massive et indiscriminée »* des données par un État n'est pas écarté. Le groupe s'inquiète aussi du statut et de l'indépendance du médiateur (*« ombudsman »*) vers lequel les citoyens européens pourront se tourner.

Un an de sursis et une mise en garde

Certaines réserves ont été prises en compte, note le G29, mais « cependant un certain nombre de préoccupations demeurent ». Au premier rang desquels, le risque toujours bien réel d'une surveillance de masse par le gouvernement américain. Il évoque le rôle du médiateur et la révision annuelle de l'accord.

Les CNIL européennes comptent beaucoup sur cette révision annuelle prévue en juillet 2017. Elles profiteront de cette occasion « *pour non seulement évaluer si les questions en suspens ont été résolues, mais aussi si les garanties prévues par le Privacy Shield entre les Etats-Unis et l'UE sont réalisées et efficaces* ». Et de prévenir, que « *tous les membres de l'équipe en charge de cette révision doivent avoir accès à toutes les informations nécessaires à l'accomplissement de leur examen y compris des éléments favorisant leur propre évaluation sur la proportionnalité et la nécessité de la collecte et l'accès aux données par les pouvoirs publics* ». Une mise en garde contre les risques d'être éconduits dans un an.

Pendant ce temps-là, le Privacy Shield pourrait être contesté par des citoyens européens, comme cela a été le cas avec Max Schrems pour le Safe Harbor. Lors d'une récente discussion dans le cadre de Cloud Confidence, le jeune avocat avais émis l'hypothèse d'une nouvelle action en justice contre le Privacy Shield.

Article original de Jacques Cheminat

Réagissez à cet article

Original de l’article mis en page : Privacy Shield : les CNIL européennes accordent 1 an de sursis

---

LastPass affecté par une faille critique d’accès à distance

LastPass affecté par une faille critique d’accès à distance

Le chercheur en sécurité Tavis Ormandy a repéré une faille critique dans LastPass qui permettrait d'établir un accès à distance dans le gestionnaire de mots de passe. Un signalement à LastPass a été effectué, qui prépare un correctif.

Les gestionnaires de mots de passe peuvent se montrer d'une grande aide pour celui qui tient à conserver en un seul endroit une multitude de codes d'accès. Surtout, ils satisfont d'un coup plusieurs exigences en matière de sécurité informatique qui sont parfois contradictoires ou inapplicables au-delà d'un certain seuil.
Regardons un instant ce que l'on demande en règle générale à l'usager : l'utilisation d'un mot de passe unique par service, tout en respectant un strict formalisme qui va de la longueur du mot de passe (x caractères au minimum) à sa complexité (des lettres, des chiffres, des symboles, des majuscules et des minuscules, en mélangeant le tout), en passant par son renouvellement (sait-on jamais).

Bien entendu, il est évidemment tout à fait déconseillé de les noter simplement sur un bout de papier (on n'est jamais trahi que par les siens) ou de les enregistrer dans un fichier sur le PC (qui peut se faire pirater). Or, la seule mémorisation n'est pas une solution d'avenir : au-delà de quelques services, l'utilisateur s'y perdrait. D'où l'intérêt de passer par des gestionnaires de mots de passe.

Mais leur utilité ne doit pas faire oublier le fait que ces programmes sont par essence imparfaits.
Malgré tout le soin qui peut être apporté pendant leur conception, ces logiciels (les plus connus sont Dashlane, 1Password, KeePass et LastPass) peuvent être sensibles à certaines attaques. On l'a vu par exemple avec LastPass, qui est annoncé comme vulnérable au hameçonnage et qui a essuyé une intrusion dans son infrastructure, a priori sans dommage pour les mots de passe eux-mêmes.
Dans ce contexte, des initiatives comme celle lancée par la Commission européenne, qui consiste à organiser un audit du code source de KeePass – qui est un logiciel libre, ce qui facilite grandement les choses – sont à accueillir avec bienveillance. Elles contribuent à un rehaussement général du niveau de fiabilité de ce type de logiciel, à défaut de le rendre invulnérable, ce qui est illusoire.
La contribution d'un chercheur comme Tavis Ormandy est aussi précieuse, même si de prime abord elle provoque légitimement une inquiétude sur le degré de finition de certains logiciels. En effet, l'intéressé indique avoir déniché dès le premier coup d'œil une série de problèmes critiques qui lui ont sauté aux yeux. Il a ajouté avoir fait suivre un rapport complet à LastPass pour qu'il les règle.
La nature des vulnérabilités repérées n'est pas précisée par Tavis Ormandy. Le blog Naked Security, édité par l'éditeur d'antivirus Sophos, écarte pour le moment la piste de la faille 0-Day. Une telle vulnérabilité désigne les brèches n'ayant fait l'objet d'aucune publication ou n'ayant aucun correctif connu. Elles sont les plus dangereuses, car elles sont secrètes et peuvent être exploitées en toute discrétion.
Tout juste sait-on que la vulnérabilité en question permettrait un accès complet à distance. L'on peut imaginer que des détails supplémentaires seront donnés ultérieurement, lorsque LastPass aura fini son intervention. Dans un autre tweet, Tavis Ormandy ajoute qu'il va se pencher dans la foulée sur 1Password et regarder s'il peut repérer des fragilités dans ce gestionnaire.
Dans le cadre d'une divulgation responsable, les spécialistes en sécurité informatique sont en effet invités à signaler d'abord aux sociétés les failles qu'ils repèrent dans les logiciels qu'elles éditent, et cela en toute discrétion. Ce n'est qu'ensuite qu'une diffusion publique peut avoir lieu, une fois les correctifs appliqués, de façon à ce que des personnes mal intentionnées ne puissent pas en profiter.
Tavis Ormandy est une pointure dans le domaine de la sécurité informatique.
Il s'est illustré à diverses reprises en signalant des brèches critiques dans un certain nombre de logiciels, comme Linux, Windows, la plateforme de jeux Uplay conçue par Ubisoft ou encore le shell Bash. Il a aussi épinglé les éditeurs d'antivirus Sophos et Trend Micro. Il travaille depuis quelques années dans l'équipe Project Zero mise sur pied par Google pour traquer les failles 0-Day, qui regroupe quelques personnalités. À tel point qu'elle est présentée comme une dream team.
Article original de Julien Lausson

Réagissez à cet article

Original de l’article mis en page : LastPass affecté par une faille critique d’accès à distance – Tech – Numerama

---

Vous utilisez des objets connectés? Gare à vos données

Vous utilisez des objets connectés? Gare à vos données

Une étude publiée par l'entreprise de cybersécurité AV-Test montre que la plupart des objets connectés testés, destinés à surveiller sa forme, sont susceptibles d'être piratés.

Ils mesurent toutes les performances. Seulement voilà: d'après une étude publiée par l'entreprise de cybersécurité AV-Test le 18 juillet 2016, les objets connectés utilisés pour surveiller sa forme ne sont pas sécurisés. Pire encore, ils présentent des failles de sécurité pouvant permettre à des pirates informatiques d'accéder à leurs données et de les manipuler.

Des appareils utilisés par les assureurs

Pour en arriver à cette conclusion, AV-Test a examiné sept appareils utilisant Android, le système d'exploitation mobile de Google, et repéré des vulnérabilités similaires à celles qu'elle avait déjà identifiées il y a un an. Beaucoup d'appareils manquent de connexions sécurisées ou de protection contre les accès non autorisés. Les fabricants « ne font souvent pas assez attention à l'aspect de la sécurité », indique l'étude.

Elle fait pourtant valoir qu'il faudrait prendre davantage au sérieux la sécurité de ces appareils dont l'usage s'élargit, certaines assureurs santé commençant même à les utiliser pour fixer leurs tarifs ou proposer des remises.

Trois appareils avec des risques de piratages importants

Dans le détail, les appareils affichent des niveaux de sécurité variés. Selon l'étude, le risque le plus élevé est présenté par les appareils de Runtastic, Striiv et Xiaomi, où AV-Test relève 7 à 8 vulnérabilités potentielles sur un total de dix. AV-Test indique notamment que « ces appareils peuvent être suivis à la trace plutôt facilement » et qu'ils utilisent des systèmes d'identification et de protection contre les accès non autorisés incohérents ou inexistants, ou encore que leur programme n'est pas assez protégé pour garantir la sécurité des données collectées.

« Pire que tout, Xiaomi stocke toutes les données de manière non cryptée sur le smartphone », s'inquiète l'étude. Les appareils les plus sûrs, avec 2 à 3 risques potentiels pour la sécurité, sont la montre Pebble Time, le bracelet Band 2 de Microsoft et le moniteur d'activité et de sommeil Basis Peak.

L'Apple Watch tire son épingle du jeu

La montre connectée Apple Watch, évaluée selon des critères différents car elle utilise un autre système d'exploitation, a pour sa part, selon les chercheurs d'AV-Test, une « note de sécurité élevée », malgré des « vulnérabilités théoriques ».

L'Apple Watch est « presque impossible à suivre à la trace », mais dévoile certaines caractéristiques d'identification quand elle est en mode avion alors que ça « ne devrait pas être le cas », détaillent-ils. L'appareil « utilise essentiellement des connexions cryptées qui ont des sécurités supplémentaires », mais ses mises à jour se font par une connexion non cryptée, notent-ils aussi.

D'après le cabinet de recherche IDC, plus de 75 millions d'appareils connectés « fitness » ont été vendus en 2015 dans le monde, et le niveau devrait franchir la barre des 100 millions cette année.

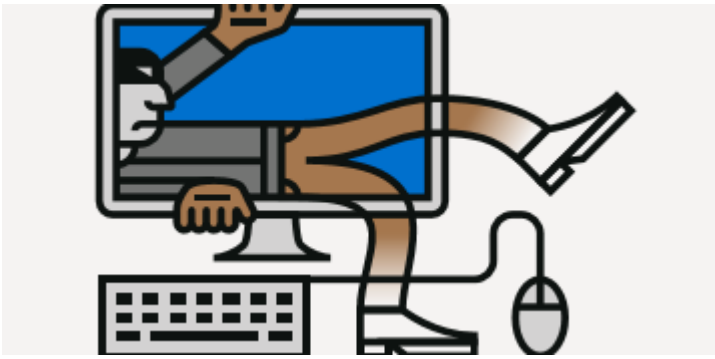
Article original de Stephen Lam

Réagissez à cet article

Original de l’article mis en page : Vous utilisez des objets connectés? Gare à vos données – L’Express L’Expansion

---

77 % des entreprises totalement impuissantes face à des Cyberattaques



77 % des entreprises totalement impuissantes face à des Cyberattaques

---

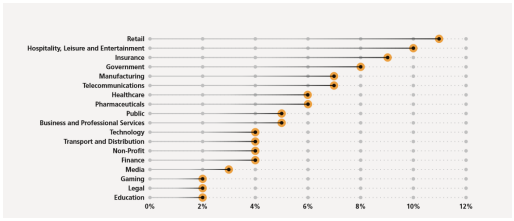
Pénurie de compétences et manque d'investissements : les entreprises sont non seulement vulnérables aux attaques, mais aussi impuissantes pour les résoudre seules. Décryptant les tendances de ces trois dernières années dans le monde, un rapport de NTT Com Security souligne le peu de progrès réalisés dans ce domaine, et note même un recul….

Le GTIR (« Global Threat Intelligence Report ») analyse une énorme masse de données issues de 24 centres d'opérations de sécurité (SOC), sept centres R&D, 3 500 milliards de logs et 6,2 milliards d'attaques. Ces résultats sont donc particulièrement intéressants pour suivre l'état des menaces dans le monde. Son édition 2016, qui décrypte les tendances de ces trois dernières années souligne le peu de progrès réalisés par les entreprises dans leur lutte contre les menaces, et note même une légère hausse du nombre d'entre elles mal préparées qui s'élève à 77 %. Face à des attaques d'envergure, elles doivent le plus souvent solliciter une intervention extérieure. Seules 23 % des organisations seraient donc en mesure de se défendre efficacement contre des incidents de sécurité majeurs.

Le retail le plus touché par les incidents

Après des années passées en tête des secteurs les plus touchés dans les précédents rapports GTIR, la finance cède sa place à la grande distribution qui enregistre 22 % des interventions sur incidents (contre 12 % l'année passée) de NTT Com Security. La grande distribution a été particulièrement exposée aux attaques de spear phishing. Parce qu'elles brassent d'importants volumes de données personnelles, dont des informations bancaires, les organisations de ce secteur constituent une cible particulièrement attractive, et ce au point d'enregistrer le plus fort taux d'attaques par client. Le secteur financier a représenté 18 % des interventions.

En 2015, le groupe NTT a également noté une augmentation des attaques à l'encontre du secteur de l'hôtellerie, des loisirs et du divertissement. Tout comme la grande distribution, ce secteur draine aussi de gros volumes d'informations personnelles, y compris des données de cartes bancaires. De même, le niveau relativement élevé des transactions dans le milieu (hôtels, stations touristiques…) suscitent la convoitise des attaquants. Avec sa palette de programmes de fidélité, l'hôtellerie est une vraie mine d'informations personnelles. Plusieurs violations de sécurité ont d'ailleurs défrayé la chronique en 2015 : Hilton, Starwood ou encore Hyatt.



Les attaques par secteur – 2015

Hausse de 17 % des menaces internes

A quels types d'incidents NTT Com Security a-t-il été confronté ? Les violations de sécurité ont représenté 28 % des interventions en 2015, contre 16 % en 2014. Un grand nombre d'incidents concernaient des vols de données et de propriété intellectuelle. Les menaces internes ont connu de leur côté une véritable envolée, passant de seulement 2 % en 2014 à 19 % en 2015. Elles résultent le plus souvent d'une utilisation abusive des données et ressources informatiques par des salariés ou prestataires externes.

En 2015, 17 % des interventions de NTT Com Security se sont produites sur des attaques par spear phishing, alors qu'elles représentaient moins de 2 % auparavant. Basées sur des tactiques sophistiquées d'ingénierie sociale, comme l'utilisation de fausses factures, ces attaques visaient principalement des dirigeants et autres personnels de la fonction comptabilité-finance.

Enfin, le GTIR 2016 a enregistré un recul des attaques DDoS par rapport aux années précédentes. Elles ont reculé de 39 % par rapport à 2014. Le rapport attribue cette baisse aux investissements réalisés dans les outils et services de défense contre ce type d'agression.

A noter cependant une augmentation des cas d'extorsion, où les victimes d'acquittent d'une rançon pour lever les menaces ou stopper une DDos en cours.

Top 10 External Vulnerabilities	
Outdated PHP Version	8%
Cross-Site Scripting (CSS/XSS)	7%
Outdated Apache Web Server	7%
SSL/TLS Information Disclosure	6%
Web Clear Text Username/Password	5%
Weak SSL/TLS Ciphers/Certificate	5%
Outdated Apache Tomcat Server	4%
Weak/No HTTPS cache policy	4%
Cookie without HTTPOnly attribute set	3%
SSL Certificate Signed using Weak Hashing Algorithm	3%

Top 10 Internal Vulnerabilities	
Outdated Java Version	51%
Outdated Adobe Flash Player	11%
Outdated Adobe Reader and Acrobat	5%
Outdated Microsoft Windows	3%
Outdated Microsoft Internet Explorer	3%
Outdated Mozilla Firefox	2%
Outdated Microsoft Office	1%
Outdated Linux Kernel	1%
Outdated Novell Client	1%
Outdated OpenSSH Version	1%

Top 10 des vulnérabilités internes et externes – 2015. Parmi l'ensemble des vulnérabilités externes identifiées, le top 10 compte pour 52 % des cas recensés. Les 48 % restants étaient composés de milliers de vulnérabilités. Parmi l'ensemble des vulnérabilités internes identifiées, le top 10 compte pour 78 % des cas recensés. Ces 10 vulnérabilités internes étaient directement liées à la présence d'applications obsolètes sur les systèmes visés.

Le rapport ici

Article original de Juliette Paoli

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

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

Contactez-nous

Réagissez à cet article

Original de l'article mis en page : Cyberattaques : 77 % des entreprises totalement impuissantes | Solutions Numériques

La Cnil épingle Windows 10 sur la collecte des données personnelles

	La Cnil épingle Windows 10 sur la collecte des données personnelles

Constatant plusieurs manquements dont la collecte de données excessives et non pertinentes par Windows 10, la Cnil a mis en demeure Microsoft de se conformer à la loi dans un délai de 3 mois.

A quelques jours de la fin de la gratuité pour migrer sur Windows 10, la Cnil s'invite dans le débat sur le dernier OS de Microsoft. Et le moins que l'on puisse dire est que le régulateur n'est pas content des méthodes de l'éditeur américain. Elle vient de mettre en demeure Microsoft de se conformer dans un délai de 3 mois à la Loi Informatique et Libertés.

Alertée sur la collecte de données de Windows 10 (dont nous nous étions fait l'écho à plusieurs reprises : « pourquoi Windows 10 est une porte ouverte sur vos données personnelles » ou « Windows 10 même muet il parle encore »), la Cnil a effectué une série de contrôles entre avril et juin 2016 pour vérifier la conformité de Windows 10 à la loi.

De ces contrôles, il ressort plusieurs manquements. Le premier concerne une collecte des données excessives et non pertinentes. Elle reproche par exemple à Microsoft de connaître quelles sont les applications téléchargées et installées par un utilisateur et le temps passé par l'utilisateur sur chacune d'elles. Microsoft s'est toujours défendu de collecter des données personnelles en mettant en avant des relevés de « télémétrie » pour améliorer son produit.

Défaut de sécurité, absence de consentements et référence au Safe Harbor

Autre point soulevé par le régulateur, un défaut de sécurité a été trouvé dans le code PIN à 4 chiffres. Ce dernier est utilisé pour s'authentifier sur l'ensemble des services en ligne. Or le nombre de tentatives de saisie du code PIN n'est pas limité.

De plus, la Cnil constate une absence de consentement des personnes notamment sur le ciblage publicitaire lors de l'installation de Windows 10. Idem pour le dépôt de cookies déposés sur les terminaux des utilisateurs.

Enfin, cerise sur le gâteau, Microsoft est enjoint par la Cnil d'arrêter de se baser sur le Safe Harbor pour transférer les données personnelles aux Etats-Unis. Cet accord a été invalidé par la Cour de Justice de l'Union européenne en octobre 2015. Il a été remplacé par le Privacy Shield qui doit bientôt rentrer en vigueur.

La balle est maintenant dans le camps de Microsoft.

Article original de Jacques Cheminat

Réagissez à cet article

Original de l'article mis en page : La Cnil épingle Windows 10 sur la collecte des données

Trois histoires vrais de vies inquiétées par du piratage informatique ciblé

Trois histoires vrais de vies inquiétées par du piratage informatique ciblé

L'expérience le prouve : même les vieux habitués d'Internet n'arrivent pas toujours à se protéger des piratages ciblés. Étant donné que notre vie quotidienne devient de plus en plus connectée à Internet et à d'autres réseaux, la sécurité en ligne s'est convertie comme un besoin impératif.

La plupart d'entre nous ont un email, un compte sur les réseaux sociaux et une banque en ligne. On commande sur le web, et utilisons notre mobile pour nous connecter à Internet (par exemple, dans les solutions de l'authentification à deux facteurs) et pour d'autres choses tout aussi importantes. Malheureusement, aucun de ces systèmes n'est 100% sûr.
Plus nous interagissons en ligne et plus nous devenons les cibles de hackers sournois. Les spécialistes en sécurité appellent ce phénomène « la surface d'attaque ». Plus la surface est grande et plus l'attaque est facile à réaliser. Si vous jetez un coup d'œil à ces trois histoires qui ont eu lieu ces trois dernières années, vous comprendrez parfaitement le fonctionnement de cette attaque.

1. Comment détourner un compte : faut-il le pirater ou simplement passer un coup de fil ?

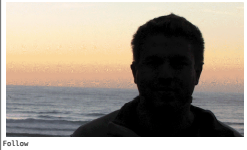
Un des outils les plus puissants utilisés par les hackers est le « piratage humain » ou l'ingénierie sociale. Le 26 février dernier, le rédacteur en chef de Fusion Kevin Roose, a voulu vérifier s'il était aussi puissant qu'il n'y paraissait. Jessica Clark, ingénieure sociale spécialisée en piratage informatique et l'expert en sécurité Dan Tentler ont tout deux accepté ce défi.
Jessica avait parié qu'elle pouvait pirater la boîte mail de Kévin rien qu'avec un email, et sans grande difficulté elle y est arrivé. Tout d'abord, l'équipe de Jessica a dressé un profil de 13 pages qui définissait quel genre d'homme il était, ses goûts, etc, provenant de données collectées de diverses sources publiques.
Après avoir préparé le terrain, Jessica a piraté le numéro mobile de Kévin et appelé sa compagnie de téléphone. Pour rendre la situation encore plus réelle, elle ajouta un fond sonore d'un bébé en train de pleurer.
Jessica se présenta comme étant la femme de Roose. L'excuse inventée par cette dernière fut qu'elle et son « mari » devaient faire un prêt, mais qu'elle avait oublié l'email qu'ils utilisaient en commun, en se faisant passer pour une mère de famille désespérée et fragile. Accompagnée des cris du bébé, Jessica ne mit pas longtemps à convaincre le service technique de réinitialiser le mot de passe du mail et ainsi d'y avoir pleinement accès.
Dan Tentler a accompli cette tâche avec l'aide de l'hameçonnage. Tout d'abord, il avait remarqué que Kevin possédait un blog sur Squarespace et lui envoya un faux email officiel depuis la plateforme, dans lequel les administrateurs de Squarespace demandaient aux utilisateurs de mettre à jour le certificat SSL (Secure Sockets Layer) pour des questions de « sécurité », permettant ainsi à Tentler d'accéder à l'ordinateur de Kévin. Dan créa de nombreux faux pop-up demandant à Roose des informations bien spécifiques et le tour était joué.
Tentler réussit à obtenir l'accès à ses données bancaires, son email, ses identifiants sur les sites web, ainsi que ses données de cartes de crédit, son numéro de sécurité sociale. De l'écran de son ordinateur, il capturait des photos toutes les deux minutes et ce pendant 48h.
View image on Twitter

Follow

Kaspersky Lab
@kaspersky
What is phishing and why should you care? Find outhttps://kas.pr/6bpe #iteducation #itsec
8:05 PM – 11 Dec 2015
•
•
1717 Retweets
•
77 likes

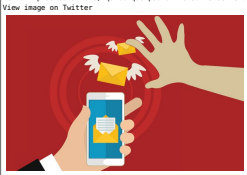
2. Comment détourner de l'argent à un ingénieur informatique en moins d'une nuit

Au printemps 2015, le développeur de logiciels Partap Davis a perdu 3000$. Durant une nuit, en seulement quelques heures, un hacker inconnu a obtenu l'accès de ses comptes mail, son numéro de téléphone et son Twitter. Le coupable a contourné habilement le système de l'authentification à deux facteurs et littéralement vidé le portefeuille des bitcoins de Partap. Comme vous devez sans doute l'imaginer, Davis a passé une mauvaise journée le lendemain.
Il est important de noter que Partap est une pointure concernant l'usage d'Internet : il choisit toujours des mots de passe fiables et ne clique jamais sur des liens malveillants. Son email est protégé avec le système d'authentification à deux facteurs de Google, ce qui veut dire que lorsqu'il se connecte depuis un nouvel ordinateur, il doit taper les six numéros envoyés sur son mobile.



Follow

The Verge
@verge
Anatomy of a hack: a step-by-step account of an overnight digital heist http://www.theverge.com/a/anatomy-of-a-hack …
4:02 PM – 4 Mar 2015
•
•
6969 Retweets
•
7171 likes
Davis gardait ses économies sur trois portefeuilles Bitcoin, protégés par un autre service d'authentification à deux facteurs, conçu par l'application mobile Authy. Même si Davis utilisait toutes ces mesures de sécurité prévoyantes, ça ne l'a pas empêché de se faire pirater.
Suite à cet incident, Davis était très en colère et a passé plusieurs semaines à la recherche du coupable. Il a également contacté et mobilisé des journalistes de The Verge pour l'enquête. Tous ensemble, ils sont parvenus à trouver comment le piratage avait été exécuté. Davis utilisait comme mail principal l'adresse suivante : Patrap@mail. Tous les mails furent envoyés à une adresse Gmail plus difficile à mémoriser (étant donné que Patrap@gmail était déjà utilisé).
Pendant plusieurs mois, quiconque pouvait ensuite se rendre sur la page Hackforum et acheter un script spécial afin d'obtenir les mots de passe qui se trouvaient dans la boite mail. Apparemment, le script était utilisé pour contourner l'authentification à deux facteurs et changer le mot de passe de Davis.
View image on Twitter



Follow

Kaspersky Lab
@kaspersky
Unfortunately two-factor authentication can't save you from#banking Trojans https://kas.pr/S4jV #mobile
4:40 PM – 11 Mar 2016
•
•
2828 Retweets
•
1515 likes
Ensuite, l'hacker a fait une demande de nouveau mot de passe depuis le compte de Davis et demandé au service client de transférer les appels entrants à un numéro de Long Beach (ville en Californie). Une fois le mail de confirmation reçu, le service technique a donné le contrôle des appels à l'hacker. Avec une telle technique, il n'était pas bien difficile de contourner l'authentification à deux facteurs de Google et avoir accès au compte Gmail de Davis.
Pour surmonter cet obstacle, l'hacker a tout simplement réinitialisé l'application sur son téléphone en utilisant une adresse mail.com et une nouvelle confirmation de code, envoyée de nouveau via un appel vocal. Une fois que l'hacker mit la main sur toutes les mesures de sécurité, il changea les mots de passe des portefeuilles Bitcoin de Davis, en utilisant Authy et l'adresse email .com afin de lui détourner de l'argent.
L'argent des deux autres comptes est resté intact, l'un des services interdisant le retrait des fonds 48h après le changement du mot de passe, et l'autre demandant une copie du permis de conduire de Davis, que l'hacker n'avait pas en sa possession.

3. La menace rôde sur nos vies

Comme l'a écrit le journal Fusion en octobre 2015, la vie de la famille Straters s'est retrouvée anéantie à cause d'une pizza. Il y a plusieurs années, des cafés et restaurants locaux se sont installés sur leur arrière-cour, les envahissant de pizzas, tartes et toute sorte de nourriture.
Peu de temps après, des camions de remorquage ont déboulé munis de grandes quantités de sable et de gravier, tout un chantier s'était installé sans aucune autorisation au préalable. Malheureusement, il ne s'agissait que de la partie visible de l'iceberg comparé au cauchemar des trois années suivantes.
Follow

Techmeme @Techmeme
How the Strater family endured 3 years of online harassment, hacked accounts, and swatting http://fusion.net/story/212802/haunted-by-hackers-a-suburban-familys-digital-ghost-story/ …http://www.techmeme.com/151025/p4##a151025p4 …
6:36 PM – 25 Oct 2015

Haunted by hackers: A suburban family's digital ghost story
A suburban Illinois family has had their lives ruined by hackers.
fusion.net
•
•
88 Retweets
•
66 likes
Paul Strater, ingénieur du son pour une chaine de télé locale et sa femme, Amy Strater, ancienne directrice générale d'un hôpital, ont été tout deux victimes d'un hacker inconnu ou de tout un groupe. Il s'avérait que leur fils Blair était en contact avec un groupe de cybercriminels. Les autorités ont reçu des menaces de bombe signées du nom du couple. Les hackers ont utilisé le compte d'Amy pour publier une attaque planifiée dans une école primaire, dans lequel figurait ce commentaire « Je tirerai sur votre école ». La police faisait des visites régulières à leur domicile, n'améliorant en rien les relations du couple avec leur voisinage, qui à force se demandait ce qu'il se passait.
Les hackers ont même réussi à pirater le compte officiel de Tesla Motors et posté un message qui encourageait les fans de la page à appeler les Strater, en échange de gagner une voiture Tesla. Les Strater « croulaient sous les appels téléphoniques », environ cinq par minute, provenant des « admirateurs » de Tesla, désireux de gagner la voiture. Un jour, un homme s'est même présenté au domicile des Strater en demandant aux propriétaires d'ouvrir leur garage, prétendant qu'ils cachaient la Tesla à l'intérieur.
Follow

r00t @rootworx
Again, There is no free car, I did not hack Elon Musk or Tesla's Twitter account. A Finnish child is having fun at your (and my) expense.
12:51 AM – 26 Apr 2015
•
•
1414 Retweets
•
1818 likes
Paul tenta de démanteler le groupe d'hackers en changeant tous les mots de passe de ses comptes et en donnant l'ordre aux patrons des restaurants locaux de ne rien dévoiler sur leur adresse. Il contacta également le Département de Police d'Oswego en leur demandant de vérifier à l'avance si une urgence était bien réelle, avant d'envoyer des renforts. En conséquence de tous ces problèmes, Paul et Amy finirent par divorcer.
Les attaques ont continué par la suite. Les réseaux sociaux d'Amy ont été piratés et utilisés pour publier toute une série de revendications racistes, ce qui a causé la perte de son emploi. Elle fut licenciée malgré avoir dit à ses supérieurs qu'elle et sa famille étaient les victimes de hackers et que leur vie s'était transformée en un véritable cauchemar.
Amy réussit à temps à reprendre le contrôle de son LinkedIn et à supprimer son compte Twitter. Malheureusement, elle était incapable de retrouver un travail dans sa branche à cause de ce qui s'était passé. Elle fut contrainte de travailler chez Uber pour arrondir ses fins de mois, mais disposait de ressources insuffisantes pour payer son loyer.
« Avant, lorsqu'on tapait son nom sur Google, on pouvait voir ses nombreux articles scientifiques et son travail admirable » a déclaré son fils Blair au journal Fusion. « Désormais, on ne voit plus que des hackers, hackers, hackers ».
De nombreuses personnes ont critiqué Blair Strater pour avoir été impliqué lui-même dans de nombreux réseaux de cybercriminels, où il n'arrivait pas à se faire d'amis. Dans le cas précis de la famille Strater, les parents de Blair ont payé pour les « crimes » de leur fils, alors qu'eux n'avaient absolument rien à voir avec les hackers.
Article original de Kate Kochetkova

Denis JACOPINI ne peut que vous recommander d'être prudent.
Si vous désirez être sensibilisé aux risques d'arnaques et de piratages afin d'en être protégés, n'hésitez pas à nous contacter, nous pouvons animer conférences, formations auprès des équipes dirigeantes et opérationnelles.
La sécurité informatique et la sécurité de vos données est plus devenu une affaire de Qualité (QSE) plutôt qu'un problème traité par des informaticiens.
Vous souhaitez être aidé ? Contactez-nous

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

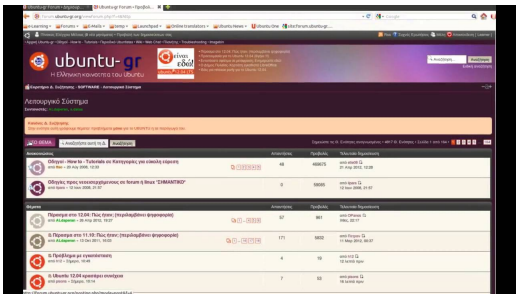
Le Net Expert INFORMATIQUE
Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Original de l’article mis en page : Comment pirater, détourner de l’argent et rendre la vie de quelqu’un impossible sur Internet : trois histoires inquiétantes de piratages ciblés. | Nous utilisons les mots pour sauver le monde | Le blog officiel de Kaspersky Lab en français.

Deux millions de données d’utilisateurs Ubuntu dérobées



Deux millions de données d’utilisateurs Ubuntu dérobées

Le forum de la distribution Ubuntu a été victime d'une grave attaque informatique. Deux millions d'utilisateurs se sont fait voler leurs données.

Le butin du pirate est plus qu'impressionnant. Noms, mots de passe, adresse mails et IP, les données de deux millions d'utilisateurs du forum d'Ubuntu se sont envolées. La nouvelle a été annoncée jeudi dans un communiqué par Canonical l'éditeur d'Ubuntu. *« A 20h33 UTC le 14 Juillet 2016, Canonical et l'équipe ont été informés par un membre du Conseil Ubuntu que quelqu'un prétendait avoir une copie de la base de données des forums. Après enquête initiale, nous avons été en mesure de confirmer qu'il y avait bien eu une exposition des données et nous avons fermé les forums par mesure de précaution. »*

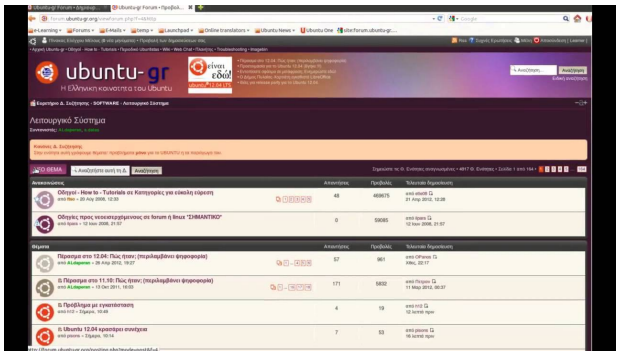
Une attaque par injection SQL

Une enquête plus poussée a révélé que la méthode employée est une injection SQL. Le pirate a pu injecter des requêtes SQL formatées dans la base de données des forums pour ensuite télécharger les datas.

Cependant, le communiqué précise que le hacker n'a pas pu accéder aux mots de passe utilisateur valides ni au référentiel de code Ubuntu ou au mécanisme de mise à jour. Moins certain, le rapport précise que normalement les services Canonical ou Ubuntu en sortent indemnes, comme certains forums.

Tout est plus ou moins rentré dans l'ordre

Des mesures correctives ont été prises et les forums restaurés. Les mots de passe du système et de la base de données ont été réinitialisés et ModSecurity, une Web Application Firewall vient renforcer le dispositif de sécurité. Selon Canonical, ça va mieux, même si après ce genre de vol il est légitime de penser que le mal est fait.



Article original de Victor Miget

Réagissez à cet article

Original de l'article mis en page : Ubuntu : les données de

deux millions d’utilisateurs dérobées