Un utilisateur de Yahoo! poursuit le groupe pour « négligence »

	Un utilisateur de Yahoo! poursuit le groupe pour « négligence »

Le plaignant regrette que les mesures de sécurité du groupe n'aient pas été renforcées. Il s'autoproclame représentant des utilisateurs lésés par le vol de données.

Après l'annonce, jeudi 22 septembre, du piratage d'au moins 500 millions de comptes d'utilisateurs de Yahoo!, le groupe est désormais poursuivi pour « *négligence grave* » à la suite de la plainte d'un utilisateur. Le groupe de Sunnyvale (Californie) fait face à un certain nombre de questions relatives à sa gestion de l'incident.
La plainte a été déposée vendredi auprès du tribunal fédéral de San Jose (Californie), par Ronald Schwartz, un résident de New York qui entend représenter tous les utilisateurs américains de Yahoo! affectés par le vol de leurs informations personnelles.
L'opérateur de services Internet a annoncé, la veille, que les données volées pourraient inclure des noms, des adresses emails, des numéros de téléphone, des dates de naissance et des mots de passe cryptés. Il a exclu à ce stade le vol de données bancaires dans ce qu'il présente comme une attaque menée par un « *agent piloté par un Etat* », sans apporter de preuve de cette hypothèse. L'action en justice vise le statut de recours collectif (« *class action* ») et entend réclamer des dommages et intérêts.
Selon le plaignant, le piratage aurait pu être évité si le groupe avait renforcé ses mesures de sécurité après plusieurs précédentes tentatives d'effraction. Il déplore également la lenteur de Yahoo!, qui aurait, selon lui, mis trois fois plus de temps que ses concurrents pour faire état du piratage…[lire la suite]

Denis Jacopini anime des **conférences et des formations** et est régulièrement invité à des **tables rondes en France et à l'étranger** pour sensibiliser les décideurs et les utilisateurs aux **CyberRisques** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Nous animons **conférences et formations** pour sensibiliser décideurs et utilisateurs **aux risques en informatique**, découvrir et comprendre les **arnaques** et les **piratages informatiques** pour mieux s'en protéger et se **mettre en conformité avec la CNIL** en matière de **Protection des Données Personnelles**. Nos actions peuvent être personnalisées et organisées dans votre établissement.
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

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 : Piratage massif : Yahoo!

poursuivi pour « négligence » par un utilisateur

Le site de la Gironde infiltré par des pirates informatiques

Le site de la Gironde infiltré par des pirates informatiques

Des pirates informatiques s'infiltrent et installent des pages malveillantes sur le site du Département de la Gironde. Un espace dédié aux personnes handicapées.

Un piratage classique, malheureusement, mais qui démontre que même face à des internautes à la culture et au savoir informatiques faibles, les dégâts peuvent être importants. Le site du Département de la Gironde en est un parfait exemple. Il est pris pour une grande cours de récréation par des « pirates ». Pour preuve, la page « Troll » John Cena n'est pas l'unique passage malveillant que j'ai pu constater. D'autres pages ont été cachées, en ce mois de septembre, par des pirates informatiques différents [SirXL3 aka Kartz], avec plus ou moins de réussite. Les archives Zone H rappellent aussi que ce même site web avait été maltraité en avril 2016 par un barbouilleur baptisé Sneaky. En avril 2015, je vous expliquais comment d'autres malveillants du numérique s'étaient invités dans le site de l'association des maires de la Gironde…[lire l'article complet]

Denis Jacopini anime des **conférences et des formations** et est régulièrement invité à des **tables rondes en France et à l'étranger** pour sensibiliser les décideurs et les utilisateurs aux **CyberRisques** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Nous animons **conférences et formations** pour sensibiliser décideurs et utilisateurs **aux risques en informatique**, découvrir et comprendre les **arnaques** et les **piratages informatiques** pour mieux s'en protéger et se **mettre en conformité avec la CNIL** en matière de **Protection des Données Personnelles**. Nos actions peuvent être personnalisées et organisées dans votre établissement.
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

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 : ZATAZ Le site Culture Accessible de la Gironde infiltré par des pirates informatiques – ZATAZ

Alerte : Un canular sur Facebook qui diffuse de fausses informations terroristes

	Alerte : Un canular sur Facebook qui diffuse de fausses informations terroristes

Les chercheurs ESET ont découvert une arnaque qui cible les utilisateurs de Facebook. D'abord répandu en République Tchèque et en Slovaquie, elle pourrait se propager dans d'autres pays

Les utilisateurs de Facebook en République Tchèque et en Slovaquie font face à une vague de fausses informations sur une attaque meurtrière à Prague. Quand l'utilisateur clique sur le canular, il est redirigé vers une page Internet de phishing qui essaye de le tromper en l'incitant à partager ses identifiants Facebook.

« D'après ce que nous savons à propos de cette campagne, l'attaque pourrait se propager dans plusieurs autres pays » met en garde Lukáš Štefanko, Malware Researcher chez ESET.

Cette prétendue attaque terroriste est facile à discréditer car la photo publiée ne ressemble pas à Prague, ni à aucune autre ville d'Europe. Malgré cela, l'arnaque se diffuse rapidement. « Les utilisateurs de Facebook partagent fréquemment des histoires sans les avoir lues. Les campagnes d'arnaques, si elles font appel à l'émotion, réussissent étonnamment bien à cause de notre empathie naturelle » commente Lukáš Štefanko.

Peu après le lancement de la campagne, Facebook a commencé à stopper les pages de phishing utilisées dans cette campagne. Les solutions de sécurité ESET sont conçues pour bloquer les pages Internet de phishing liées à ce type d'escroquerie ainsi que d'autres domaines enregistrés par cette même personne.

« Au cours des dernières semaines, il y a eu 84 domaines enregistrés par la même personne. La plupart d'entre eux possède une fonction de phishing, tandis que d'autres pourraient être utilisées à l'avenir lors d'une attaque à plus grande échelle » ajoute Lukáš Štefanko.

Voici les recommandations des experts ESET pour ceux qui pensent avoir été escroqué en partageant leurs identifiants Facebook :

– Changez votre mot de passe Facebook et utilisez les deux facteurs d'authentification fournis par Facebook

– Si vous avez utilisé le même mot de passe pour plusieurs services, changez-le partout – et mettez un terme à cette pratique très dangereuse.

Denis JACOPINI vous recommande les outils de protection suivants :

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.

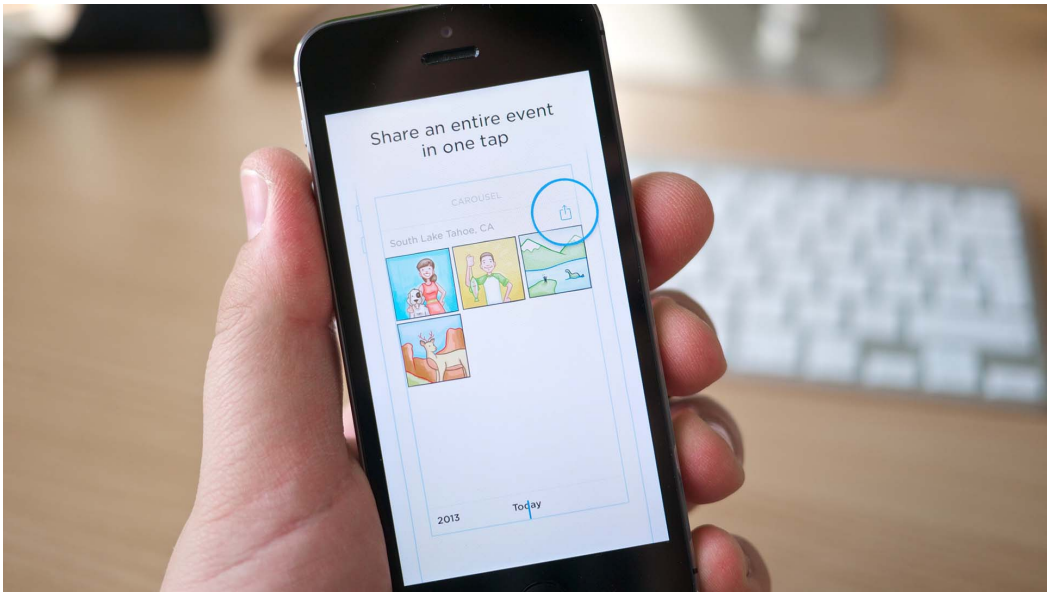
Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Original de l’article mis en page : Boîte de réception – denis.jacopini@gmail.com – Gmail

68 millions de comptes Dropbox piratés



68 millions de comptes Dropbox piratés

Quatre ans avoir avoir été victime d'un piratage et avoir su qu'il avait donné accès à une liste d'adresses e-mail, Dropbox a décidé il y a quelques jours de réinitialiser les mots de passe. Mais ce n'est qu'aujourd'hui que l'on en découvre l'ampleur.

La semaine dernière, Dropbox annonçait la réinitialisation de mots de passe d'utilisateurs inscrits depuis au moins 2012, en expliquant avoir été informé du fait qu'une base de données piratée à l'époque circulait, dans laquelle des adresses e-mails et des mots de passe hashés figurent. Dropbox avait prévenu dès 2012 qu'il avait été victime d'un tel piratage dû au vol d'un mot de passe d'un employé, et que les adresses e-mails obtenues avaient été utilisées pour envoyer des spams.

DROPBOX A MIS QUATRE ANS À RÉAGIR

Rien ne permet de penser que des mots de passe ont pu être déchiffrés. En revanche si vous utilisez le même mot de passe sur Dropbox que sur d'autres services en ligne, et si ces services ont eux-aussi été piratés, il est possible d'accéder à votre Dropbox en utilisant le mot de passe obtenu ailleurs. En 2012, le service en ligne avait d'ailleurs indiqué que des accès frauduleux avaient été faits par cette méthode, neutralisée lorsque l'on active la validation en deux étapes.

Dès lors, on ne comprend pas pourquoi Dropbox a attendu quatre ans (!) avant de réinitialiser les mots de passe.

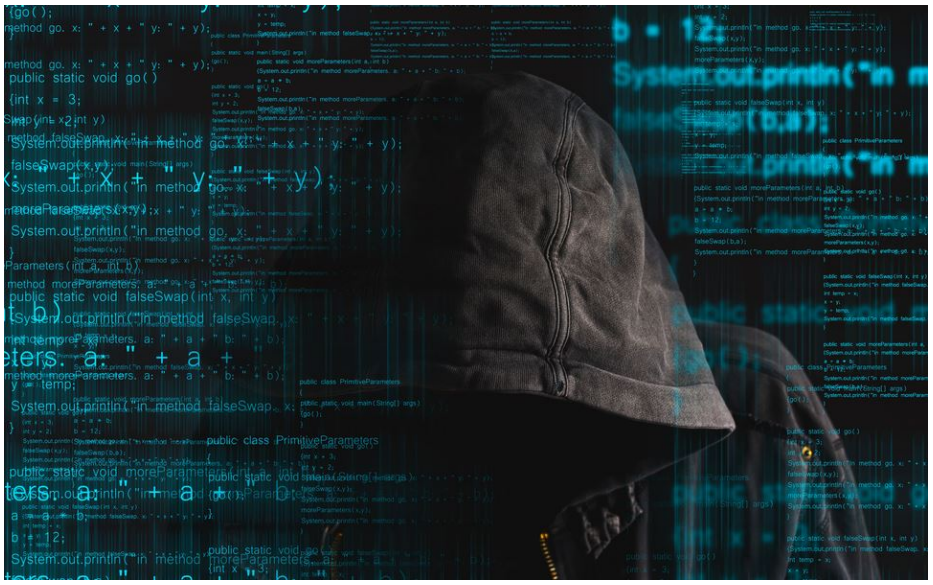
Ce piratage dont la base de données resurgit après plusieurs années est le dernier en date d'une série similaire, qui fait penser qu'il pourrait s'agir du même groupe, ou de mêmes failles ont pu être exploitées à l'époque. Ainsi ces derniers mois on a appris la diffusion de 171 millions de mots de passe VK (le Facebook russe),427 millions de comptes Myspace,167 millions de mots de passe LinkedIn ou encore 32 millions de mots de passe Twitter.

Article original de Guillaume Champeau

Réagissez à cet article

Original de l'article mis en page : Une base de 68 millions de comptes Dropbox circule chez les pirates — Tech — Numerama

Un cousin du malware Furtim cible les énergéticiens européens



Un cousin du malware Furtim cible les énergéticiens européens

SentinelOne a découvert une variante du malware Furtim qui vise les sociétés européennes dans le domaine de l'énergie.

En mai dernier, des chercheurs la société EnSilo ont découvert un malware baptisé Furtim qui devait son nom à une obsession virant à la paranoïa de ne pas être détecté par les outils de sécurité. De la préparation à son installation jusqu'à son implémentation, le malware scrute, analyse et bloque tout ce qui touche de près ou de loin à la sécurité IT.

Il semble que ce malware revienne sous une autre forme pour s'attaquer au système industriel des entreprises énergétiques européennes. Des chercheurs de SentinelOne l'ont détecté au sein du réseau d'un énergéticien européen. Cette menace a un nom, SFG, et a été trouvée à la fois par une remontée d'information des logiciels de SentinelOne, mais aussi sur des forums privés. Les experts ont travaillé sur les échantillons pour comprendre son fonctionnement. Les résultats de cette analyse montrent que le comportement, la sophistication et la furtivité du malware sont l'œuvre d'un Etat ou pour le moins d'une organisation soutenue par un gouvernement. Les experts penchent pour une initiative provenant de l'Europe de l'Est.

Jusqu'au sabotage du réseau énergétique

Dans le détail, le cousin de Furtim s'appuie sur les mêmes exploits pour éviter d'être repéré par les outils de sécurité (antivirus, firewall next gen, solution endpoint, sandboxing). Plusieurs développeurs de haut niveau ont mis la main à la pâte pour perfectionner SFG. L'objectif est multiple, extraire des données ou faire tomber le réseau d'énergie, sans laisser de traces. Le malware affecte toutes les versions de Windows, précise SentinelOne dans un blog. Il situe ses débuts au mois de mai dernier et il est encore actif.

Ce n'est pas la première fois que les entreprises énergétiques sont visées par des malwares ayant pour ambition le sabotage du réseau. On pense bien évidemment au premier virus qui visait les SCADA, Stuxnet. Mais plus récemment, l'Ukraine a été victime d'une panne de courant provoquée par une cyberattaque s'appuyant sur le malware Blackenergy. Ce type de menaces est pris très au sérieux par les gouvernements au point de forcer les entreprises à remonter leurs niveaux de sécurité. En France, l'ANSSI peaufine les arrêtés sectoriels sur la sécurité des OIV (opérateurs d'importance vitale) notamment dans le domaine de l'énergie.

Article original de Jacques Cheminat

Réagissez à cet article

Original de l'article mis en page : Malware : un cousin de Furtim cible les énergéticiens européens

Un concessionnaire Lamborghini de Mulhouse piraté

Un concessionnaire Lamborghini de Mulhouse piraté

Le vol de données peut souvent cacher des arnaques et attaques informatiques plus vicieuses encore. Exemple avec le piratage d'un concessionnaire de Lamborghini de l'Est de la France.

Derrière un piratage informatique, 99 fois sur 100, se cache le vol des données que le malveillant à pu rencontrer dans son infiltration. Des données qui se retrouvent, dans l'heure, quand ce n'est pas dans les minutes qui suivent la pénétration du site dans des forums et autres boutiques dédiés à l'achat et revente d'informations subtilisées.Un concessionnaire de Lamborghini, à Mulhouse, vient d'en faire les frais.

Une fois les contenus dérobés exploités (phishing, escroqueries…) le pirate s'en débarrasse en les diffusant sur la toile. C'est ce qui vient d'arriver à un concessionnaire automobile de l'Est de la France. Ici, nous ne parlons pas de la voiture de monsieur et madame tout le monde, mais de Lamborghini.

Prend son site web par dessus la jambe et finir piraté !

Le concessionnaire se retrouve avec l'ensemble des pousses bouton de la planète aux fesses. De petits pirates en mal de reconnaissance qui profitent d'une idiote injection SQL aussi grosse que l'ego surdimensionné de ces « piratins ». Bilan, le premier pirate a vidé le site, revendu/exploité les données. Il a ensuite tout balancé sur la toile. Les « suiveurs » se sont jetés sur la faille et les données. J'ai pu constater des identifiants de connexion (logins, mots de passe) ou encore des adresses électroniques lâchées en pâture. Des courriels internes (webmaster, responsables du site…).

Article original de Damien Bancal

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 : ZATAZ Un concessionnaire Lamborghini de Mulhouse piraté – ZATAZ

Nouvelle forme d’attaque informatique, les crypto-vers

Nouvelle forme d’#attaque informatique, les crypto-vers

Les cybercriminels ont trouvé une nouvelle manière de se faire de l'argent. Cela faisait longtemps qu'ils tentaient de prendre en otage des disques durs, mais les gens sont devenus plus vigilants et n'ouvrent plus n'importe quelle pièce jointe à un mail. Voilà pourquoi les cybercriminels se sont vu contraints d'inventer une nouvelle façon d'installer leur rançongiciel (#ransomware). Leur solution: le ver.

Le spécialiste de la sécurité Kaspersky lance donc une mise en garde. Le 'crypto-ver' est « une forme mixte dangereuse de maliciel (malware) et de rançongiciel qui se répand d'elle-même ». Elle peut se propager d'ordinateur à ordinateur, sans spam (pourriel) ou autre infection. Le malware se duplique simplement dans les appareils interconnectés.
Le premier ver, baptisé SamSam, s'est manifesté en avril. Et au cours des dernières semaines, des experts en sécurité ont découvert le ver ZCryptor. Ce dernier se présente sous la forme d'une simple mise à jour d'un programme largement utilisé tel Flash. Une fois en place, le ver commence à se propager, puis il crypte des dizaines d'extensions. Les victimes voient ensuite apparaître leur écran habituel, qui les informe que leurs fichiers ont été pris en otage et qu'ils doivent verser une rançon pour pouvoir y accéder de nouveau.
Les spécialistes des la sécurité n'ont pas encore trouvé une parade contre ZCryptor. Voilà pourquoi Kaspersky prodigue le conseil suivant: soyez sur vos gardes, veillez à disposer d'une bonne protection et effectuez régulièrement des sauvegardes (backups).

Réagissez à cet article

Original de l'article mis en page : Nouveau: le ver ravisseur – ICT actualité – Data News.be

Des caméras de surveillance piratées pour mener des attaques DDoS

	Des caméras de surveillance piratées pour mener des attaques DDoS

Tous ceux qui refusent d'admettre que l'Internet des Objets pourrait être à l'origine de nombreuses menaces dans la sphère informatique de demain vont probablement avoir du mal à tenir leur position après l'affaire présentée ici. En effet, des hackers ont utilisé un réseau de 25 000 caméras de surveillance piratées pour conduire des attaques DDoS.

Des caméras de surveillance piratées pour former un botnet

Il y a quelques heures, l'entreprise Sucuri, spécialisée dans la sécurité informatique, a découvert que des hackers avaient réussi à prendre le contrôle de quelques 25 000 caméras de surveillance présentes au quatre coins de la planète.

Mais l'objectif des pirates n'était pas que de récupérer des images ou d'espionner des individus puisqu'ils ont utilisé les caméras de surveillance pour créer un botnet, autrement dit un réseau de machines contrôlées à distance par un seul et même individu.

Capables d'agir ensemble, les 25 000 caméras ont ainsi pu être à l'origine d'attaques DDoS contre plusieurs sites Internet. En effet, les hackers se sont servis du réseau de caméras de surveillance pour envoyer des requêtes simultanées sur des sites causant ainsi leur paralysie pendant de longues minutes.

Une preuve supplémentaire de la menace que laissent planer les objets connectés

Si l'utilisation d'objets connectés par les pirates pour mener des attaques DDoS est tout sauf une nouveauté, c'est l'ampleur de l'attaque qui surprend. En effet, même les spécialistes sont restés « coi » devant la capacité d'un réseau de 25 000 caméras de surveillance à générer autant de requêtes simultanément.

L'autre surprise tient au fait que les caméras piratées sont dispatchées aux quatre coins de la planète. 2% seraient d'ailleurs basées en France alors que c'est aux Etats-Unis, en Indonésie et à Taïwan que la majorité d'entre elles se situerait.

Sucuri a d'ailleurs cherché à comprendre ce que pouvait avoir en commun l'ensemble de ces appareils et la piste la plus sérieuse mène à BustyBox, un système qui serait intégré à tous. Or, une importante faille avait été découverte au printemps dans celui-ci ce qui aurait pu permettre à des pirates de l'exploiter pour commettre leurs actions.

Affaire à suivre…

Article original de Jérôme DAJOUX

Réagissez à cet article

Original de l’article mis en page : Des caméras de surveillance piratées pour mener des attaques DDoS

Alerte nouveau ransomware : Le Javascript RAA est diffusé par spams

Alerte nouveau ransomware : Le Javascript RAA est diffusé par spams

---

Le ransomware RAA se propage à grande vitesse en Russie par le biais de campagnes de spams. Il prend la forme d'une pièce jointe en Javascript.

RAA, un ransomware entièrement écrit en Javascript

Si la plupart des logiciels malveillants qui ciblent des machines Windows est écrite en C++, voilà que RAA surprend puisque lui est intégralement écrit en Javascript, un langage destiné principalement à être interprété par les navigateurs web.

Pour les cybercriminels, le choix de ce langage n'est pas dû au hasard étant donné qu'ils tentent d'infecter les machines à distance via la diffusion de spams. Toutefois, tout utilisateur doit normalement agir avec méfiance avec les pièces jointes, d'autant plus si celles-ci sont dans un format Javascript. En effet, ce format doit inciter les utilisateurs à mettre le mail dans leur corbeille et surtout à ne pas ouvrir la pièce jointe.

Si tel est le cas, RAA peut faire des ravages puisqu'il est conçu pour chiffrer les documents disposant des extensions .doc, .xls, .rtf, .pdf, .dbf, .jpg, .dwg, .cdr, .psd, .cd, .mdb, .png, .lcd, .zip, .rar et .csv comme le révèlent nos confrères du Monde Informatique.

Autant dire donc que le téléchargement de la pièce jointe n'est pas sans conséquences.

Pas de vaccin disponible pour déchiffrer les contenus

S'il existe parfois des vaccins contre les ransomwares, RAA n'a pas encore le sien si bien qu'une fois vos fichiers chiffrés, vous n'aurez aucune autre alternative que payer la rançon si vous voulez débloquer de nouveau l'accès à vos documents.

Pour l'heure, ce rançongiciel se propage principalement en Russie puisqu'il semble que c'est depuis ce pays qu'opèrent les cybercriminels. Toutefois, il y a fort à parier que la diffusion de RAA va s'étendre dans les prochains mois et qu'une version « internationale » du rançongiciel sera développée par ces spécialistes du genre.

Article original de Fabrice Dupuis

Réagissez à cet article

Original de l’article mis en page : RAA : un nouveau ransomware diffusé par spams

---

32 millions de mots de passe Twitter dérobés

	**32 millions de mots de passe Twitter dérobés**

Après LinkedIn, MySpace et Tumblr, Twitter a lui aussi été victime d'un piratage massif. 32,8 millions de comptes seraient affectés.

Une nouvelle fuite de données pour un réseau social. Un hacker russe affirme avoir dérobé 379 millions d'adresses email et de mots de passe non chiffrés associés à des comptes Twitter. Identifié sous le pseudonyme Tessa88, il aurait mis en vente la base de données en question sur VK, le Facebook russe. LeakedSource, qui a révélé l'information, estime que 32,8 millions de comptes seraient effectivement compromis, une fois les doublons éliminés.

«Nous sommes convaincus que ces noms d'utilisateurs et les identifiants n'ont pas été obtenus par une violation des données Twitter. Nos systèmes n'ont pas été hackés», a déclaré un porte-parole de Twitter. La base de données serait donc le fruit d'une campagne de malware ciblant les particuliers pour récupérer leurs mots de passe.

Sollicité par Techcrunch, Troy Hunt, le fondateur de site haveibeenpwned.com qui permet de voir si une adresse mail fait partie d'une base de données piratée, émet des doutes par rapport à l'authenticité des données piratées: «Les piratages de comptes que nous avons vus jusqu'à présent sont très probablement le résultat de la réutilisation de données issues d'autres piratages», indique-t-il.

Une incitation de plus à modifier son mot de passe

Si Leakedsource propose de vérifier si vos identifiants et mots de passe sont dans leur base et de les retirer gratuitement, le plus simple reste encore de modifier son mot de passe.

Twitter a suggéré au passage de le complexifier, en suivant ses recommandations.

7 Juin

Twitter Support
@Support
To help keep people safe and accounts protected, we've been checking our data against what's been shared from recent password leaks.
Suivre

Twitter Support
@Support
Any time is a good time to make sure your account is secure, starting w[illegible] an updated password. More tipshttps://support.twitter.com/articles/76036
00:36 – 7 Juin 2016

Safe Tweeting: the basics
Keeping your account secure We want Twitter to be a safe and open community. This help page provides some information and tips to help you practice safe Tweeting and keep your acco
support.twitter.com
•
•
128128 Retweets
•
170170 j'aime

Selon la liste des données divulguées, bien trop de ***mots de passe*** *restent basiques et facilement trouvables. 123455 prend la première place du podium, suivi de 123456789, qwerty et du classique password.*
Ce piratage suit celui de MySpace, de Tumblr et de LinkedIn. ***100 millions de mots de passe*** *du réseau professionnel récupérés en 2012 ont été mis en vente mi-mai. Ce piratage avait valu à Mark Zuckerberg, adepte du mot de passe unique «dadada», de* ***voir ses comptes Twitter et Pinterest piratés****.*
Article original

Réagissez à cet article

Original de l’article mis en page : Un hacker russe prétend avoir dérobé des millions de mots de passe Twitter