Attention, le navigateur Maxhton espionne ses utilisateurs !

Attention, le navigateur Maxhton espionne ses utilisateurs !

Le navigateur Maxhton ne serait rien d'autre qu'un outil d'espionnage à la solde de la Chine ?

Des experts en sécurité informatiques de l'entreprise polonaise Exatel viennent de révéler la découverte de faits troublant visant le navigateur *Maxhton*. Ce butineur web recueille des informations sensibles appartenant à ses utilisateurs. Des informations qui sont ensuite envoyées à un serveur basé en Chine. Les chercheurs avertissent que les données récoltées pourraient être très précieuses pour des malveillants.

Les données des utilisateurs de Maxhton envoyées en Chine !
Et pour cause ! Les ingénieurs de *Fidelis Cybersecurity* et *Exatel* ont découvert que Maxthon communiquait régulièrement un fichier nommé ueipdata.zip. Le dossier compressé est envoyé en Chine, sur un serveur basé à Beijing, via HTTP. Une analyse plus poussée a révélé que ueipdata.zip contient un fichier crypté nommé dat.txt. Dat.txt stocke des données sur le système d'exploitation, le CPU, le statut ad blocker, l'URL utilisé dans la page d'accueil, les sites web visités par l'utilisateur (y compris les recherches en ligne), et les applications installées et leur numéro de version.
En 2013, après la révélation du cyber espionnage de masse de la NSA, Maxhton se vantait de mettre l'accent sur la vie privée, la sécurité, et l'utilisation d'un cryptage fort pour protéger ses utilisateurs. (Merci à I.Poireau)
Article original de Damien Bancal

Réagissez à cet article

Original de l’article mis en page : ZATAZ Le navigateur Maxhton espionne ses utilisateurs – ZATAZ

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

Réagissez à cet article

Original de l'article mis en page : ZATAZ Un concessionnaire Lamborghini de Mulhouse piraté – ZATAZ

La fraude au Président n’arrive pas qu’aux autres

La fraude au Président n’arrive pas qu’aux autres

Des millions d'euros envolés dans une escroquerie aux faux virements bancaires. Une entreprise Dunkerquoise découvre qu'elle vient de perdre plus de neuf millions d'euros dans la manipulation de ses informations bancaires.

Qu'ils sont fatigants ces gens qui savent toujours tout. Il y a quelques semaines, lors d'une conférence que m'avait demandé une collectivité locale, un responsable d'un bailleur social m'expliquait qu'il ne fallait pas trop exagérer sur les risques de piratage informatique, de fuites de données… J'expliquais alors comment des malveillants s'attaquaient aussi aux locataires de logements sociaux. Le monsieur expliquait alors, pour conforter ses dires « ***depuis que j'ai un antivirus et le firewall incorporé*** […] ***je n'ai plus jamais eu d'ennui avec mon ordinateur portable***« . Le monsieur travaillait pour un bailleur social de la région de Dunkerque (Nord de la France – 59). Et c'est justement à Dunkerque, chez un bailleur social, *Le Cottage social des Flandres*, qu'une nouvelle affaire de fraude au président vient de toucher la banlieue de la cité de Jean-Bart. Une manipulation des informations bancaires qui coûte 25% du chiffre d'affaires de la victime.

23 versements de 400.000 euros

Alors, cela n'arrive qu'aux autres ? L'entreprise Dunkerquoise n'est pas une structure à la Nestlé, Michelin, Total, Le Printemps. 140 employés, 6.000 locataires et un quelques 40 millions d'euros de chiffre d'affaires. Bref, une petite entreprise comme il en existe des dizaines de milliers en France. Le genre d'entité économique qui pense que les pirates informatiques, les escrocs ne s'intéresseront pas à elles. Erreur grave ! Pour *Le Cottage social des Flandres*, les professionnels de la Fraude au Président, la fraude au FoVI, se repartis avec 23 virements de plus de 400.000 euros. Bilan, 9,8 millions d'euros envolés dans les caisses d'une banque basée en Slovaquie. Autant dire que revoir l'argent revenir à la maison est peine perdue. D'autant plus que la fraude a couru du 7 avril au 23 mai. Piratage qui n'aura été découvert qu'un mois plus tard, au départ en vacances d'un dès comptable. Bref, en manquement évident de sérieux, et cela dans toutes les strates stratégiques de l'entreprise. Surtout à la lecture de la Voix du Nord : un responsable explique que l'arnaque était tellement bien montée que la société n'y a vu que du feu, et plus grave encore « ***On a les reins solides, on va pouvoir faire face***. » Après tout, 9,8 millions d'euros « ne » représente que 25% du CA de cette société (Sic !).

Méthode rodée mais simple à contrer

Un exploit que cette fraude ? Les adeptes du social engineering (l'étude de l'environnement d'une cible avant de s'attaquer à son univers informatique) savent très bien que non. Dans l'affaire Dunkerquoise, un compte mail piraté aurait permis le début de cette fraude au président. Détail troublant, les courriels arrivaient ailleurs que sur une adresse type adresse@Cottages.fr ? Car si piratage il y a eu, c'est l'ensemble des services couplés au domaine qui ont pu être corrompu. A moins que le responsable usurpé utilisait un gMail, Yahoo! ou tout autre compte webmail. Toujours est-il que le pirate a mis la main sur une adresse officielle et a pu ainsi manipuler les employés.

Parce que pour éviter un FoVI, c'est aussi simple que de protéger son argent personnel, normal. C'est d'ailleurs très certainement là où le bât blesse. Ce n'est pas mon argent, donc j'en prends soin, mais pas trop. Penser que cela n'arrive qu'aux autres est une grande erreur. Éduquer vos personnels, éduquez-vous, patrons, dirigeants…

Pour éviter un FoVI, contrôler ses informations bancaires

N'autoriser le transfert d'argent qu'après applications de mesures décidées en interne, et quelle que soit l'urgence de la demande de manipulation des informations bancaires. D'abord, la somme d'argent. Plafonner le montant. Si ce montant dépasse le chiffre convenu, obligation d'en référer à la hiérarchie. Un élément qui doit obligatoirement faire « tiquer » dans les bureaux : la demande d'un second transfert, d'une nouvelle modification des Le mot-clé principal « informations bancaires » n'apparait pas dans le titre SEO de la page par la même personne, même entité, doit également être indiquée à la hiérarchie. « ***Paulo, c'est normal de faire 23 versements de 400.000 euros en 2 mois ?*** » – « ***Oui ! Le boss achète des chouquettes en Slovénie. Il me l'a dit par mail !***« . La validation de transfert doit se faire par, au moins, deux personnes différentes, dont un supérieur hiérarchique.

Article original de Damien Bancal

Réagissez à cet article

Original de l'article mis en page : ZATAZ Informations bancaires : la fraude au Président n'arrive pas qu'aux autres – ZATAZ

Le site de rencontres adultères Ashley Madison menaçait de briser l'anonymat de ses clients

Le site de rencontres adultères Ashley Madison menaçait de briser l'anonymat de ses clients

En cas de factures impayées, les utilisateurs du portail de rencontres avaient droit à des courriers menaçants.

Le géant canadien Ashley Madison admet avoir fait du chantage aux mauvais payeurs, révèle le site CNNMoney. L'information vient directement d'Avid Life Media, groupe propriétaire du site de rencontres adultères. Le média américain avait dans un premier temps mis la main sur des échanges entre un ancien membre et le service client du site. L'affaire remonte à 2012. L'homme en question – qui a souhaité rester anonyme – explique avoir acheté pour 40 dollars de crédits après avoir reçu une douzaine de messages de femmes. Une fois l'argent dépensé, il n'a jamais reçu la moindre réponse de ces dernières.

Sur le Web, il a rapidement découvert d'autres plaintes similaires à la sienne. Les clients suspectaient alors Ashley Madison d'avoir recours à de faux profils féminins pour les inciter à la dépense. Après avoir demandé à être remboursé, l'homme a reçu une réponse plutôt ferme: "Si vous rejetez le débit, tous les enregistrements seront envoyés à votre domicile". Sur les forums, d'autres utilisateurs ont témoigné de ce type de chantage, en étant parfois menacés d'appels téléphoniques à leur domicile.

La porte-parole du site a confirmé à CNNMoney que ces pratiques avaient cessé avec la prise de fonction de Rob Segal, le nouveau PDG, soit il y a seulement trois mois. Les suspicions du jeune homme se sont par ailleurs révélées fondées. L'an dernier, le piratage d'Ashley Madison révélait que la majorité des profils féminins étaient des faux. Il y a quelques jours, les nouveaux dirigeants du site ont admis l'utilisation de robots pour attirer les hommes. Une pratique qui appartiendrait au passé, selon eux, mais qui vient d'aboutir à l'ouverture d'une enquête de la part de la Commision fédérale du commerce aux Etats-Unis.

Article original de Raphaël GRABLY

Réagissez à cet article

Original de l’article mis en page : Le site de rencontres adultères Ashley Madison menaçait de briser l’anonymat de ses clients

---

Découvrez le TOP 5 des arnaques informatiques les plus récurrentes au premier trimestre 2016 selon la PLCC

Découvrez le TOP 5 des arnaques informatiques les plus récurrentes au premier trimestre 2016 selon la PLCC

En Côte d'Ivoire, les préjudices financiers causés par les cybercriminels se chiffrent en milliards. Dans sa stratégie de sensibilisation, la Plateforme de Lutte Contre la Cybercriminalité (PLCC) entreprend d'informer les populations sur les arnaques les plus récurrentes afin de leur permettre de ne pas tomber dans le piège.

Selon les chiffres communiqués par la PLCC, au cours de l'année 2015, le préjudice financier causé par la cybercriminalité a atteint 3 980 833 802 FCFA, contre **5 280 000 FCFA** en 2015. Ce sont **1 409** plaintes qui ont été enregistrées. Elles ont abouti à l'arrestation de **205** individus, dont **159** ont été déférés au parquet. Afin d'informer davantage les populations, la PLCC a sorti les 5 types arnaques qui ont été les plus récurrentes au cours du premier trimestre 2016.

1- La Sextorsion (Enregistrement illégal de communication privée, chantage à la vidéo)

Ce type d'arnaque a occasionné un préjudice de **119 millions de Franc CFA**. Cette technique consiste pour un cybercriminel à se procurer une vidéo intime de sa victime et d'exercer sur elle un harcèlement dont la condition de dénouement est le paiement d'une somme d'argent. Pour y arriver, le cybercriminel s'arrange à établir une relation amicale voire amoureuse avec sa future victime, de manière à gagner son entière confiance. Par la suite, il lui demandera de lui fournir ladite vidéo (en lui demandant d'activer sa caméra au cours d'un échange par exemple), qui deviendra finalement le moyen de pression du cybercriminel.

2 – L'accès frauduleux à un système informatique

Ce type d'arnaque est généralement orienté vers les entreprises. Au premier trimestre 2016, il a causé un préjudice financier de **42.271.426 F CFA**. Elle consiste pour le cybercriminel, à forcer l'accès d'un système informatique pour éventuellement voler des donner, ou causer des dégâts pour porter préjudice.

3 – L'usurpation d'identité (Utilisation frauduleuse d'élément d'identification de personne physique ou morale)

L'usurpation d'identité consiste pour un individu à se faire passer pour une autre. Avec des moyens détournés, le cybercriminel réussi à soutirer des informations sensibles qu'il utilise plus tard pour effectuer des paiements, effectuer des paiements etc. Il peut même aller plus loin en engageant la personne de sa victime, par une signature d'accord par exemple, sans son consentement préalable. Ce sont 37.851.973 Franc CFA de dommages qui ont été causés par ce type d'arnaque sur la même période.

Lire aussi : INTERNET : La sécurité des usagers, dernier soucis des fournisseurs d'accès en Côte d'Ivoire ?

4 – L'arnaque au faux sentiment

Ce type d'arnaque est en net recul, après avoir fait de nombreuses victimes à travers le monde. De plus en plus, les internautes sont plus prudents quoique des victimes continuent de se faire duper. 28.754.746 F CFA, c'est le préjudice causé par ce type d'arnaque au premier trimestre 2016.

5 – La fraude sur le porte-monnaie électronique

Avec l'expansion des services de porte-monnaie électronique via le mobile, ce type d'arnaque a pris de l'ampleur.

Bien ficelée, cette technique pousse la victime donner le contrôle absolu à un cybercriminel sur son compte, sans même le réaliser. Par un simple appel ou SMS, le cybercriminel invite son sa victime à saisir un code USSD, pour bénéficier d'un prétendu bonus. Une fois que la procédure est engagée, la carte SIM de la victime est désactivée, son compte transférée sur une nouvelle carte SIM. Le cybercriminel a alors le contrôle absolu.

Article original de Stéphane Agnini

CREDIT : DR

Réagissez à cet article

Original de l’article mis en page : Regionale.info CYBERCRIMINALITE : TOP 5 des arnaques les plus récurrentes au premier trimestre 2016 selon la PLCC > Regionale.info

---

Des complices de cyberescrocs arrêtés en Côte d’Ivoire

Des complices de cyberescrocs arrêtés en Côte d’Ivoire

Utilisation frauduleuse d’éléments d’identification de personne physique, tentative d’escroquerie et complicité d’escroquerie sur internet. Accusés de tous ces crimes, Traoré Issouf, 28 ans, et Kouadio Konan Daniel, 27 ans, tous deux caissiers dans une agence de transfert d’argent nouvellement ouverte, séjournent à la Maison d’arrêt et de correction d’Abidjan (Maca), dans l’attente d’un procès.

Comme l’explique la Plateforme de lutte contre la cybercriminalité (PLCC), ces deux individus ont été arrêtés le 20 juin 2016 par ses agents. Ils sont suspectés d’avoir effectué des transferts frauduleux au profit de quelques cyberescrocs, qui recourent bien souvent à des employés de maisons de transfert d’argent pour encaisser leur butin.

Pour chaque transfert effectué, Kouadio Konan Daniel a avoué avoir perçu une commission de 10%. Mais pouvaient-ils vraiment nier les faits? Après analyse des éléments en leur possession, le Laboratoire de criminalistique numérique (LCN) de la Direction de l’informatique et des traces technologiques (DITT) a pu extraire de nombreux codes de transfert d’argent envoyés par téléphone portable.

Article original de Anselme Akéko – CIO-Mag Abidjan

Réagissez à cet article

Original de l’article mis en page : Transfert d’argent : des complices de cyberescrocs arrêtés en Côte d’Ivoire | CIO MAG

Des cybercriminels s’attaquent à la ministre Raymonde Goudou

Des cybercriminels s’attaquent à la ministre Raymonde Goudou

La cybercriminalité prend de plus en plus de l’ampleur en Côte d’Ivoire. Malgré les moyens mis en place par le ministère de l’Intérieur à travers la plateforme de lutte contre la cybercriminalité (PLCC), certaines personnes s’évertuent à poursuivre cette infraction sans être inquiétés. La dernière en date est celle d’une personne qui se fait passer pour la Ministre de la Santé, Raymonde Goudou Coffie, pour arnaquer.

Nous ne savons pas si des individus ont piraté le compte Facebook de la ministre ivoirienne de la santé ou s’il s’agit d’une usurpation d’identité. Quoiqu’il en soit, des individus utilisent l’identité de la ministre Raymonde Goudou Coffie pour faire de l’aumône auprès des utilisateurs des réseaux sociaux.
A titre illustratif, nous vous publions la conversation que ces prémusés arnaqueurs (brouteurs dans le jargon ivoirien) ont eu avec l’une de leurs victimes.

K.O.
Article original de imatin

Réagissez à cet article

Original de l’article mis en page : Cybercriminalité: Des « brouteurs » s’attaquent à la ministre Raymonde Goudou

---

Les Smart TV, nouvelle cible des ransomwares ?

Les Smart TV, nouvelle cible des ransomwares ?

Si les ransomwares sont chaque jour plus nombreux à venir « pourrir » le quotidien des particuliers comme des entreprises, voilà que ces derniers ne s'en prennent plus seulement aux ordinateurs et aux smartphones. En effet, Frantic Locker s'attaque également aux Smart TV.

Frantic Locker, le rançongiciel qui bloque les Smart TV

Alors que les ransomwares font de nombreuses victimes, le spécialiste de la sécurité informatique Trend Micro révèle que le rançongiciel Frantic Locker s'en prend désormais aux Smart TV.

Présent sur le marché depuis avril 2015, il n'a cessé d'évoluer et un grand nombre de variantes différentes ont développées lui permettant de s'ouvrir à de nouveaux horizons.

Ainsi, dernièrement, Frantic Locker, aussi connu sous le nom FLocker, est diffusé via des campagnes de spam par SMS ou bien par un site web préalablement piégé. Bien évidemment, l'objectif des cybercriminels est toujours le même : faire télécharger des applications malveillantes par l'intermédiaire de clics sur des liens frauduleux.

Mais là où le rançongiciel étonne, c'est qu'il ne bloque pas que les ordinateurs et les smartphones tournant sous Android. En effet, les cybercriminels ont fait des Smart TV leurs nouvelles victimes. Autrement dit, de nombreux téléspectateurs peuvent désormais vivre la mauvaise expérience de voir leur télévision laisser apparaître un message informant qu'une rançon de 200 dollars (en cartes-cadeaux iTunes) était nécessaire pour débloquer leur appareil.

Si tel n'est pas le cas, l'écran restera figé.

Un type d'attaque qui épargne encore certains pays

Depuis son lancement au printemps 2015, le rançongiciel Frantic Locker n'a cessé de se propager au point de cibler un nombre croissant de terminaux.

Concernant les Smart TV, toutes sont potentiellement vulnérables au ransomware FLocker mais selon Trend Micro, il s'autodétruirait en s'installant sur les Smart TV localisées dans plusieurs pays de l'Est de l'Europe comme la Russie, l'Ukraine, la Biélorussie, la Géorgie, la Bulgarie, l'Arménie, l'Azerbaïdjan, le Kazakhstan ou encore la Hongrie.

Article original de Jérôme DAJOUX

Réagissez à cet article

Original de l’article mis en page : Les Smart TV, nouvelle cible des ransomwares ?

QRCodes : pièges à internaute ? – ZATAZ

	QRCodes : pièges à internaute ? – ZATAZ

Détection du premier cas d'email frauduleux utilisant des QRCodes. Le Flashcode, une porte d'entrée à pirate qu'il ne faut pas négliger.

On retrouve ces QRcodes, baptisés aussi Flashcode, dans les journaux, la publicité… Il est possible de naviguer vers un site internet ; mettre l'adresse d'un site en marque-page ; faire un paiement direct via son cellulaire (Europe et Asie principalement) ; ajouter une carte de visite virtuelle (vCard, MeCard) dans les contacts, ou un événement (iCalendar) dans l'agenda électronique ; déclencher un appel vers un numéro de téléphone ; envoyer un SMS ; montrer un point géographique sur Google Maps ou Bing Maps ; coder un texte libre. SnapChat, par exemple, propose un QR Code maison pour suivre un utilisateur. Bref, toutes les possibilités sont ouvertes avec un QRcode. Il suffit de présenter l'image à votre smartphone, et à l'application dédiée, pour lancer la commande proposée par le QR Code. A première vue, un pirate a eu l'idée de fusionner QR Code et hameçonnage.

Fusionner QR Code et hameçonnage

Le hameçonnage, baptisé aussi Phishing/Filoutage, est une technique qui ne devrait plus être étrangère aux internautes. Pour rappel, cette attaque informatique utilise le Social Engineering dont l'objectif est la collecte des identifiants de connexion (mail, login, mot de passe, adresse IP…). Dans l'attaque annoncée il y a quelques jours par la société Vade retro, le cybercriminel a présenté son mail comme une image usurpée à un opérateur national et proposant au destinataire un remboursement consécutif à une facture payée. Le QR Code conduisait à un site présentant une page falsifiée qui incitait la victime à renseigner son identifiant et mot de passe légitime chez l'opérateur usurpé, puis présentait un message d'erreur.

L'illustration flagrante des cyber-risques pour tous

Comme le rappel Maitre Antoine Chéron, avocat spécialisé en propriété intellectuelle et NTIC aujourd'hui, presque tout le monde a une adresse électronique personnelle ou du moins professionnelle. C'est en effet devenu un mode de communication indispensable non seulement pour travailler mais également pour consommer toutes sortes de biens et services. Destinées aux particuliers, les messageries électroniques ne sont pas toujours sécurisées. Avec l'usage en masse de l'internet, et la dématérialisation des richesses, ce sont de précieux biens tels que nos données personnelles, « l'or noir du 21ème siècle », qui sont aujourd'hui convoités par les personnes mal intentionnées.

QRCodes : carrés aux angles dangereux

Les QRcodes envahissent le web et nos vies. Déjà, dès 2012, je vous informais d'une attaque découverte dans le métro parisien. Preuve que les pirates se penchaient sur la manipulation des QRcode depuis longtemps. J'ai pu rencontrer un chercheur « underground » qui s'est penché sur le sujet. Nous l'appellerons DBTJ. Il se spécialise dans la recherche de procédés détournés pour QRcode. « ***Avec mes collègues,*** explique-t-il à ZATAZ.COM, ***nous avons testés plusieurs cas, qui, hélas, se sont avérés efficaces.*** » Dans les cas de Qrcodes malveillants que j'ai pu constater : naviguer vers un site internet et se retrouver face à un code raquetteur (Ransomware) : mettre l'adresse d'un site en marque-page (Shell) ; ajouter une carte de visite virtuelle (vCard, MeCard) dans les contacts, ou un événement (iCalendar) dans l'agenda électronique, lancer un DDoS… bilan, derrière cette possibilité se cachait un vol de données et une mise en place d'usurpation d'identité.
J'ai pu constater aussi des QR Code capable de déclencher un appel vers un numéro de téléphone ou envoyer un SMS. « Nous avons réfléchis aux méthodes d'infections les plus débiles aux plus élaborés, s'amuse mon interlocuteur. Envoyer le QRcode depuis votre téléphone ; la fonctionne SMS dans SET pourrait être intéressante et ne laissera pas de traces ; utiliser le QRcode sur de faux sites, ou encore des sites vulnérables XSS (via un iframe) ; fausses publicités ; remplacer les QRcode aperçus sur des affiches. »
Ce dernier cas a été remarqué par ZATAZ.COM. Il suffit de coller un autre Flashcode, malveillant cette fois, en lieu et place de l'original sur une affiche, dans un arrête de bus par exemple. Effet malheureusement garanti. « Dans le cadre de la démonstration, nous avons infecté exactement 1.341 personnes d'une banlieue de Saint-Denis, et cela en seulement 14 heures, souligne le témoin de ZATAZ.COM. Avec une technique de SE (Social Engineering) d'une simplicité redoutable, nous avons fait des publicités contenant notre QRcode pour un jeu mobile gratuit que nous avons ensuite imprimé en plusieurs exemplaires et diffuser dans les lieux publics (gare/train – centre-ville). » ZATAZ.COM peut confirmer qu'après le test, les « pentesteurs » du QRcode ont effacé l'intégralité des informations collectées.
Bref, voilà de quoi regarder ces petits carrés noirs et blancs d'un œil nouveau … et plus suspicieux. Pour se protéger, des logiciels comme GData QRCode permettent de palier ce type d'intrusion. A utiliser sans modération.

Article original de Damien BANCAL

Réagissez à cet article

Original de l'article mis en page : QRCodes : pièges à internaute ? – ZATAZ

La double authentification de Google contournée par des hackers

La double authentification de Google contournée par des hackers

---

Alors que la double authentification semblait être la meilleure solution pour protéger les données personnelles des internautes, voilà que celle de Google a réussi à être contournée par des pirates. Autrement dit, les spécialistes de la sécurité vont encore devoir se creuser la tête pour trouver encore mieux !

La double authentification plombée par des pirates ?

Puisque la double identification implique qu'un utilisateur saisisse un mot de passe puis qu'il confirme son identité en saisissant un code préalablement reçu par SMS afin de pouvoir accéder à ses comptes, elle semblait être une solution fiable pour bien protéger les données des internautes.

Mais ça, c'était avant puisque des pirates ont réussi à contourner la double authentification de Google pour accéder aux comptes d'utilisateurs tiers.

Pour ce faire, les hackers ont mis en place une méthode plutôt astucieuse. En effet, s'ils disposent de l'adresse mail et du mot de passe, ils se font passer pour la firme de Mountain View, expliquent qu'une activité suspecte a été repérée et invitent l'utilisateur à renvoyer le code de sécurité qui leur a été envoyé.

Sans le savoir, les utilisateurs fournissent alors la clé de l'ultime protection aux pirates qui ont désormais le temps de commettre tous les actes malveillants qui désirent.

Une porte d'entrée vers les terminaux mobiles des utilisateurs ?

En s'offrant un accès aux comptes de messagerie des internautes, les pirates s'offrent une vraie porte d'entrée vers les terminaux mobiles de leurs propriétaires.

En effet, s'ils contrôlent le compte mail de leurs victimes, ils pourront facilement envoyer des mails sur Gmail incluant des pièces jointes frauduleuses qui peuvent être des applications malveillantes. Si le mail est ouvert depuis le mobile, le terminal sera alors automatiquement infecté.

Autrement dit, le hacker pourra avoir un accès complet à l'ensemble des données qu'il contient. Incontestablement, la double authentification a donc ses limites…

Article original de Jérôme DAJOUX

Réagissez à cet article

Original de l'article mis en page : La double authentification de Google contournée par des hackers