Bientôt finis tous les mots de passe ! | Le Net Expert Informatique

	Bientôt finis tous les mots de passe !

Pour en finir avec les mots de passe, PayPal propose d'implanter une puce dans votre cerveau, ou de vous faire ingérer un dispositif "d'identification embarquée" (dans une micropuce).

Il ne s'agit encore que d'une idée, mais pour Jonathan LeBlanc, chef du développement de PayPal, l'avenir est en marche et bientôt nous pourrons oublier les mots de passe, et même les dispositifs biométriques (scanner de l'iris, empreintes digitales), qui « sont déjà obsolètes ».
« Tant que les mots de passe demeureront un standard pour identifier les internautes, les gens continueront à utiliser 'password123' pour se connecter… », indique-t-il au Wall Street Journal. Dans une présentation destinée à être utilisée dans plusieurs conférences sur le sujet, intitulée « Tuez tous les mots de passe », Jonathan LeBlanc prône le développement de nouveaux systèmes, adaptés à la « technologie actuelle », qui tendrait vers une « véritable intégration avec le corps humain ».
Pour Jonathan Leblanc, les systèmes d'analyse du rythme cardiaque via des systèmes embarqués et ingérables sont l'avenir. Ils devraient permettre « d'identifier naturellement un corps » – et donc de barrer la route, définitivement, aux cyberpirates. D'autres « périphériques internes » pourraient être utilisés, comme des implants cérébraux. Les dispositifs ingérables seraient de leur côté alimentés par l'acide de l'estomac, qui ferait office de « batterie ».
Des banques, comme Halifax, testent des systèmes d'identification reposant sur l'analyse du rythme cardiaque des individus – mais pour l'heure, il s'agit de bracelets intelligents, et non de micropuces à avaler. Selon Jonathan Leblanc, les ingénieurs de PayPal planchent d'ores et déjà sur un système similaire.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.zdnet.fr/actualites/paypal-tuez-tous-les-mots-de-passe-39818340.htm
Par Fabien Soyez

Un pirate informatique peut-il détourner un avion connecté au Wi-Fi ? | Le Net Expert Informatique

Un pirate informatique peut-il détourner un avion connecté au Wi-Fi ?

Le GAO aux Etats-Unis, l'équivalent de la Cour des Comptes en France, estime que les systèmes informatiques embarqués à bord des avions pourraient être contrôlés par des pirates informatiques se connectant au système Wi-Fi.

Il recommande donc à la FAA, l'agence fédérale américaine de l'aviation, que les systèmes de protection en terme de cyber-criminalité soient revus à la hausse.
Dans ce rapport publié en avril par le GAO, les experts constatent que les avions modernes embarquent de plus en plus de systèmes connectés, et qu'il existe un risque qu'un pirate informatique parvienne à prendre le contrôle de l'avion via une simple connexion Wi-Fi. « Les technologies modernes de communication sont toujours plus utilisées par les systèmes des avions, ce qui permet à des individus non autorisés d'avoir accès et de compromettre les systèmes avioniques de l'appareil » écrit le GAO. « Le réseau IP pourrait permettre à un pirate d'avoir accès à distance aux systèmes avioniques et de les compromettre. »
Les pare-feux existants à bord des avions les plus modernes utilisant un fort taux de systèmes connectés comme le Boeing 787, l'A350, voire l'A380 ne sont donc pas imparables pour le GAO qui demande à la FAA de revoir à la hausse ces vérifications en matière de cyber-criminalité, alors que les avions modernes installent de plus en plus une connexion Wi-Fi.
Les deux constructeurs aéronautiques européen et américain ont rassuré sans s'avancer en détails techniques sur le sujet, pour bien sûr ne pas donner de renseignements induits aux éventuels futurs pirates informatiques. Airbus a répondu que sa priorité était de « «maintenir les normes les plus élevées en matière de sécurité » et Boeing « qu'aucun changement au plan de vol enregistré dans l'ordinateur de bord ne peut être effectué sans le feu vert du pilote ». (Air Journal)
Pour lire le rapport du GAO (en anglais), cliquer ICI.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.anacgabon.org/fr/index.php/actualites-internationales/4606-un-pirate-informatique-peut-il-detourner-un-avion-connecte-au-wi-fi-

Cybercriminalité : trois techniques en vogue chez les pirates | Le Net Expert Informatique

15

Cybercriminalité : trois techniques en vogue chez les pirates

Avez-vous déjà entendu parler de « rançongiciels » ? Le rapport annuel de la société américaine de sécurité informatique Symantec, publié mardi 14 avril, assure que le recours à ce type de programmes malveillants parmi d'autres est de plus en plus fréquent. « De manière générale, la cybercriminalité a encore crû en 2014, avec 317 millions de nouveaux programmes malveillants créés au niveau mondial, soit près d'un million par jour », explique à l'AFP Laurent Heslault, expert en cybersécurité de Symantec et Norton.

La France progresse d'une place et passe donc au 14e rang mondial (6e rang européen) des pays où la cybercriminalité est la plus active, selon le rapport. **Au niveau mondial, cinq grandes entreprises sur six ont été attaquées en 2014**, soit une progression de **40 % sur un an**, avance Symantec. Francetv info vous présente certaines techniques d'attaque remarquées en 2014.

Viser les éditeurs de logiciels

Les pirates ne sont pas toujours là où on les cherche. Alors que les entreprises se méfient de plus en plus des vols de mots de passe et des usurpations d'identité de leurs employés, les cybercriminels changent de tactique, selon le rapport de Symantec. Pour échapper à toute détection, ils détournent les infrastructures des grandes entreprises, pour les utiliser contre elles.

« Beaucoup sont capables de faire s'auto-infecter les infrastructures des entreprises, via des 'chevaux de Troie', lors de mises à jour de logiciels standards, et d'attendre ensuite patiemment que leurs cibles téléchargent ces mises à jour infectées, leur donnant ainsi libre accès au réseau de l'entreprise », détaille Laurent Heslault. Les cyberattaquants ciblent donc de plus en plus les fournisseurs des grandes entreprises, comme les éditeurs de logiciels.

Réclamer des rançons

Les « rançongiciels » ont plus que doublé dans le monde en 2014, selon le rapport de Symantec. Ces logiciels malveillants prennent le contrôle des PC, tablettes et smartphones et les utilisateurs se voient ensuite réclamer de l'argent pour pouvoir à nouveau utiliser leur machine. **L'an dernier, l'utilisation de ce type de programme (appelé en anglais « ransomware ») a augmenté de 113%**.

Sa variante, dite « cryptolocker », qui retient en otage les données personnelles, a fait 45 fois plus de victimes qu'en 2013. Dans ce système, si la rançon n'est pas payée au terme d'un compte à rebours, les données de la victime sont détruites. « Là où un particulier doit payer 300 euros, une entreprise française s'est vu réclamer 90 000 euros pour récupérer 17 téraoctets de données », relèvent Les Echos.

Miser sur les vulnérabilités encore non détectées

L'année 2014 aura connu un record avec 24 découvertes de vulnérabilités « zero day », c'est-à-dire des pirates qui utilisent des failles non détectées jusque-là dans un logiciel. Ces vulnérabilités entraînent un délai de réponse fortement accru et donc offrent plus de temps aux pirates pour s'en servir.

« Il aura fallu en moyenne 59 jours aux éditeurs de logiciels pour créer et déployer des correctifs [en 2014] alors qu'ils en avaient besoin de seulement quatre en 2013 », relève Laurent Heslault.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.francetvinfo.fr/internet/cybercriminalite-trois-techniques-en-vogue-chez-les-pirates_876373.html
Par Par Yann Thompson

Arte victime d’une attaque informatique jeudi | Le Net Expert Informatique

	Arte victime d’une attaque informatique jeudi

Le lendemain de l'attaque informatique qui a frappé TV5 Monde mercredi, Arte à Strasbourg a également subi une intrusion dans son réseau. Fort heureusement, il ne s'agissait pas d'une attaque menée par des cyber-djihadistes autoproclamés, mais d'un cas classique de « ransom ware », autrement dit de racket par l'intermédiaire d'un virus.

Rançon contre les fichiers

Téléchargé jeudi en milieu d'après-midi via la messagerie, un virus du type « crypto-wall » ou « cryptolocker » s'est installé sur trois ordinateurs d'Arte Culture avant de rapidement se propager. Un salarié témoigne :

« On a vu nos fichiers et nos dossiers devenir inaccessibles, ils avaient tous une taille de 0 octet. On a appelé le service informatique qui a identifié la menace et a mis en quarantaine tout le service culture et éteint nos ordinateurs. Quelques heures après, on a pu reprendre le travail à partir de sauvegardes. »

Une trentaine de postes ont été isolés pendant le reste de la journée. Les fichiers infectés sont rendus illisibles par le virus, qui les crypte les uns après les autres. Il n'y a aucun moyen de les récupérer, sauf à accepter de payer une rançon, généralement via la monnaie Bitcoin qui a l'avantage d'être difficile à tracer. Arte disposait de sauvegardes pour ses fichiers, mais tout de même 500 Go de données ont été corrompues.

Le service informatique d'Arte n'a pas pu déterminer d'origine à cette attaque, relativement fréquente. Il a renouvelé ses consignes de sécurité auprès des employés, qui consistent essentiellement à se méfier des fichiers envoyés par des inconnus.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.rue89strasbourg.com/index.php/2015/04/10/breve/arte-victime-dune-attaque-informatique-jeudi/

Un drone qui pirate les smartphones | Denis JACOPINI

10

Un drone qui pirate les smartphones

Les drones civils commencent à gagner en popularité, et certains s'inquiètent déjà des atteintes à la vie privée qu'ils pourraient faciliter. Au-delà de la simple surveillance, un spécialiste en sécurité met en avant leur utilisation possible à des fins de piratage de données personnelles.

Des experts en sécurité de la société Sensepost ont développé un drone capable de pirater le contenu d'un smartphone depuis les airs. Glenn Wilkinson, qui l'a créé en collaboration avec Daniel Cuthbert, se définit comme un hacker consciencieux, et ses recherches ont pour but de pointer du doigt les failles de sécurité des objets connectés, et notamment des smartphones.
Il présente en ce moment ses travaux à la conférence Black Hat qui se tient à Singapour du 25 au 28 mars. La technologie installée sur le drone, baptisée Snoopy, cherche des appareils mobiles dont le Wi-Fi est activé. Il tire parti de la fonction de recherche de réseaux Wi-Fi auxquels l'appareil s'est déjà connecté, qui est intégrée par défaut à tous les smartphones et tablettes. Le drone prétend alors être l'un de ces anciens réseaux déjà connus, et dupe le smartphone (ou la tablette), interceptant toutes les informations qu'il envoie. Il peut de plus se connecter à plusieurs appareils simultanément, usurpant plusieurs réseaux au besoin.
Les informations interceptées vont des sites visités à tous les identifiants utilisés (Amazon, PayPal, etc.) en passant par les coordonnées bancaires, les données de géolocalisation, et d'autres informations critiques, y compris les noms de tous les réseaux auxquels il s'est déjà connecté.
Le site CNNMoney a récemment testé Snoopy avec son concepteur lors d'une virée à Londres. En à peine une heure, ses équipes ont collecté des informations provenant de 150 appareils mobiles. L'utilisation d'un drone rend cette technologie particulièrement impressionnante, car elle permet de suivre des cibles tout en restant hors de portée, pratiquement indétectable.

Ci-dessous une vidéo du drone en action réalisée par CNN :

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.industrie-techno.com/un-drone-qui-pirate-les-smartphones.29240
Par Julien BERGOUNHOUX

La chaîne TV5 Monde victime d'un piratage de grande ampleur par des individus se réclamant du groupe Etat Islamique | Le Net Expert Informatique

La chaîne TV5 Monde victime d'un piratage de grande ampleur par des individus se réclamant du groupe Etat Islamique

Stupeur à TV5 Monde. La chaîne publique francophone internationale est victime, mercredi 8 avril au soir, d'une importante attaque informatique menée par des militants islamistes se revendiquant de l'organisation Etat islamique (EI), a confirmé son directeur général Yves Bigot. « Nous ne sommes plus en état d'émettre aucune de nos chaînes. Nos sites et nos réseaux sociaux ne sont plus sous notre contrôle et ils affichent tous des revendications de l'Etat islamique », a-t-il indiqué

Propagande et documents postés sur Facebook

Les pirates ont posté des contenus de propagande sur la page Facebook de la chaîne, ainsi que des documents présentés comme des pièces d'identité et des CV de proches de militaires français impliqués dans les opérations contre l'EI. Après près de deux heures, les équipes de la chaîne ont pu reprendre la main sur la page de le TV5 Monde sur le réseau social. Les programmes ont par ailleurs été interrompus, tandis que le site internet de TV5 Monde est toujours indisponible.

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure protection juridique du chef d'entreprise.
Contactez-nous

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

S o u r c e
http://www.francetvinfo.fr/monde/proche-orient/offensive-jihadiste-en-irak/la-chaine-tv5-monde-victime-d-un-piratage-de-grande-ampleur-par-des-individus-se-reclamant-du-groupe-etat-islamique_871789.html#xtor=EPR-51-la-chaine-tv5-monde-victime-d-un-piratage-de-grande-ampleur-par-des-individus-se-reclamant-du-groupe-etat-islamique_871789-20150408-bouton

Nouvelles formes d’attaques informatiques | Le Net Expert Informatique

Nouvelle formes d’attaques informatiques

Sévissant depuis l'année dernière, ce malware de nouvelle génération combine techniques informatiques sophistiquées, ingénierie sociale et intervention humaine pour que la fraude soit effective. Nom de code : Dyre Wolf

Entre 500 000 et 1,5 million de dollars par attaque. Tel est le butin ramassé lors de l'attaque réalisée à l'aide du malware Dyre qui sévit depuis le mois d'octobre dernier. Mais les criminels derrière ce programme ont récemment franchi une nouvelle étape qui permet au programme de retrouver une nouvelle jeunesse, au grand dam des entreprises qui en sont victimes.
L'attaque se déroule en plusieurs étapes. Dans un premier temps, des utilisateurs reçoivent un mail contenant une pièce jointe, elle-même infectée par le logiciel Upatre. Le but de ce logiciel est uniquement de permettre le téléchargement de Dyre, un programme beaucoup plus dangereux. Lorsque Dyre est téléchargé, il va essayer de se répandre le plus largement possible chez les autres employés de l'entreprise ou les amis de la personne infectée au travers du programme de messagerie Outlook. En parallèle, le logiciel va surveiller le travail de la personne infectée et attendre qu'elle se connecte à un parmi des centaines de sites bancaires que le maliciel est programmé pour surveiller.

Le voleur au bout du fil
Et c'est là que cela devient tout à fait nouveau. Lors de la tentative de connexion au site, Dyre va afficher un message indiquant que la connexion et le compte posent un problème et va inviter la personne à contacter un numéro de téléphone. Précisons que ceci se passe indépendamment du navigateur utilisé : Chrome, Firefox ou Internet Explorer. En effet, les trois navigateurs ont été usurpés.
En composant le numéro de téléphone, la victime ne va pas tomber sur un centre d'appel mais sur une vraie personne qui va se proposer de « l'aider » à régler son problème. Cette personne en apparence tout à fait bien intentionnée va donc vous demander des informations sur votre compte et pendant que vous discutez avec elle, elle procédera à un transfert de fonds depuis le compte bancaire de l'entreprise vers les propres comptes des criminels. « L'intervention d'un opérateur au téléphone en direct est unique», précise Caleb Barlow, vice-président d'IBM.

Et un petit DDOS pour bien masquer le tout
Enfin, simultanément au transfert de fonds, le site web de l'entreprise qui vient d'être pillée va être victime d'une attaque en DDOS. Le but de cette attaque est de détourner l'attention des services IT et de sécurité qui seront trop occupés à endiguer cette attaque pour s'occuper d'une escroquerie financière, du moins dans les premiers jours.
On le voit : l'imagination des cybercriminels est débordante. Comme à l'habitude, IBM répète une série de conseils, notamment de ne jamais fournir des informations bancaires à quiconque, les « vraies » banques ne demandant jamais ce type d'informations.

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure protection juridique du chef d'entreprise.
Contactez-nous

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.mag-securs.com/news/articletype/articleview/articleid/34604/dyre-wolf-nouvelle-etape-dans-la-cybercriminalite.aspx
Par Raphaël Stencher

Android, une vulnérabilité affecterait 50% du parc… | Le

Net Expert Informatique

	Android, une vulnérabilité affecterait 50% du parc…

Si 50% du parc Android est théoriquement vulnérable à cette faille, celle-ci présente de nombreuses restrictions limitant son exploitation potentielle. De l'aveu même de Palo Alto, aucune attaque réelle n'exploitant cette méthode n'a été constatée. Pas de panique à l'horizon donc, d'autant plus que cette vulnérabilité a été corrigée dans les dernières mises à jour de l'OS.

Cette vulnérabilité permet d'exploiter le mécanisme de validation des applications d'Android avant l'installation de celles-ci. Rien à craindre si vous restez cantonnés au Google Play Store, mais reste envisageable à l'encontre des utilisateurs qui se procurent des applications chez des app store tiers tel que ceux proposés par Amazon. Cette vulnérabilité exploite un mécanisme connu, la différence entre le Time to check et le Time To use.

Un temps pour tout

Concrètement, il convient tout d'abord de proposer une première application entièrement légitime à l'utilisateur. Dans un premier temps, l'OS va récupérer un certain nombre d'informations relatives à l'application : son nom ainsi que les permissions dont elle a besoin pour fonctionner. Elle va ensuite les présenter à l'utilisateur qui va ensuite valider l'installation de l'application en appuyant sur le bouton Installer.

Mais Palo Alto note que, contrairement aux applications provenant de Google Play Store, les fichiers d'installation ne sont pas placés dans un espace de stockage protégé lorsqu'ils proviennent de sources tierces. Cette particularité permettrait à un attaquant de proposer une première application, déclenchant le Time to Check, puis avant que l'utilisateur ne valide le processus d'installation, de remplacer par une seconde application cette fois malveillante, sans que l'utilisateur ne soit prévenu du changement ni s'en aperçoive.

Cette vulnérabilité a été patchée dans la release 4.3_r0.9. Un post de blog expliquant en détail le fonctionnement de la vulnérabilité a été mis en ligne par Palo Alto, ainsi que des vidéos et un outil permettant de détecter la présence ou non de la vulnérabilité sur un terminal.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.zdnet.fr/actualites/android-une-vulnerabilite-affecterait-50-du-parc-39817006.htm
Par Louis Adam

Laboratoire d’analyses médicales piraté : demande de rançon et publication de résultats médicaux | Le Net Expert Informatique

Le laboratoire de biologie médicale Labio est la cible d'un groupe de pirates. Ce dernier revendique avoir dérobé pas moins de 40 000 identifiants (nom, prénom, login et mot de passe), ainsi que « des centaines » de bilans médicaux. Une rançon de 20 000 euros est demandée et les fuites d'informations confidentielles ont déjà commencé.Les demandes de rançons sont de plus en plus courantes dans le cas des piratages de données informatiques. Récemment, on a par exemple le cas de SynoLocker sur les NAS Synology, de Feedly, puis de Domino's Pizza. Dans ce dernier cas, la société nous avait indiqué qu'elle se refusait à céder aux demandes de son maitre chanteur, le groupe de pirates Rex Mundi, et qu'aucune transaction financière n'aurait lieu. Des données auraient finalement été mises en ligne quelques mois plus tard.

Rex Mundi demande une rançon de 20 000 euros ou des résultats d'analyse seront publiés
Aujourd'hui, rebelotte avec le même groupe Rex Mundi et, là encore, avec une demande de rançon. Cette fois-ci, c'est un laboratoire français d'analyse médicale qui est visé : Labio.fr. Via l'un de ses comptes Twitter, Rex Mundi indique avoir piraté le site la semaine dernière et détenir « des centaines » de résultats d'analyses sanguines ainsi que pas moins de 40 000 noms, prénoms, identifiants et mots de passe des clients. Les revendications sont les mêmes que pour Domino's Pizza : si la rançon exigée n'est pas payée – 20 000 euros dans le cas présent – les documents récupérés seront publiés dans leur intégralité.

Un ultimatum était fixé. Arrivé à son terme il y a peu, le groupe Rex Mundi a mis ses menaces à exécution et a commencé à dévoiler des informations via son site hébergé sur le réseau Tor. Deux documents sont disponibles. Le premier contient 15 000 noms, prénoms, identifiants et mots de passe qui proviendraient de comptes clients Labio. Le second comporte pour sa part une dizaine de résultats d'analyse du laboratoire de recherche médicale, certains récents, d'autres plus anciens.
Suivant les patients, on y retrouve de l'immuno-sérologie, de la biochimie urinaire et sanguine, de l'hématologie, etc. Autant dire que les informations sont très sensibles :

Nous avons effacé toutes les données confidentielles avant la mise en ligne de l'image

Labio aux abonnés absents, le serveur de résultats fermé « suite à un problème technique »
Nous avons évidemment tenté de contacter par téléphone différents laboratoires affiliés Labio.fr (ils sont quatorze, répartis dans le sud-est et principalement autour de Marseille). Une fois que nous nous sommes présentés en bonne et due forme (en tant que journalistes) et que nous que nous avons expliqué les raisons de notre appel (piratage et bilans médicaux dans la nature), nos correspondants nous ont tous répondu ne pas être au courant et ne rien pouvoir faire pour nous. Impossible également de demander à parler un responsable ou d'obtenir le nom d'une personne à contacter pour évoquer ce problème. La conversation coupait généralement court très vite.

On remarquera par contre que, hasard ou pas du calendrier, dès sa page d'accueil Labio.fr informe ses clients que, « suite à un problème technique, le serveur internet de résultats est temporairement indisponible », et ce, depuis plusieurs jours maintenant. Bien évidemment, nous avons contacté la CNIL et nous attendons également son retour sur la question.

Entre obligation de sécurisation et peine encourue par les pirates
Sur son site, la Commission nationale de l'informatique et des libertés rappelle qu'avec les données de santé, la sécurité est un « impératif » pour ceux qui les hébergent : « il vous appartient de prendre les dispositions nécessaires pour assurer la sécurité des données enregistrées et empêcher qu'elles ne soient divulguées ou utilisées à des fins détournées, surtout s'il s'agit d'informations couvertes par le secret médical » précise-t-elle. Il est notamment question du « chiffrement de tout ou partie des données », mais aussi du « chiffrement de la communication (ex. : chiffrement SSL avec une clef de 128 bits) » lorsque les données circulent sur Internet.

Pour autant, le laboratoire de recherche n'est soumis à aucune obligation de communication auprès de ses clients, seuls les opérateurs le sont (voir le cas d'Orange par exemple), et il semblerait que Labio semble bien décidé à ne pas évoquer le sujet outre mesure, avec nous tout du moins. Si le laboratoire devait répondre à nos questions (nous les avons également contactés via le formulaire présent sur leur site), nous mettrons évidemment cette actualité à jour.

Mais que risquent exactement les pirates dans cette histoire ? Selon l'article 226-16 du Code pénal, « le fait, hors les cas prévus par la loi, de mettre ou de conserver en mémoire informatisée, sans le consentement exprès de l'intéressé, des données à caractère personnel qui, directement ou indirectement, font apparaître les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses, ou les appartenances syndicales des personnes, ou qui sont relatives à la santé ou à l'orientation sexuelle de celles-ci, est puni de cinq ans d'emprisonnement et de 300 000 € d'amende ».

Quoi qu'il en soit, l'histoire n'est pas encore terminée puisque Rex Mundi indique que les publications de documents confidentiels continueront si la rançon exigée n'est pas payée.

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINE et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure protection juridique du chef d'entreprise.
Contactez-nous

Liste des Laboratoires Labio proche de chez-vous (http://www.labio.fr/nos-laboratoires#labs) :
Laboratoire Centraix – Aix en Provence
Laboratoire des 2 Ormes – Aix en Provence
Laboratoire Celse L'Reste – Aix en Provence
Unité de Fertilité et de Procréation Médicalement Assistée du Pays d'Aix (PMA)
Centre Hospitalier du Pays d'Aix
Laboratoire d'Eguilles
Laboratoire des 5 Avenues – Marseille 6ème
Laboratoire de Saint Marcel – Marseille 11ème
Laboratoire de Saint Julien – Marseille 12ème
Laboratoire des 3 Lucs – Marseille 12ème
Laboratoire de Saint Jérôme – Marseille 13ème
Laboratoire de Saint Mitre- Marseille 13ème
Laboratoire de la Rotonde – Plan de Cuques
Laboratoire de Puricard
Laboratoire de Saint Rémy de Provence

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.nextinpact.com/news/93499-labio-fr-pirate-demande-rancon-et-publication-resultats-medicaux.htm

---

Attention, insérer cette clé USB dans votre PC peut le détruire ! | Le Net Expert Informatique

Attention, insérer cette clé USB dans votre PC peut le détruire !

Un facétieux hacker a mis au point une fausse clé USB capable de griller une machine lorsqu'elle est insérée dans une prise d'un ordinateur.

On ne le répètera jamais assez : n'insérez jamais dans votre ordinateur une clé USB si vous ne savez pas d'ou elle provient. Car elle pourrait non seulement inoculer un malware dans votre machine, mais aussi carrément… le détruire !
Bon, inutile de trop s'inquiéter, ce danger n'est encore que très théorique. Mais un facétieux hacker russe a bel et bien mis au point une fausse clé USB en mesure de griller les circuits d'un ordinateur en lui infligeant une décharge électrique. L'idée de ce projet est partie d'une légende urbaine amusante : « j'ai lu un article sur un gars qui a volé une clé USB dans le métro. Elle traînait dans la poche extérieure du sac d'un autre type. Il y avait marqué 128 dessus. Le gars est rentré chez lui, l'a inséré dans son ordinateur et la clé a grillé la machine. Alors il a écrit 129 sur la clé et l'a mis dans la poche extérieure de son sac. »

Pour fabriquer sa petite bombe, notre homme, qui travaille dans une entreprise d'électronique, a conçu un petit circuit imprimé et acheté quelques composants. Sa fausse clé contient plusieurs condensateurs et un convertisseur DC/DC. Lorsque la clé est branchée, les condensateurs se chargent grâce au port USB. Lorsqu'ils sont chargés, le convertisseur s'arrête et un transistor décharge l'énergie via les fils de données du port. Lorsqu'ils sont déchargés, le processus de charge reprend… et ainsi de suite jusqu'à ce que la clé grille la machine. Il estime être capable de détruire jusqu'au processeur avec son « invention ».
Ouf, notre hacker ne donne aucun détail qui pourrait permettre de créer son propre « USB Killer ». Il a évidemment plutôt conçu son appareil pour éveiller les consciences aux dangers que représente une clé USB inconnue. Et termine par une boutade : « quant aux applications de cet appareil, je ne les évoquerai pas. Mais un ancien collègue me dit que c'est comme la bombe atomique : c'est cool de l'avoir, mais il ne faut pas l'utiliser. »

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.01net.com/editorial/648920/attention-inserer-cette-cle-usb-dans-votre-pc-peut-le-detruire/
Par Eric LB