Plusieurs millions de clés de chiffrement plus du tout sécurisées

Plusieurs millions de clés de chiffrement plus du tout sécurisées

Des clés de chiffrement de 1024 bits utilisées pour sécuriser échanges Internet et VPN peuvent intégrer des « trappes » indétectables.

Des clés de chiffrement de 1024 bits utilisées pour sécuriser les échanges et les communications sur Internet (sites Web, VPN et serveurs), peuvent utiliser des nombres premiers munis de« *trappes* » indétectables. L'exploit permettrait à des pirates de déchiffrer plusieurs millions de communications chiffrées, et d'identifier les propriétaires des clés. C'est ce qui ressort des travaux d'une équipe de chercheurs : Joshua Fried et Nadia Heninger, de l'Université de Pennsylvanie, Emmanuel Thomé et Pierrick Gaudry, de l'équipe projet CARAMBA (Inria-CNRS-Université de Lorraine).

« *Nous démontrons dans nos travaux que la création et l'exploitation de trappes des nombres premiers (trapdoored primes) pour les standards d'échange de clés Diffie-Hellman et du DSA (Digital Signature Algorithm) est faisable pour les clés de 1024 bits avec des ressources informatiques universitaires modernes* », déclarent les chercheurs dans leur article technique. Ils disent avoir « *effectué un calcul de logarithmes discrets dans une trappe des nombres premiers, en deux mois sur un cluster académique* ».

Traffic HTTPS et VPN déchiffrés

Les standards internationaux de cryptographie reposent sur des nombres premiers dont l'origine devrait être vérifiable. Mais, aujourd'hui, trop de serveurs communiquent en s'appuyant sur des nombres premiers dont l'origine est invérifiable : 37% des sites en HTTPS (parmi le million de sites les plus visités du top Alexa) et 13% des VPN IPsec, rappelle Inria.

Pour son propriétaire, une clé de chiffrement dotée d'une trappe ressemble à toute autre clé fiable. Pour les attaquants qui exploiteraient la trappe, en revanche, la sécurité de la clé peut être brisée à travers la résolution plus rapide du problème du logarithme discret. Selon les chercheurs, l'échelle de difficulté pour un pirate deviendrait « *très facile* » pour une clé de 768 bits, « *facile* » pour une clé de 1024 bits, mais hors de portée pour du 2048 bits…. pour le moment…[lire la suite]

Notre métier : Sensibiliser les décideurs et les utilisateurs aux risques liés à la **Cybercriminalité** et à la **Protection des Données Personnelles** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).

Denis JACOPINI anime dans toute le France et à l'étranger des conférences, des tables rondes et des formations pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles (Mise en Place d'un Correspondant Informatique et Libertés (CIL) 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 : Des trappes dans plusieurs millions de clés de chiffrement

---

Spotify diffuserait des malwares

Spotify diffuserait des malwares

La version gratuite de Spotify diffuse en ce moment des publicités renvoyant vers des sites infestés de malwares. (CCM) – C’est quand on croit avoir tout vu qu’on était toujours le plus surpris.…[Lire la suite]

Denis JACOPINI anime des **conférences, des formations** en Cybercriminalité et est régulièrement invité à des **tables rondes en France et à l’étranger** pour sensibiliser les décideurs et les utilisateurs aux **Dangers liés à la Cybercriminalité (Arnaques, Piratages…) pour mieux s’en protéger** (Autorisation de la Direction du travail de l’Emploi et de la Formation Professionnelle n°93 84 03041 84).
Plus d’informations sur sur cette page.

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

Une faille dans OpenSSH remet en question la sécurité de certains objets connectés

Une faille dans OpenSSH remet en question la sécurité de certains objets connectés

---

Akamai a découvert que les attaques DDoS IoT utilisées une faille dans OpenSSH existaient depuis 12 ans.

L'Internet des objets est en pleine croissance et la sécurité est au cœur des préoccupations des responsables informatiques. Qui plus est, ces objets connectés sont utilisés par des cybercriminels pour mener des attaques en déni de service. OVH et le spécialiste de la sécurité Brian Krebs en ont fait l'expérience ces dernières semaines.
On apprend maintenant que ces attaques ont été rendues possibles en raison d'une faille présente depuis 12 ans dans OpenSSH. Deux chercheurs d'Akamai, Ory Segal et Ezra Caltum ont découvert cette vulnérabilité et l'ont baptisé SSHowDowN Proxy. Elle vise notamment à enrôler plusieurs objets connectés comme les caméras de surveillance (CCTV) et leurs enregistreurs numériques (DVR), les antennes satellites, les routeurs, les NAS. « Ces dispositifs sont maillés pour attaquer une multitude de sites ou de services Internet à travers http, SMTP ou via un scan réseau », constate les experts. Ils ajoutent que les attaques peuvent aussi cibler les réseaux qui hébergent les objets connectés…[lire la suite]

Notre métier : Sensibiliser les décideurs et les utilisateurs aux risques liés à la **Cybercriminalité** et à la **Protection des Données Personnelles** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Denis JACOPINI anime dans toute le France et à l'étranger des conférences, des tables rondes et des formations pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles (Mise en Place d'un Correspondant Informatique et Libertés (CIL) 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 : Une faille dans OpenSSH âgée de 12 ans fragilise l'IoT

52 % des DSI Français acceptent moins de sécurité pour plus de mobilité

52 % des DSI Français acceptent moins de sécurité pour plus de mobilité

C’est une nouvelle à la fois peu surprenante et inquiétante : plus de la moitié des responsables informatiques en France cèdent du terrain sur le plan sécuritaire pour avantager la mobilité et le Bring Your Own Device.

« **Rendre les salariés et les opérations plus agiles** »
On ne cesse de le répéter depuis des années : le BYOD est loin d’être toujours un choix, il n’est pas rare qu’il s’impose de lui-même. Rejeter cette situation, c’est risquer une utilisation sous-marine, multipliant ainsi les risques. L’accepter, c’est limiter les risques en question en encadrant le BYOD.
Dans une étude menée par le cabinet Vanson Bourne pour le compte de VMware (plus de détails en fin d’article), nous apprenons que 52 % des responsables informatiques français font face à une telle pression vis-à-vis de la mobilité d’entreprise « qu’ils sont prêts à prendre des risques inconsidérés vis-à-vis de la sécurité des données de leur organisation ».
Ces risques sont en grande partie pris pour contenter les cadres dirigeants qui souhaitent absolument accéder aux données pro via leurs propres terminaux, « même si cela va à l’encontre des stratégies de leur entreprise » et que cela multiplie les risques de cyberattaques.
Mais les gains en valent la chandelle puisque les DSI cèdent. 51 % d’entre eux estiment ainsi que les bénéfices sont supérieurs aux risques. « Transformation numérique et mobilité sont indissociables. Les organisations doivent sans cesse chercher à développer leurs activités et à innover. Elles prennent donc des risques à court terme sur le plan de la sécurité afin de rendre les salariés et les opérations plus agiles » explique notamment Sylvain Cazard, directeur général de VMware France.
Pour s’adapter au marché et aux désirs de certains salariés, les DSI n’hésitent donc pas à prendre plus de risques. Il faut dire que près d’un quart des responsables informatiques estiment que le manque de mobilité des salariés réduit leur productivité. Un argument qui fait mouche et pousse logiquement les DSI à lâcher du lest côté sécurité.

Des salariés mal formés, des patrons sous-informés
Bien évidemment, les responsables n’ont pas à laisser la porte ouverte au premier pirate informatique venu. Une plus forte pédagogie auprès des salariés devient ainsi indispensable si l’entreprise ne souhaite pas voir toutes ses données partir dans la nature. Ce point est d’autant plus majeur sachant que l’étude indique que 60% des salariés mobiles précisent ne pas connaître la politique de sécurité de leur entreprise… Une statistique douloureuse et effrayante qu’il convient de ne pas minimiser.
Plus grave encore pour les dirigeants d’entreprises, une ancienne enquête de Vanson Bourne montrait que 25 % des DSI français ont confié ne pas informer leur patron en cas de cyberattaque. Ceci alors même que 29 % des DSI et 21 % des employés estiment que leurs patrons sont responsables en cas de fuite de données. Une incohérence qui en dit long sur la complexité de la problématique…[lire la suite]

Notre métier : Sensibiliser les décideurs et les utilisateurs aux risques liés à la **Cybercriminalité** et à la **Protection des Données Personnelles** (Autorisation de la Direction du travail de l’Emploi et de la Formation Professionnelle n°93 84 03041 84).
Denis JACOPINI anime dans toute le France et à l’étranger des conférences, des tables rondes et des formations pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles (Mise en Place d’un Correspondant Informatique et Libertés (CIL) 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 : BYOD : 52 % des DSI Français acceptent moins de sécurité pour plus de mobilité

Pourquoi les vols de données sont en forte hausse ?

Pourquoi les vols de données sont en forte hausse ?

Une étude du Ponemon Institute pour Varonis révèle que la plupart des collaborateurs disposent d'accès trop importants, ce qui multiplie les dommages lorsque leurs comptes sont compromis

Trois entreprises sur quatre ont été victimes de la perte ou du vol de données importantes au cours des deux dernières années. Selon une nouvelle enquête menée auprès de plus de 3 000 collaborateurs et informaticiens aux États-Unis et en Europe, cela représente une très forte augmentation depuis 2014. Le rapport publié aujourd'hui a été rédigé par le Ponemon Institute et sponsorisé par Varonis Systems, Inc., principal fournisseur de solutions logicielles permettant de protéger les données contre les menaces internes et les cyberattaques.
Selon l'enquête, l'augmentation de la perte et du vol des données est en grande partie due aux compromissions de comptes internes. Celles-ci sont aggravées par des accès aux informations critiques bien plus permissifs que nécessaire par les collaborateurs et les tiers. Sans oublier le constant défaut de supervision des accès et de l'activité dans les systèmes de messagerie et les systèmes de fichiers, là où se trouvent les données les plus sensibles et les plus confidentielles.
Parmi les principales conclusions :
• 76 % des informaticiens indiquent que leur entreprise a fait l'expérience de la perte ou du vol de ses données au cours des deux dernières années. Ce chiffre représente une augmentation importante par rapport aux 67 % d'informaticiens interrogés ayant donné la même réponse lors de l'étude de 2014 réalisée par Ponemon pour le compte de Varonis.
• Les informaticiens indiquent que la négligence des collaborateurs a deux fois plus de chances d'entraîner la compromission des comptes internes que tout autre facteur, y compris les attaquants externes ainsi que les collaborateurs ou les prestataires malveillants.
• 78 % des informaticiens déclarent être très préoccupés par les ransomware, un type de logiciels malveillants qui bloque l'accès aux fichiers jusqu'au paiement d'une somme d'argent. 15 % des entreprises ont déjà fait l'expérience des ransomware et seule une petite moitié d'entre elles a détecté l'attaque au cours des 24 premières heures.
• 88 % des utilisateurs finaux indiquent que leur travail exige l'accès et l'emploi d'informations propriétaires telles que des données relatives aux clients, des listes de contacts, des renseignements sur les collaborateurs, des rapports financiers, des documents commerciaux confidentiels ou d'autres actifs informationnels critiques. C'est nettement plus que les 76 % enregistrés dans l'étude de 2014.
• **62 % des utilisateurs finaux indiquent avoir accès à des données de l'entreprise qu'ils ne devraient probablement pas pouvoir consulter**.
• Seuls 29 % des informaticiens interrogés indiquent que leur entreprise applique un modèle strict de moindre privilège pour s'assurer que les collaborateurs ont accès aux données de l'entreprise en fonction de leur besoin de les connaître.
• Seulement 25 % des entreprises supervisent toute l'activité relative à la messagerie et aux fichiers, alors que 38 % ne supervisent aucune activité.
• 35 % des entreprises ne disposent d'aucun enregistrement interrogeable de l'activité du système de fichiers, ce qui les rend incapables de déterminer les fichiers chiffrés par ransomware (entre autres choses).
Le rapport d'étude intitulé « *Closing Security Gaps to Protect Corporate Data: A Study of U.S. and European Organizations* » se fonde sur des entretiens menés en avril et mai 2016 auprès de 3 027 employés aux États-Unis, au Royaume-Uni, en France et en Allemagne. L'ensemble des personnes interrogées comprend 1 371 utilisateurs finaux ainsi que 1 656 informaticiens et professionnels de la sécurité informatique issus d'entreprises de tailles variant de quelques douzaines à plusieurs dizaines de milliers d'employés. Ils proviennent de divers secteurs, dont les services financiers, le secteur public, le secteur des soins de santé et des sciences de la vie, la vente au détail, le secteur industriel, le secteur technologique et l'industrie du logiciel…[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 : Vols de données en forte hausse, cause principale: les menaces internes | Docaufutur

Quelles failles pour les voitures connectées ?

Quelles failles pour les voitures connectées

L'édition du salon de l'auto interpelle le grand public sur les nouveaux pirates de la route. Voitures connectées : les cybercriminels dans l'angle mort ?

Nul doute, la voiture connectée est encore l'une des stars du salon de l'auto cette année. Comme tout ce qui attrait à internet et aux objets connectés, il est légitime de se poser quelques questions notamment sur la sécurité liée au partage des données ainsi qu'à cette forme de déplacement autonome. Un véhicule connecté est en effet doté d'un accès à Internet ainsi que, plus généralement, d'un réseau local sans fil. L'accès Web offre divers services supplémentaires tels que la notification automatique des embouteillages, la réservation de parking, la surveillance du style de conduite (pouvant par ailleurs avoir une incidence sur le montant des primes d'assurance automobiles) etc.
De multiples raisons peuvent motiver les cybercriminels à tenter de pirater des voitures connectées :
L'appât du gain : ll s'agit de bloquer l'accès au véhicule jusqu'à ce la victime paie une rançon.
L'espionnage : l'activation du micro ou de la caméra équipant le véhicule peut donner accès à des informations exclusives et des données sensibles.
La violence physique : les attaques peuvent avoir pour but de blesser le conducteur, ses passagers, ou encore d'endommager d'autres véhicules sur la route.
C'est en analysant ses raisons que la société russe développe une approche de la sécurité interne des véhicules connectés. Elle reposent sur deux principes : D'abord l'isolement veille à ce que deux entités indépendantes (applications, pilotes, machines virtuelles) ne puissent interférer l'une avec l'autre en aucune façon. Ensuite, le contrôle des communications signifie que deux entités indépendantes ayant à communiquer dans le système doivent le faire conformément à des règles de sécurité. L'utilisation de techniques de cryptographie et d'authentification pour l'envoi et la réception des données fait également partie intégrante de la protection du système.
Pour respecter notre travail, merci de ne reprendre que l'intro. Pour lire la suite de cet article original direction ->
http://www.datasecuritybreach.fr/voitures-connectees-cybercriminels-langle-mort/#ixzz4MV1xJas6

…[lire la suite]

Notre métier : Sensibiliser les décideurs et les utilisateurs aux risques liés à la **Cybercriminalité** et à la **Protection des Données Personnelles** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Denis JACOPINI anime dans toute le France et à l'étranger des conférences, des tables rondes et des formations pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles (Mise en Place d'un Correspondant Informatique et Libertés (CIL) 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

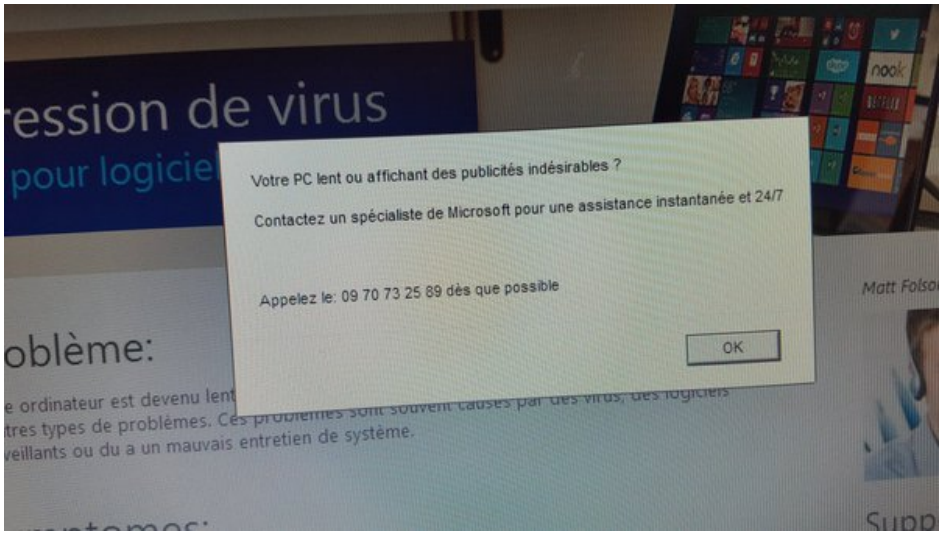
Contactez-nous

Réagissez à cet article

Original de l’article mis en page : Voitures connectées : les cybercriminels dans l’angle mort ? – Data Security Breach

---

FakeAlert : Découverte d’une infection qui touche la France



FakeAlert : Découverte d’une infection qui touche la France

Détection d'une très forte augmentation du nombre d'échantillons du malware HTML / FakeAlert, à destination de la France.

HTML / FakeAlert est le nom générique donné par l'éditeur de solution de sécurité informatique ESET. Un terme qui nomme les fausses pages web hébergeant des messages d'alertes. Ces derniers indiquent à l'utilisateur qu'il est infecté par un virus ou qu'il a un autre problème susceptible de compromettre son ordinateur ou ses données. Pour stopper la soi-disant menace, l'utilisateur est invité à contacter par téléphone le faux support technique ou à télécharger une fausse solution de sécurité.
Le malware HTML / FakeAlert est généralement utilisé comme point de départ pour ce que l'on appelle les escroqueries de faux support. En conséquence, les victimes perdent de l'argent (en appelant des numéros surtaxés ou internationaux) ou sont infectés par un vrai malware installé sur leur ordinateur via les programmes « recommandés » figurant sur la page des fausses alertes…[lire la suite]

Notre métier : Sensibiliser les décideurs et les utilisateurs aux risques liés à la **Cybercriminalité** et à la **Protection des Données Personnelles** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Denis JACOPINI anime dans toute le France et à l'étranger des conférences, des tables rondes et des formations pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles (Mise en Place d'un Correspondant Informatique et Libertés (CIL) 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.

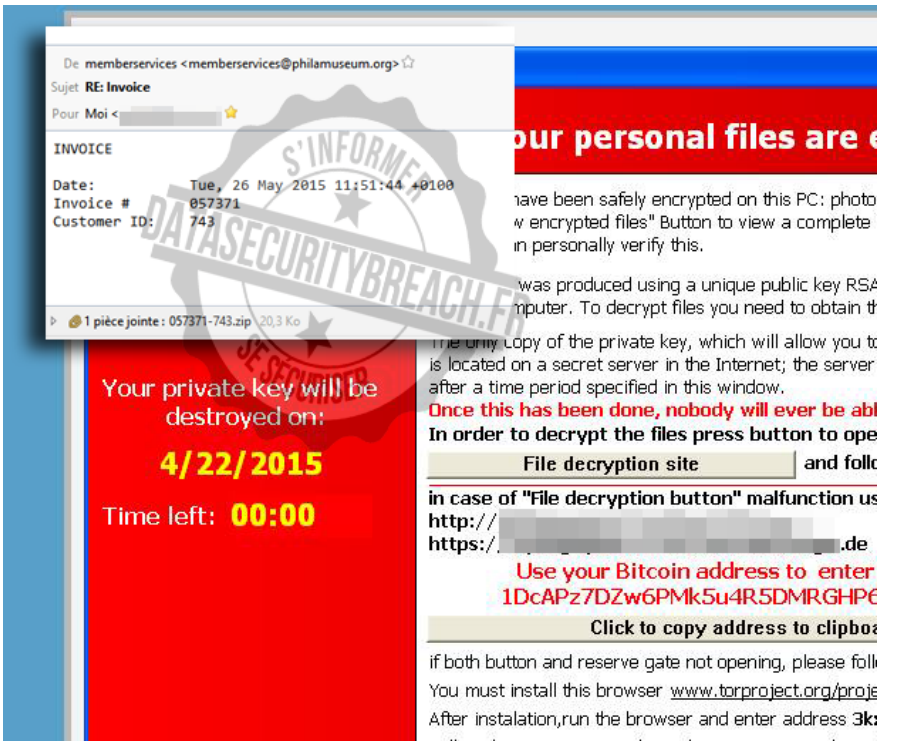
Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Original de l'article mis en page : FakeAlert : Découverte d'une infection qui touche la France – ZATAZ

Mise à disposition de l’outil de déchiffrement contre le ransomware Polyglot



Mise à disposition de l’outil de déchiffrement contre le ransomware Polyglot

Les victimes du ransomware Polyglot, aussi connu sous le nom MarsJoke, peuvent maintenant récupérer leurs fichiers grâce à l'outil de déchiffrement développé par Kaspersky Lab.

Comment fonctionne Polyglot ? Il se propage via des emails de spam qui contiennent une pièce jointe malicieuse cachée dans une archive RAR. Durant le processus de chiffrement, il ne change pas le nom des fichiers infectés mais en bloque l'accès. Une fois le processus de chiffrement terminé, le wallpaper de bureau de la victime est remplacé par la demande de rançon. Les fraudeurs demandent que l'argent leur soit remis en bitcoins et si le paiement n'est pas fait dans les temps, le Trojan se détruit en laissant tous les fichiers chiffrés.

Lien avec CTB-Locker ?

Le fonctionnement et le design de ce nouveau ransomware sont proches de ceux de CTB-Locker, un autre ransomware découvert en 2014 qui compte de nombreuses victimes à travers le monde. Mais après analyse, les experts de Kaspersky Lab n'ont trouvé aucune similarité dans le code. En revanche, contrairement à CTB-Locker, le générateur de clés de chiffrement utilisé par Polyglot est faible. Les créateurs de Polyglot semblaient penser qu'en imitant CTB-Locker, ils pourraient piéger les utilisateurs en leur faisant croire qu'ils étaient victimes d'un grave malware, ne leur laissant d'autre option que de payer…[Téléchargez l'outil]

Article de Data Secutity Breach

Notre métier : Sensibiliser les décideurs et les utilisateurs aux risques liés à la **Cybercriminalité** et à la **Protection des Données Personnelles** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).

Denis JACOPINI anime dans toute le France et à l'étranger des conférences, des tables rondes et des formations pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles (Mise en Place d'un Correspondant Informatique et Libertés (CIL) 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 : Outil de déchiffrement contre le ransomware Polyglot — Data Security BreachData Security Breach

Yahoo espionne tous vos e-mails pour le compte de la NSA ou du FBI

Yahoo espionne tous vos e-mails pour le compte de la NSA ou du FBI

Yahoo a accepté sans combattre d'installer un logiciel sur ses serveurs, qui regarde le contenu des e-mails qui arrivent et transmet aux services de renseignement américains ceux qui peuvent les intéresser. Il est plus que temps de fermer son compte Yahoo.

L'agence Reuters a révélé mardi que les ingénieurs en charge du service des e-mails de Yahoo ont développé et mis en place en 2015 un logiciel qui scanne le contenu de tous les messages envoyés vers les centaines de millions de comptes Yahoo, pour copier et mettre à la disposition des autorités américaines ceux qui contiennent certaines chaînes de caractères intéressant les services de renseignement. L'ordre confidentiel, qui émanerait de la NSA ou du FBI et a été confirmé par quatre sources dont trois anciens employés de Yahoo, a été suivi sans que la direction de Yahoo le conteste.
C'est la découverte du bout de code qui aurait conduit le chef de la sécurité de Yahoo, Alex Stamos, à démissionner et partir chez Facebook en juin 2015. Ses équipes n'avaient pas été informées et il jugeait que le code mettait en danger la sécurité des utilisateurs…[lire la suite]

Notre métier : Sensibiliser les décideurs et les utilisateurs aux risques liés à la **Cybercriminalité** et à la **Protection des Données Personnelles** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Denis JACOPINI anime dans toute le France et à l'étranger des conférences, des tables rondes et des formations pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles (Mise en Place d'un Correspondant Informatique et Libertés (CIL) 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 : Yahoo espionne tous vos e-mails pour le compte de la NSA ou du FBI – Tech – Numerama

Campagne de fraude ciblant les utilisateurs American Express – Data Security BreachData Security Breach

Campagne de fraude ciblant les utilisateurs American Express

On n'apprend jamais des erreurs des autres, en tout cas, c'est qu'il faut croire après le nombre élevé d'utilisateurs American Express victimes de la plus récente attaque de phishing.

Les attaques de phishing ciblées deviennent de plus en plus difficiles à détecter. Voilà pourquoi il est important de toujours redoubler de vigilance dans la vérification d'adresses des expéditeurs, même si elles peuvent sembler venir de sources sûres. Dans l'escroquerie American Express, les pirates ont envoyé des e-mails en se faisant passer pour la société, et en reproduisant un modèle fidèle de mail de l'entreprise, ils sont allés jusqu'à créer un faux processus de configuration, pour installer une « clé personnel de protection personnel American Express.
Les e-mails frauduleux exhortent les clients à créer un compte pour protéger leur ordinateur contre les attaques de phishing -quelle ironie !-. Lorsque les utilisateurs cliquent sur le lien dans le mail, la page vers laquelle ils sont redirigées, leur demande des informations privées telles que le numéro de sécurité sociale, date de naissance, nom de jeune fille de la mère, date de naissance, e-mail et tous les détails de leurs cartes American Express, y compris les codes et la date d'expiration.
L'augmentation massive des attaques de ce type devrait sensibiliser les utilisateurs à ne jamais répondre à des e-mails suspects, mais il est toujours difficile de distinguer le vrai du faux, surtout si l'utilisateur n'est pas doué en informatique ou s'il ne maitrise pas bien l'Internet…[lire la suite]

Notre métier : Sensibiliser les décideurs et les utilisateurs aux risques liés à la **Cybercriminalité** et à la **Protection des Données Personnelles** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Denis JACOPINI anime dans toute le France et à l'étranger des conférences, des tables rondes et des formations pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles (Mise en Place d'un Correspondant Informatique et Libertés (CIL) 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 : Campagne de fraude ciblant les utilisateurs American Express – Data Security BreachData

Security Breach