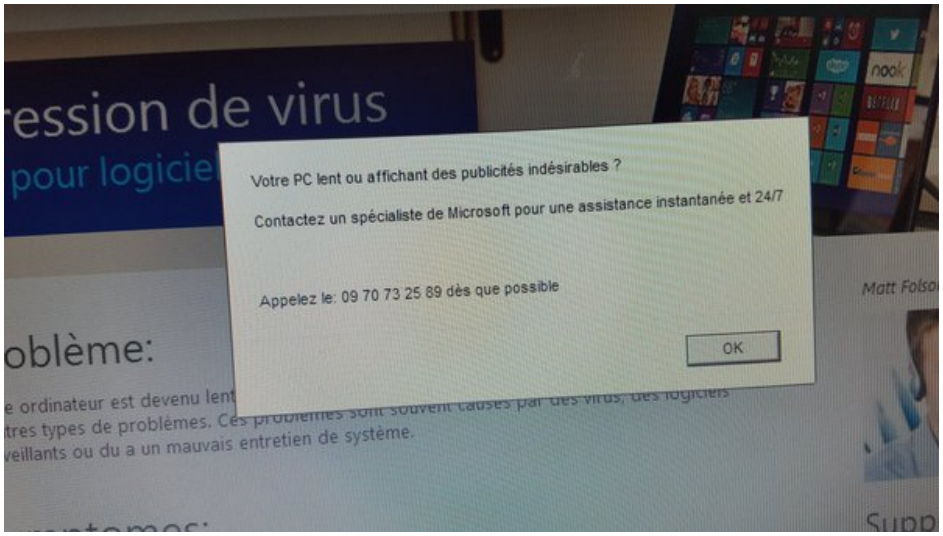
FakeAlert : Découverte d’une infection qui touche la France



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

Alerte : le gestionnaire de mots de passe SplashID piraté

	Alerte : le gestionnaire de mots de passe SplashID piraté

Le gestionnaire de mots de passe SplashID a été victime d'un piratage. Une base de données complète lui appartenant est en vente sur le Dark Web.

SplashID victime d'un piratage d'envergure

Alors qu'en début d'année, c'est le gestionnaire de mots de passe de Trend Micro qui avait vu son image écorner après la découverte de nombreuses failles dans ce logiciel, voilà qu'un concurrent vient de connaître pareille mésaventure.
Eh oui, au cours des derniers jours semble-t-il, SplashID a été victime d'un très vaste piratage qui a permis à des hackers, probablement en exploitant des failles décelées au niveau du coffre-fort numérique, de dérober la base de données complète du gestionnaire de mots de passe.
C'est d'ailleurs celle-ci qui a été retrouvée sur le Dark Web au prix de 8,5 bitcoins soit un peu plus de 4600€.

Un gestionnaire de mots de passe en ligne qui montre ses limites

Si les services comme SplashID peuvent sembler très pratiques puisqu'il est possible de s'y connecter très simplement depuis n'importe quel terminal, fixe ou mobile, ils présentent toutefois d'importants risques sur le plan sécuritaire.
Eh oui, parce que ce type de services est en ligne, il est potentiellement exposé à de nombreuses menaces alors qu'un service hors-ligne est par essence plus sécurisé.
Reste que dans l'affaire SplashID, l'inquiétude des internautes est grande puisque la société qui gère le service ne s'est pour l'instant pas exprimée à propos du piratage dont elle a été victime. Or, les rumeurs laissent entendre que les cybercriminels détiendraient encore un accès dérobé au serveur à ce jour !…[lien vers l'article informanews]

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

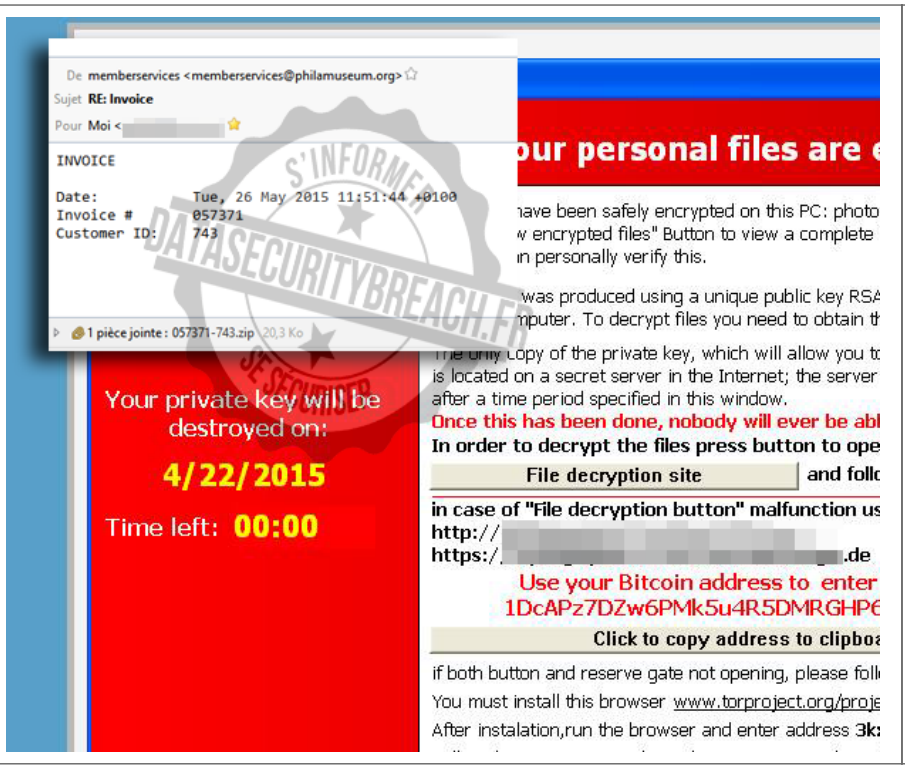
Contactez-nous

Réagissez à cet article

Original de l’article mis en page : SplashID piraté, des mots de passe dans la nature

---

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

L’accord Privacy Shield entre en vigueur

L’accord Privacy Shield entre en vigueur

[par le Général d'armée (2S) Marc Watin-Augouard, Fondateur du FIC et Directeur du CREOGN]
Il y a quelques semaines, le Privacy Shield vient d'être adopté en remplacement du Safe Harbor. Cet accord, relatif à la protection des données à caractère personnel des Européens, est un progrès, même s'il suscite des réserves de la part du G29. Sa révision en 2017 sera l'occasion de faire un premier bilan.

Les principes du Safe Harbor ont été établis pour protéger les données à caractère personnel, conformément aux dispositions de l'ancienne directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995, encore en vigueur jusqu'au 25 mai 2018. Celle-ci impose un niveau élevé de protection des droits et libertés des personnes, équivalent dans tous les États membres, en particulier pour permettre la libre circulation de leurs données à l'intérieur de l'Espace économique européen (EEE). Elle interdit le transfert de données à caractère personnel vers un pays tiers, lorsque celui-ci n'offre pas un « niveau de protection adéquat ».
La décision d'adéquation du 26 juillet 2000 de la Commission 2000 relative à la pertinence de la protection assurée par les principes de la « sphère de sécurité » reconnaissait que les transferts entre l'Union et les États-Unis répondaient aux conditions. La décision ne visait pas le secteur financier ou bancaire concerné par l'accord SWIFT[1]. Elle ne s'appliquait pas non plus lorsque sont établies des règles internes de transfert de données (*Binding Corporate Rules* ou BCR) validées par les 28 régulateurs nationaux (à vrai dire un seul en vertu du principe de reconnaissance mutuelle), des « clauses contractuelles types » élaborées par la Commission européenne, ou lorsque le transfert répond aux conditions définies par l'article 69 de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés[2].
La décision de la Commission a été annulée par l'arrêt CJUE C-362/14 *Maximillian Schrems/ Data Protection Commissionner* du 6 octobre 2015. L'arrêt concernait plus de 4000 entreprises américaines implantées en Europe directement affectées par ses conséquences. Tout en étant salué par les défenseurs des droits de l'internaute, il inquiétait les milieux économiques, notamment les PME. Celles-ci ne disposent pas, en effet, de services juridiques suffisamment étoffés pour établir des clauses contractuelles type, des règles internes d'entreprises, ou d'obtenir des autorisations de la CNIL (art.69 de la loi du 6 janvier 1978) prévoyant le transfert de données hors du Safe harbor.
Le 26 octobre, la commissaire européenne à la justice, Vera Jourová, annonce un « Safe Harbor II », preuve que l'urgence est prise en compte. La Commission, sommée de présenter un nouvel accord avant le 31 janvier 2016, accélère les négociations (déjà engagées auparavant) en vue d'aboutir à un texte pouvant être jugé satisfaisant, notamment par le G29. Elle présente ainsi, le 29 février 2016, son projet de «décision sur le caractère adéquat du niveau de protection», ainsi que les textes (*Privacy Shield Principles*) qui composeront le «bouclier de protection des données UE-États-Unis».

Les grandes lignes du Privacy Shield peuvent être ainsi résumées :
1/ Les entreprises seront soumises à des obligations assorties de mécanismes de surveillance permettant de les sanctionner ou de les exclure. Les nouvelles règles comprennent également des conditions plus strictes pour les transferts à d'autres partenaires par les entreprises adhérant au dispositif.
2/ L'accès par les autorités américaines sera étroitement encadré et transparent: le gouvernement américain, par la voix du directeur du renseignement national, a donné par écrit des garanties à l'UE. Tout accès des pouvoirs publics aux données à des fins de sécurité nationale sera subordonné à des limitations, des conditions et des mécanismes de supervision bien définis, qui empêcheront un accès généralisé aux données personnelles. Un mécanisme de médiation, indépendant des services de sécurité nationaux, sera mis en place.
3/ La protection des citoyens de l'UE sera mieux assurée par un mécanisme de règlement extrajudiciaire des litiges, accessible sans frais. Les entreprises visées devront apporter une réponse aux plaintes dans les 45 jours. Les citoyens de l'UE pourront également s'adresser à leur autorité nationale chargée de la protection des données, qui collaborera avec la Federal Trade Commission (Commission fédérale du commerce), un mécanisme d'arbitrage étant disponible, en dernier ressort, pour trouver une solution.
4/ Un réexamen annuel conjoint sera opéré par la Commission européenne et le ministère américain du commerce, associant des experts travaillant au sein des autorités américaines et européennes de protection des données. La Commission organisera une rencontre annuelle avec des ONG et des parties prenantes dans le domaine du respect de la vie privée, pour débattre de l'évolution plus générale de la législation américaine sur la vie privée et de ses répercussions pour les citoyens européens. Elle adressera un rapport annuel public au Parlement européen et au Conseil.
Après la promulgation par Barack Obama, le 24 février, de la loi sur le recours juridictionnel (*Judicial Redress Act[3]*),la Commission ouvre la procédure de signature de l'accord-cadre. Le dispositif doit être adopté par le Collège des commissaires européens, après consultation d'un comité composé de représentants des États membres et après avis des autorités européennes chargées de la protection des données (G29). Entre-temps, les États-Unis doivent mettre en place le nouveau cadre et les mécanismes de contrôle et de médiation. Le 13 Avril 2016, le G29 a fait savoir, par la voix de sa présidente Isabelle Falque-Pierrotin, que le texte constitue une avancée encore perfectible.
La décision sur la conclusion de l'accord est adoptée par le Conseil, le 12 juillet 2016, après approbation du Parlement européen. Elle entrera en vigueur dès sa notification aux États membres. Le 25 juillet 2016, le G29 se réunit et maintient sa position. Parmi les points suscitant les critiques, l'absence de garanties sur l'abandon de la surveillance massive des données des Européens par les services américains, les doutes sur l'impartialité du médiateur et les difficultés que peuvent rencontrer les plaignants. Tout citoyen européen peut en effet se tourner vers la justice américaine, mais, comme le souligne le G29, ce mécanisme pourrait s'avérer trop complexe, notamment lorsqu'ils ne sont pas anglophones. L'accord doit être révisé chaque année. Lors de sa participation à sa réévaluation, le G29 « cherchera à savoir si les problèmes soulevés à l'égard du texte ont été résolus, mais aussi à déterminer si les garde-fous mis en place par le texte sont fonctionnels et effectifs ».
Quoi qu'il en soit, on notera que la démarche isolée d'un homme de 27 ans, s'engageant dans la brèche ouverte par les révélations d'Edward Snowden, remet en cause tout un dispositif engageant 29 Etats. Une démonstration supplémentaire de l'extraordinaire pouvoir asymétrique qu'ont les particuliers dans l'espace numérique.

[1] Accord passé le 28 juin 2010 entre l'UE et les Etats-Unis permettant à ces derniers d'accéder aux données bancaires des européens stockées sur le réseau de la Society for Worldwide Interbank Financial Telecommunication.
[2] Le transfert est expressément accepté par la personne concernée ou réponde à des conditions énumérées par l'article 69 (sauvegarde de la vie de la personne, d'un intérêt public, exercice ou défense d'un droit en justice, etc.)
[3] Cette loi permet aux européens d'engager des actions civiles aux Etats-Unis en cas de violation des règles relatives à leurs données à caractère personnel.

Merci mon Général pour votre clarté ! [Denis JACOPINI]

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, attaques 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 : L'accord Privacy Shield entre en vigueur [par le Général d'armée (2S) Marc Watin-Augouard, Fondateur du FIC et Directeur du CREOGN] | Observatoire FIC

Gestion des mots de passe : Où en sont nos comportements ?

Gestion des mots de passe : Où en sont nos comportements ?

Les internautes ont conscience du risque. Malgré tout, 61 % réutilisent les mêmes mots de passe sur différents comptes, selon une enquête internationale de Lab42 pour LastPass.

Malgré les recommandations en faveur de l'utilisation de mots de passe robustes, malgré la médiatisation de violations de données à grande échelle (Yahoo, LinkedIn…), la réutilisation de mots de passe aisément mémorisables est une pratique courante. C'est le principal enseignement d'un sondage réalisé par la société d'études Lab42 pour le gestionnaire de mots de passe LastPass.
L'enquête a été menée en mai dernier auprès d'un échantillon de 2000 internautes majeurs dans 6 pays : France, Allemagne, Royaume-Uni, États-Unis, Nouvelle Zélande et Australie.

Déni et prise de risque

Malgré la compréhension du risque (pour 91 % du panel), 61 % des internautes interrogés réutilisent les mêmes mots de passe sur différents comptes, sites et services en ligne. Autre enseignement du sondage : l'oubli d'un mot de passe est la principale raison à l'origine d'un changement. Seulement 29 % des personnes interrogées changent de mot de passe pour des raisons de sécurité.
La majorité rationalise le fait d'utiliser des mots de passe « *faibles* ». Près de la moitié des répondants (identifiés comme des personnalités de Type A par le Lab42) veulent garder le contrôle et mémoriser les mots de passe utilisés. Ils pensent ainsi ne pas être directement menacés.
En revanche, plus de 50 % des répondants (identifiés comme des personnalités de type B) disent limiter leur activité en ligne par crainte d'une violation de mots de passe. Ils parviennent à se convaincre que leurs données n'ont pas de valeur pour les hackers. Et maintiennent ainsi une approche distante, voire négligente en ce qui concerne la sécurité des mots de passe…[lire la suite]

Réagissez à cet article

Original de l'article mis en page : Mots de passe : le déni et la prise de risque exposés

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

Un sous-traitant de la NSA accusé de vol de données secrètes

Un sous-traitant de la NSA accusé de vol de données secrètes

’affaire est embarrassante pour la National Security Agency (NSA). Le ministère américain de la justice a annoncé, mercredi 5 octobre, l’arrestation d’un homme soupçonné d’avoir volé des données classées « top secret » alors qu’il travaillait pour une agence fédérale, identifiée comme la NSA par le New York Times.

L’homme arrêté, Harold Thomas Martin III, travaillait comme sous-traitant à l’agence de renseignement américaine, spécialisée dans l’espionnage des communications mondiales. Il était employé par Booz Allen Hamilton, un grand groupe privé américain qui fournit de nombreux sous-traitants aux agences du renseignement des Etats-Unis.
« Lorsque nous avons appris l’arrestation de notre employé, nous avons immédiatement joint les autorités fédérales pour proposer notre totale coopération, et nous avons licencié » le sous-traitant, a confirmé, mercredi, dans un communiqué Craig Veith, le vice-président de Booz Allen Hamilton.

Embarrassant pour la NSA

Pour la deuxième fois en trois ans, la NSA voit l’un de ses sous-traitants dérober des informations ultrasecrètes. Edward Snowden, qui a révélé au grand public l’ampleur des programmes de surveillance de la NSA, était également un sous-traitant de Booz Allen Hamilton. La NSA n’a pas répondu aux sollicitations de l’Agence France-Presse.
Selon le *New York Times*, M. Martin est *« soupçonné d’avoir pris les codes source très secrets développés par la NSA pour s’introduire dans les systèmes informatiques d’adversaires comme la Russie, la Chine, l’Iran et la Corée du Nord »*.
L’acte d’accusation se borne à mentionner que M. Martin a emporté chez lui du matériel informatique et des documents confidentiels qui n’auraient jamais dû sortir du bureau où il travaillait. Il encourt respectivement un an et dix ans de prison pour ces faits, selon la même source.
[Source : Le Monde]

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 : Etats-Unis : un sous-traitant de la NSA accusé de vol de données secrètes

---

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

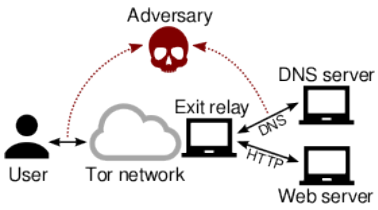
Original de l'article mis en page : Campagne de fraude ciblant les utilisateurs American Express – Data Security BreachData

Désanonymiser Tor. Possible ?

Désanonymiser Tor. Possible ?

Des chercheurs ont étudié la variante d'une attaque par corrélation permettant de démasquer les utilisateurs du réseau d'anonymisation Tor. « DefecTor » est centrée sur les requêtes DNS.

Des chercheurs de Princeton, aux État-Unis, et des universités Karlstad et KTH, en Suède, ont étudié la faisabilité d'une méthode permettant de démasquer les utilisateurs du réseau d'anonymisation Tor. Leurs travaux orientés sur le DNS sont en ligne (*« The Effect of DNS on Tor's Anonymity »*).
L'attaque nommée DefecTor est une variante d'une attaque par corrélation centrée sur les requêtes DNS (Domain Name System). Elle est possible car Tor Browser, le navigateur qui permet aux internautes d'accéder au réseau Tor, regroupe et chiffre le trafic HTTP et le trafic DNS. Ensuite la requête DNS est traitée au niveau du noeud de sortie, et le trafic HTTP est envoyé vers sa destination…[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 : DefecTor : s'appuyer sur

le DNS pour désanonymiser Tor

Alerte aux vidéo piégées sur Facebook

Alerte aux vidéo piégées sur Facebook

Technique de piratage baptisée Eko : de fausses vidéos sur Facebook piègent les internautes un peu trop curieux.

Il y a comme un … Eko dans le tuyau ! Cette technique de piratage n'est pas nouvelle. Elle a eu son « heure » de gloire lors de grands rendez-vous médiatiques dramatiques (*11 septembre, tsunami en Thaïlande…*). L'idée, inciter les internautes, utilisateurs de Facebook, à partager une vidéo. Les malveillants profitent de ces surfeurs qui partagent sans même vérifier le contenu partagé. La vidéo, n'est qu'un piège. Il s'agit d'inciter les utilisateurs du portail américain à se rendre sur une page. Espace numérique qui affiche une vidéo qui a besoin d'un plugin, d'une mise à jour logiciel de votre ordinateur pour être regardée. Bien entendu, ne participez surtout pas à ce « *diner de cons*« , vous en seriez l'invité vedette. Dans cette mise à jour, un piège. Vous avez le choix entre un virus qui se chargera de prendre en main votre machine, ou encore un ransomware qui vous extorquera de l'argent si vous souhaitez récupérer vos photos, documents…[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 : ZATAZ Eko : vidéo piégée sur Facebook – ZATAZ