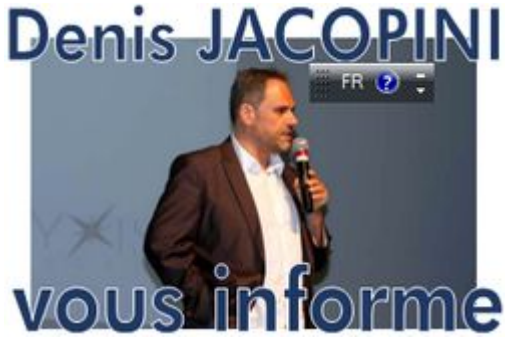
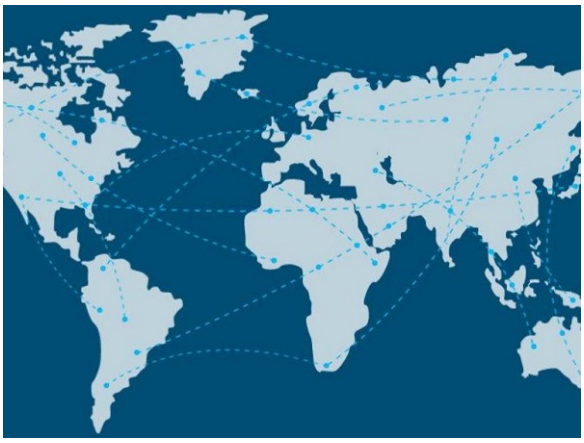
900 000 routeurs de Deutsche Telekom infectés par un malware



900 000 routeurs de Deutsche Telekom infectés par un malware

Deutsche Telekom a confirmé la thèse d'un malware ayant infecté plus de 900.000 de ses routeurs. Selon Flashpoint, environ 5 millions de routeurs à travers le monde seraient vulnérables à la faille exploitée par cette variante de Mirai.

Le Cert-FR alerte les utilisateurs français sur cette attaque. L'équipe rappelle ainsi que « plusieurs version du binaire malveillant sont en circulation ». Le Cert-FR recommande de changer les mots de passe par défaut, de restreindre l'accès aux outils d'administration et de désactiver « les services inutilement lancés sur les équipements exposés sur le réseau. »
Mirai se tourne vers de nouvelles cibles et la nouvelle version du ver informatique s'attaque maintenant aux routeurs. On avait déjà constaté par le passé des variantes de ce malware modifiées afin de s'attaquer à de nouveaux appareils. Mais l'attaque ayant visé Deutsche Telekom montre que les opérateurs de cette nouvelle variante entendent maintenant changer de cible et délaisser les objets connectés pour s'attaquer aux routeurs.



Comme l'explique Flashpoint dans une note de blog, la mise à disposition du code source de Mirai par son créateur a entraîné une guerre entre les cybercriminels, alors que plusieurs groupes tentaient d'utiliser Mirai pour prendre le contrôle du maximum d'objets connectés vulnérables. « L'évolution logique pour ce malware était de découpler le mécanisme d'infection de la charge utile du malware, en exploitant un nouveau vecteur d'attaque » précise ainsi Flashpoint sur son blog.
La dernière déclinaison de Mirai n'exploite donc plus simplement Telnet pour tenter de se connecter à des objets connectés en utilisant les identifiants par défaut. Selon Flashpoint, celle-ci exploite des vulnérabilités connues au sein des protocoles TR-064 et TR-069, des protocoles de maintenance utilisés par les opérateurs. C'est grâce à cette faille que les opérateurs du réseau botnet sont parvenus à infecter plus de 900.000 routeurs livrés par Deutsche Telekom à ses clients. Mais selon Flashpoint, l'opérateur allemand n'est pas le seul à devoir s'inquiéter de ce type d'attaques. Flashpoint évoque ainsi le fait que des appareils infectés ont également été détectés au Brésil et en Grande-Bretagne. Selon Flashpoint, environ 5 millions de routeurs à travers le monde sont vulnérables à cette nouvelle variante.
Reste à déterminer l'origine de l'attaque contre l'opérateur. Flashpoint précise que les administrateurs de cette variante semblent être des habitués de Mirai, puisque le nouveau malware présente plusieurs points communs (notamment des serveurs de command and control) avec des Botnets déjà identifiés lors d'attaques précédentes effectuées grâce à Mirai.
Selon le journal allemand Tagesspiegel, les soupçons se tournent vers la Russie. Dans une prise de parole, la chancelière Angela Merkel s'est refusée à confirmer cette thèse, mais précise néanmoins que de nombreuses cyberattaques ont été constatées en Europe et appelle ses citoyens à s'habituer à ce type d'attaques. Cité par la presse locale, le directeur de l'équivalent allemand de l'Anssi, le BSI, évoque de son côté « le crime organisé » à l'origine de l'attaque, mais rappelle que l'attaque n'a pas fonctionné. Le malware a bien déconnecté les routeurs des abonnés, mais celui-ci n'est pas parvenu à s'installer correctement. Plus de peur que de mal donc…[lire la suite]

Notre métier : Sensibiliser les décideurs et les utilisateurs. Vous apprendre à vous protéger des pirates informatiques, vous accompagner dans votre mise en conformité avec la CNIL et le règlement Européen sur la Protection des Données Personnelles (RGPD). (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

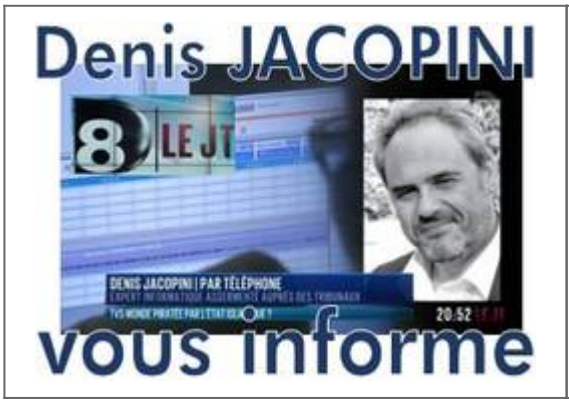
Contactez-nous

Réagissez à cet article

Original de l’article mis en page : Deutsche Telekom : 5 millions de routeurs vulnérables au malware – ZDNet

---

Une cyberattaque sur quatre réussit en France (Accenture)



En France, une cyberattaque sur quatre réussit

Les entreprises françaises subiraient deux ou trois cyberattaques effectives par mois, selon le cabinet de conseil Accenture.

C'est une nouvelle statistique inquiétante pour les entreprises. Plus d'une attaque ciblée sur quatre a abouti à une violation effective des dispositifs de sécurité au cours des douze derniers mois en France, selon une étude du cabinet de conseil Accenture. L'enquête a été menée auprès de 2.000 dirigeants, en charge de la sécurité dans les entreprises réalisant un chiffre d'affaire d'au moins un milliard de dollars et basées dans 15 pays, dont la France (124 répondants). Douze secteurs sont concernés par cette enquête : assurance, banque, marchés de capitaux, communication, énergie, santé, hautes technologies, sciences de la vie, produits de consommation, équipement industriel, distribution, utilities.

Cette statistique équivaut en moyenne, à deux ou trois attaques effectives par mois et par entreprise en France. Ainsi, sur 114 tentatives d'intrusion identifiées dans l'Hexagone sur un an, 32 ont réussi, assure-t-on à La Tribune. Plus d'un quart (28%) des tentatives d'intrusion réussies sont le fruit de hackers en France alors que la moyenne mondiale est à 19%.

Excès de confiance des Anglo-saxons?

En dépit de la fréquence des attaques, l'étude d'Accenture souligne un excès de confiance. Ainsi, la majorité des responsables interrogés (73%) se disent confiants dans leur capacité à protéger leur entreprise contre les cyberattaques. Ce qui reste loin, très loin de la réalité d'aujourd'hui. Ce n'est pas totalement le cas en France où les entreprises sont conscientes du danger en raison de la sensibilisation des pouvoirs publics (ANSSI, notamment) à travers la loi de programmation militaire. Ainsi, elles consacrent la plus grande partie de leurs dépenses informatiques (9,4 %) à la cybersécurité, par rapport à une moyenne mondiale de 8,2 %.

En revanche, les entreprises basées au Royaume-Uni (7,6%) et aux États-Unis (8%) sont celles qui dépensent le moins en pourcentage dans le domaine informatique pour répondre aux enjeux de cybersécurité. Résultat, la détection des intrusions semble prendre plus de temps aux États-Unis et au Royaume-Uni, où plus d'un quart des entreprises mettent plus d'un an pour identifier une attaque réussie : 30 % aux États-Unis et 26 % au Royaume-Uni.

Par ailleurs, les entreprises allemandes (52 %) et britanniques (50 %) sont les plus confiantes sur leurs capacités de suivi des incidents, par rapport à la moyenne mondiale (38 %). Ce qui ne les met pas à l'abri des attaques. Loin s'en faut. Ainsi Deutsche Telekom a très certainement dû faire face à une attaque informatique lundi : jusqu'à 900.000 foyers en Allemagne, clients de l'opérateur allemand rencontraient d'importants problèmes d'accès à internet, selon le groupe allemand.

« Les Anglo-saxons investissent dans des solutions packagées en estimant qu'elles sont les meilleures pour les mettre à l'abri des attaques mais ils ne traitent pas toutes les menaces », analyse le directeur d'Accenture Security en France.

Enfin, les entreprises basées en France, en Australie et aux États-Unis sont les plus pessimistes sur leur capacité à assurer une surveillance efficace des intrusions de sécurité, par rapport à la moyenne mondiale. « Plus on sait, plus on doute », confirme Stéphane Geyres…[lire la suite]

Notre métier : Former et Sensibiliser les décideurs et les utilisateurs. Vous apprendre à vous protéger des pirates informatiques, vous accompagner dans votre mise en conformité avec la CNIL et le règlement Européen sur la Protection des Données Personnelles (RGPD). (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 formations, des conférences et des tables rondes 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.

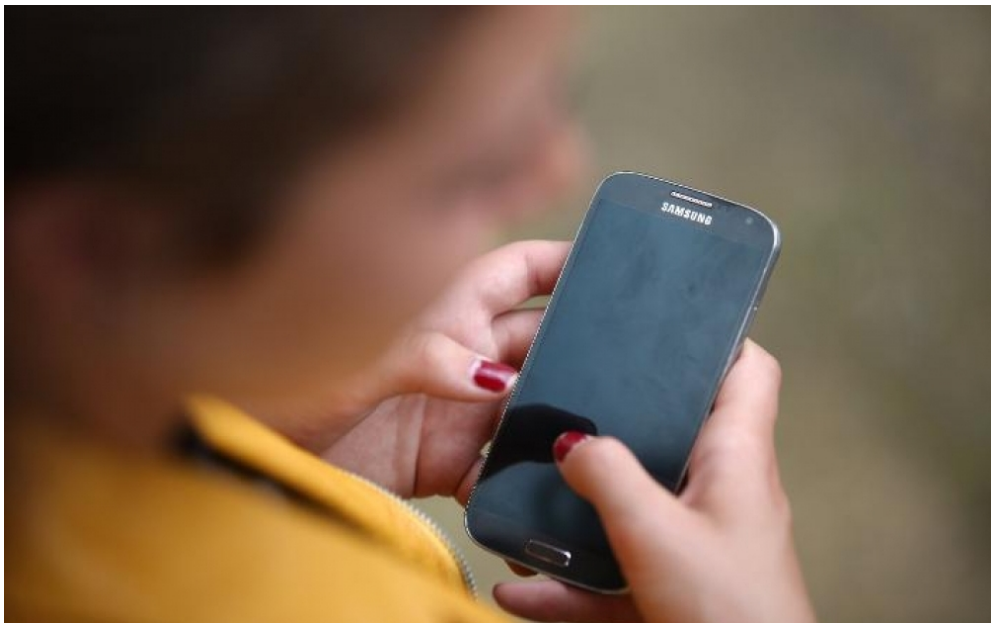
Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Original de l’article mis en page : Une cyberattaque sur quatre réussit en France (Accenture)

Alerte : 1 million de comptes Google dérobés. Outil gratuit pour vérivier votre compte



Alerte : 1 million de comptes Google dérobés. Outil gratuit pour vérivier votre compte

---

Un logiciel malveillant, ou malware, nommé Gooligan, a infecté plus d'un million de téléphones fonctionnant sur Android et permis à des pirates de dérober les données d'autant de comptes Gmail, a révélé aujourd'hui la compagnie israélienne spécialisée en solutions de sécurité, Check Point.
«Grâce à ces informations, les agresseurs peuvent accéder aux données confidentielles des utilisateurs dans Gmail, Google Photos, Google Docs, Google Play, Google Drive et G Suite», précise la compagnie dans un communiqué.

13 000 appareils infectés chaque jour

Gooligan infecterait 13 000 appareils par jour, en ciblant les appareils sur Android 4 (Jelly Bean, KitKat) et 5 (Lollipop), soit 74% des appareils Android aujourd'hui en usage. C'est la première fois qu'une cyberattaque de ce genre parvient à toucher plus d'un million d'appareils.
Selon Check Point, environ 57% de ces appareils infectés sont situés en Asie et environ 9% en Europe.

Comment fonctionne ce malware ?
L'infection se produit lorsqu'un utilisateur télécharge puis installe une application infectée par *Gooligan* sur un appareil Android vulnérable, ou s'il clique sur des liens malveillants dans des messages de *phishing*. «Une fois que les agresseurs parviennent à prendre le contrôle d'un appareil, ils gênèrent des revenus frauduleux en installant des applications à partir de Google Play et en les évaluant au nom de la victime», explique Check Point.

Vérifier l'état de son compte en ligne

Prévenu par la société israélienne, Google aurait contacté les utilisateurs concernés pour «désinfecter» les appareils touchés et ajouter de nouvelles protections à sa technologie Verify Apps.

Check Point propose un outil en ligne gratuit permettant aux utilisateurs d'Android de vérifier si leur compte n'a pas été infecté par *Gooligan*.
[Lien vers l'outil gratuit en ligne]

Réagissez à cet article

Original de l’article mis en page : Cyberattaque : les données d’un million de comptes Google dérobées par Gooligan – Le Parisien

---

La coopération Internationale renforcée dans le Cloud

	La coopération Internationale renforcée dans le Cloud

« Le quinzième anniversaire de la Convention de Budapest sur la cybercriminalité est un tournant dans la mesure où la Convention atteint maintenant les « nuages », a déclaré le Secrétaire Général du Conseil de l'Europe Thorbjørn Jagland lors de l'inauguration de la Conférence Octopus 2016.

Les données et donc les preuves électroniques sont de plus en plus stockées sur des serveurs relevant de juridictions étrangères, inconnus ou multiples. C'est pourquoi, il peut être extrêmement difficile pour les autorités chargées de la justice pénale d'obtenir régulièrement de telles preuves. Faute de celles-ci, les délinquants qui opèrent dans le cyberespace ne peuvent être poursuivis.
Le Secrétaire Général a salué le jeu de recommandations adoptées par le Comité de la Convention sur la cybercriminalité lors de sa réunion des 14-15 novembre, dans lesquelles il voit une réponse véritable au problème de l'informatique en nuage (cloud computing). Les recommandations prévoient la négociation d'un protocole additionnel à la Convention à partir du milieu de 2017.
« La coopération entre les Etats s'est considérablement améliorée. Cela est dû pour beaucoup au travail du Comité de la Convention. Les notes d'orientation adoptées par le Comité ont aidé à préserver la pertinence et l'actualité de la Convention, à renforcer notre capacité de combattre le terrorisme, le vol d'identités ou les attaques contre des infrastructures d'informations critiques », a déclaré le Secrétaire Général, qui a invité les gouvernements à mieux protéger les droits des particuliers dans le cyberespace.
« Nous avons élaboré une sorte de « triangle dynamique » – Convention, Comité et renforcement des capacités – si bien que la Convention de Budapest reste aujourd'hui le traité international le plus important sur la cybercriminalité et la preuve électronique », a-t-il conclu.
A l'occasion de la conférence, Andorre a ratifié la Convention en présence d'Eva Descarrega Garcia, Secrétaire d'Etat andorrane à la Justice et à l'Intérieur.
68 Etats sont soit déjà parties à la Convention de Budapest, soit se sont formellement engagés à la respecter. Au moins 70 pays de plus ont pris la Convention comme source d'inspiration pour élaborer leur législation interne.
[Discours de Thorbjørn Jagland (*anglais*)]

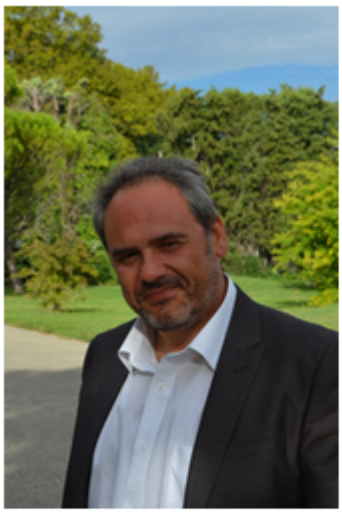
Original de l'article mis en page : Cybercriminalité : vers un nouvel outil juridique sur la preuve électronique – News

---

Plus de 380 000 comptes xHamster dérobés et mis en vente par des pirates

xHamster a subi une attaque d'une très grande ampleur : les pirates ont pris possession de de 380 000 comptes enregistrés sur le site pornographique. Des données qui sont désormais à vendre sur le deep web.…[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.

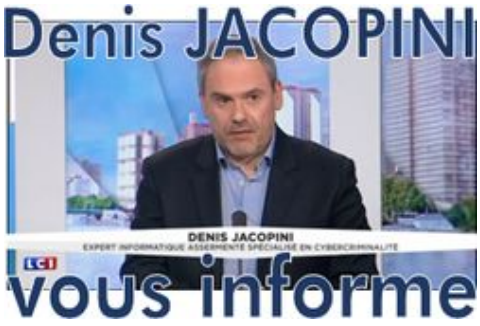
- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation 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

Les collectivités territoriales aussi concernées par la cybersécurité



Les collectivités territoriales aussi concernées par la cybersécurité

Pour mieux appréhender la transition numérique, les écoles de Saint-Cyr Coëtquidan organisent un colloque régional destiné aux collectivités territoriales,
Trois questions à…
Gérard de Boisboissel, ingénieur au centre de recherche des écoles Saint-Cyr Coëtquidan, organisateur du colloque.

En quoi la cybersécurité concerne les collectivités territoriales ?
La transformation numérique touche tout le monde, donc la protection des données aussi. Il y a des enjeux et des risques, les petites communes comme la région sont vulnérables car elles détiennent des données personnelles.

Quels types d'attaques sont les plus fréquentes ?
On observe plusieurs types d'attaques : le piratage ou cryptage de données mais aussi une prise de contrôle des sites Internet par des hackers. En janvier 2015, plusieurs sites bretons, dont celui de la mairie de Port-Louis (56), ont été piratés et présentaient une page d'accueil avec un message islamiste.

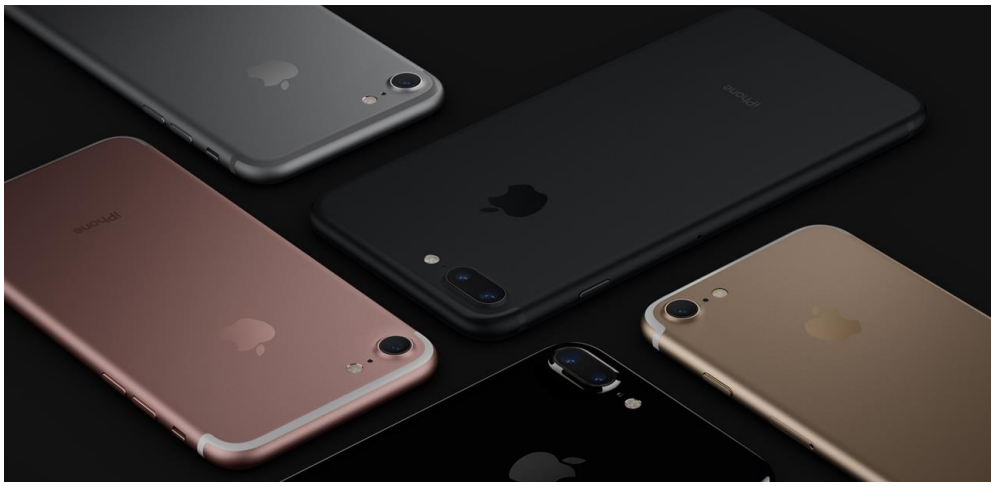
Comment se protéger ?
Si toutes les collectivités territoriales sont conscientes de la transformation numérique, les élus n'avancent pas tous au même rythme. Pendant le colloque, nous aborderons les bons réflexes à adopter : sauvegarder ses données en double, changer ses mots de passe régulièrement, et pourquoi pas désigner une personne dédiée à cette question. Vannes apportera son témoignage demain, car la ville a un référent cybersécurité et consacre 25 000 € à ce sujet…[lire la suite]

Réagissez à cet article

Original de l’article mis en page : Vannes. Les petites communes aussi concernées par la cybersécurité

---

iCloud indiscret sur nos journaux d’appels…



iCloud indiscret sur nos journaux d’appels…

La synchronisation iCloud envoie sur les serveurs d'Apple le journal des appels d'un appareil sous iOS, en remontant jusqu'à quatre mois. Une option sur laquelle l'utilisateur ne peut pas influer directement et qui nécessite une désactivation complète d'iCloud Drive pour être coupée. Pour la société, il ne s'agit que de simplifier la vie des clients.

iCloud, quand il est actif sur un appareil Apple, synchronise et sauvegarde de nombreux éléments : contacts, agendas, messages, réglages et ainsi de suite. L'idée est de simplifier la vie de l'utilisateur s'il vient à perdre son appareil ou tout simplement s'il en utilise plusieurs. La « réserve » de données est ainsi la même et il ne s'embarrasse pas de doublons et autres.

Une synchronisation active, même quand la sauvegarde iCloud est coupée

Mais iCloud synchronise aussi le journal des appels, ce qui n'est en fait mentionné nulle part. La découverte a été faite par Elcomsoft, à qui l'on doit déjà les révélations sur la fragilité du chiffrement dans les sauvegardes faites par iOS 10. Toutes les informations du journal d'appel sont présentes : les appels classiques émis et reçus, les appels FaceTime, et globalement tout ce qui peut y inscrire des évènements depuis iOS, comme Skype et WhatsApp.

Selon Elcomsoft, la seule manière de couper cette synchronisation, qui remonte le journal jusqu'à quatre mois en arrière, est de désactiver complètement iCloud Drive, un choix que l'on trouve dans les options du service dans iOS et macOS. Désactiver iCloud lui-même ne suffit pas.

Mais ce faisant, d'autres services peuvent ne plus fonctionner. WhatsApp, justement, se sert de Drive pour stocker ses sauvegardes. D'autres applications l'utilisent pour entreposer leurs documents et les synchroniser entre les machines de l'utilisateur. Il reste bien entendu le cas où cette révélation ne dérange pas l'utilisateur.

Une commodité, et pas seulement pour les utilisateurs

Pour Apple, il n'y a pas vraiment de problème, comme la firme l'a indiqué à *Forbes* : « *Nous offrons la synchronisation du journal d'appels comme une commodité à nos clients, pour qu'ils puissent rappeler depuis n'importe lequel de leurs appareils.* […]*L'accès aux données iCloud – y compris les sauvegardes – requiert l'identifiant Apple et le mot de passe. Nous recommandons à tous nos clients de choisir des mots de passe forts et d'utiliser l'authentification à deux facteurs* ».

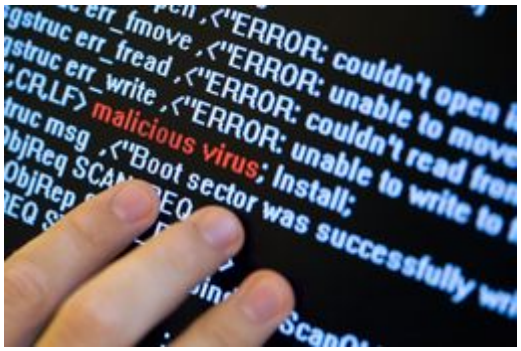
Tout irait bien donc à partir du moment où le mot de passe serait assez fort. Cependant, ce n'est pas aussi simple. L'affaire de l'iPhone 5c a certes montré qu'Apple ne pouvait pas déverrouiller par la force un appareil et récupérer les données (le code de verrouillage participe à la clé de chiffrement), mais iCloud, même s'il communique de manière chiffrée, dépose des données sur les serveurs de l'entreprise.

Or, comme pour iMessage, ces données sont disponibles sur demandes si les forces de l'ordre les réclament, dument armées d'un mandat. Une situation similaire à ce que l'on retrouve dans le domaine de la téléphonie mobile « classique » depuis des années.

L'expert Jonathan Zdziarski, interrogé par Forbes, a indiqué que rien n'empêchait en théorie Apple de basculer dans le chiffrement intégral pour l'ensemble de ses services. « *Mais d'un point de vue politique* » ajoute-t-il, « *cela pourrait déclencher une guerre avec certaines agences fédérales qui utilisent ces données quotidiennement* ». Une situation à ce qu'on a pu voir avec WhatsApp lors de son passage au chiffrement de bout-en-bout.

Original de l'article mis en page : Apple : iCloud synchronise sans accord les journaux d'appels

Les lanceurs d’alertes dans la Loi pour une République numérique



Les lanceurs d’alertes dans la Loi pour une République numérique

Les lanceurs d'alertes ou « white hats » interpellent de plus en plus les medias depuis quelques années. Ces hackers éthiques interviennent dans l'informatique et le numérique, ils veillent à avertir les responsables de la sécurité des SI des vulnérabilités de leurs systèmes d'information ou de leurs sites web.

De plus, avec le développement de plates-formes de bug bounty comme YesWeHack, il était important de légaliser une pratique exposée à des sanctions pénales (ex : art. 323-1 du code pénal, 2 ans de prison et 60.000 euros d'amende). La loi n° 2016-1321 du 7 octobre 2016 pour une République numérique vient préciser le cadre légal de leurs actions.

L'AFFAIRE DE L'ANSES ET LE VOL DE DONNÉES

Un journaliste-blogueur surnommé « Bluetouff » avait extrait, puis publié de nombreux fichiers confidentiels en pénétrant sur le site extranet de l'Agence nationale de sécurité sanitaire de l'alimentation, de l'environnement et du travail (ANSES). Il a été condamné par la Cour d'appel de Paris le 5 février 2014, puis par la Cour de cassation le 20 mai 2015 pour maintien frauduleux dans le SI et vol de données. Le législateur, « alerté » de cette situation, a commencé par modifier l'article 323-3 du code pénal en y ajoutant les actions d'extraire, de détenir, de reproduire, de transmettre frauduleusement des données (Loi n°2015-912 du 24 juillet 2015).

LA PREMIÈRE MOUTURE VISÉE À L'ARTICLE 20 SEPTIE DE LA LOI

C'est un amendement du 15 janvier 2016, dit « Bluetouff » qui a relancé les débats sur le sujet ayant abouti à la proposition d'ajouter un nouvel alinéa à l'article 323-1 du code pénal, ainsi rédigé :
« Toute personne qui a tenté de commettre ou commis le délit prévu au présent article est exempte de peine si elle a immédiatement averti l'autorité administrative ou judiciaire ou le responsable du système de traitement automatisé de données en cause d'un risque d'atteinte aux données ou au fonctionnement du système. »

Il était censé protéger les lanceurs d'alerte lorsqu'ils veillent *« à avertir les responsables de traitement des failles dans leurs systèmes.* » Or, cette rédaction laissait dubitatifs les juristes et posait plus de questions qu'elle n'en résolvait, notamment : quelle autorité saisir et par quel canal (appel téléphonique à la police, courrier postal ou électronique à une cour d'appel ou à la CNIL, etc.) ? Que se passe-t-il après l'avertissement et surtout, si entre temps le responsable du SI a porté plainte, ou encore si le lanceur d'alertes diffuse les informations sur l'internet pour se faire de la publicité ? De plus, exemption de peine ne signifie pas non inscription au casier judiciaire de la condamnation. Pourtant, une décision du 9 septembre 2009 a jugé que tout accès non autorisé à un SI constitue un trouble manifestement illicite alors même que cela peut permettre d'éviter des atteintes ultérieures aux données ou au fonctionnement du système.

LA PROTECTION NOUVELLE DES LANCEURS D'ALERTE

L'article 47 de la nouvelle loi prévoit que le code de la défense soit complété par un article L. 2321-4 ainsi rédigé : « *Art. L. 2321-4.- Pour les besoins de la sécurité des systèmes d'information, l'obligation prévue à l'*article 40 du code de procédure pénale *n'est pas applicable à l'égard d'une personne de bonne foi qui transmet à la seule autorité nationale de sécurité des systèmes d'information une information sur l'existence d'une vulnérabilité concernant la sécurité d'un système de traitement automatisé de données. »*
« L'autorité préserve la confidentialité de l'identité de la personne à l'origine de la transmission ainsi que des conditions dans lesquelles celle-ci a été effectuée. »
« L'autorité peut procéder aux opérations techniques strictement nécessaires à la caractérisation du risque ou de la menace mentionnés au premier alinéa du présent article aux fins d'avertir l'hébergeur, l'opérateur ou le responsable du système d'information. »

L'information vise les vulnérabilités de sécurité des SI (art. 323-1) mais sans doute pas les autres délits informatiques prévus aux articles 323-2 (entraver et fausser le fonctionnement d'un SI), 323-3 (introduction de données, extraction, transmission, reproduction, suppression, modification des données) et 323-3-1 (programmes malveillants), ainsi que les infractions commises en groupe ou en bande organisée. Ces dernières infractions peuvent, en effet, causer des dommages importants au responsable du SI. L'un des points essentiels sera de déterminer les conditions de la *bonne foi* de la personne ayant détecté la vulnérabilité, étant observé que si la personne agit dans le cadre d'un programme de Bug bounty, on peut supposer que la bonne foi est présumée dans la mesure où le programme est déterminé par l'utilisateur, c'est à dire l'entreprise (idem pour la société qui réalise un Pentest).Il en va de même, si l'informateur a pénétré dans le site et qu'il s'en retire dès le moment où il s'aperçoit qu'il accède à une partie du site ou des données protégées…[lire la suite]

Notre métier : Sensibiliser les décideurs et les utilisateurs. Vous apprendre à vous protéger des pirates informatiques, vous accompagner dans votre mise en conformité avec la CNIL et le règlement Européen sur la Protection des Données Personnelles (RGPD). (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

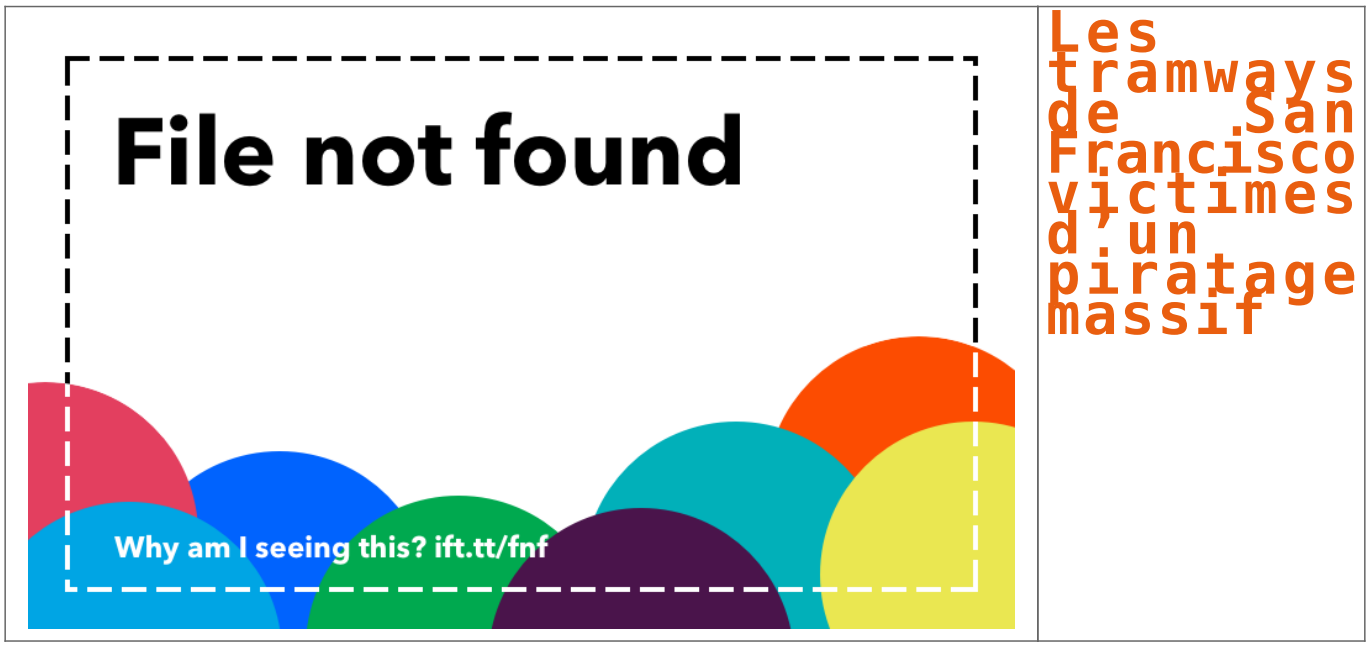
Contactez-nous

Réagissez à cet article

Original de l'article mis en page : Les lanceurs d'alertes dans la Loi pour une République numérique

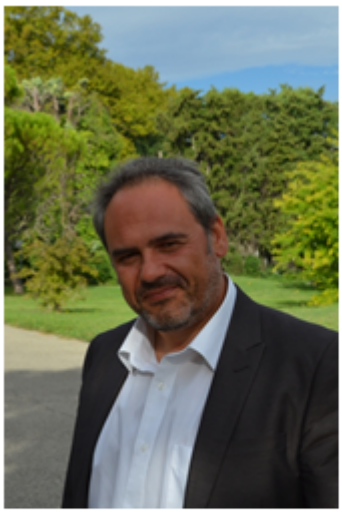
---

Les tramways de San Francisco victimes d'un piratage massif



Ce week-end, l'ensemble du réseau de transport de San Francisco a été la cible d'une attaque, qui a paralysé les ordinateurs gérant les tickets et le trafic. L'opération visait à soutirer de l'argent en échange de données cryptées.…[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.

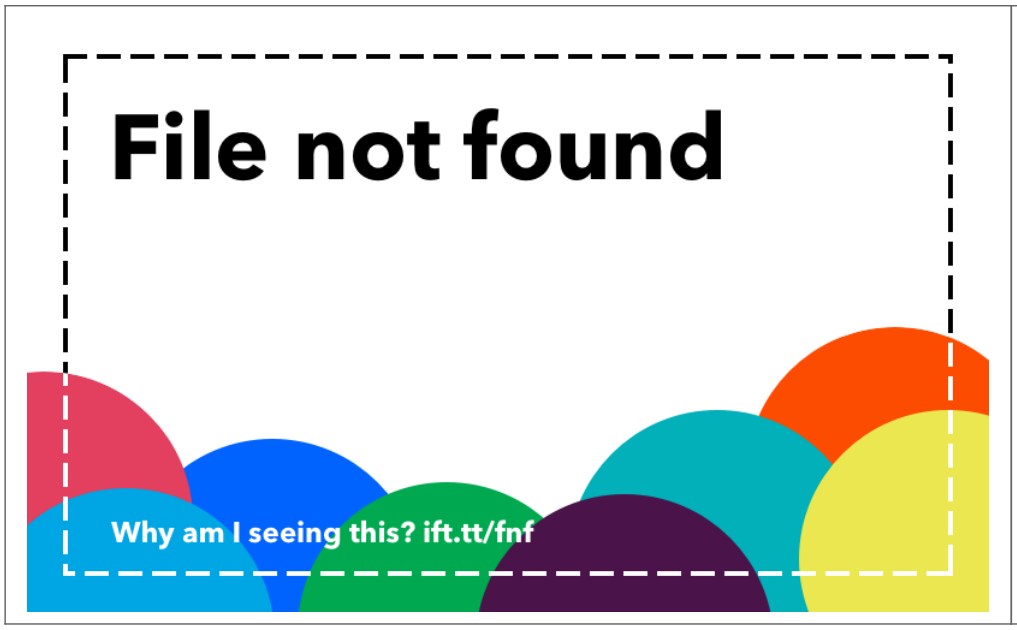
- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation 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

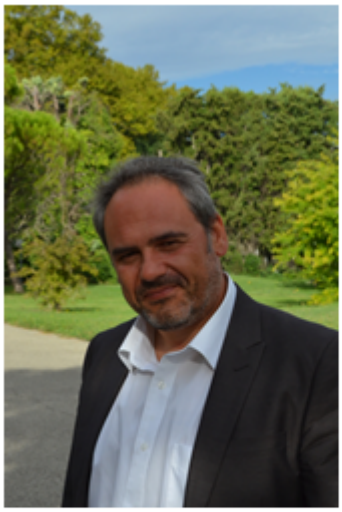
La Commission européenne mise à terre par une attaque DDoS



La Commission européenne mise à terre par une attaque DDoS

Les attaques DDoS ont fait une nouvelle victime hier, jeudi 24 novembre : la Commission européenne. L'institution a confirmé l'information à Politico.…[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