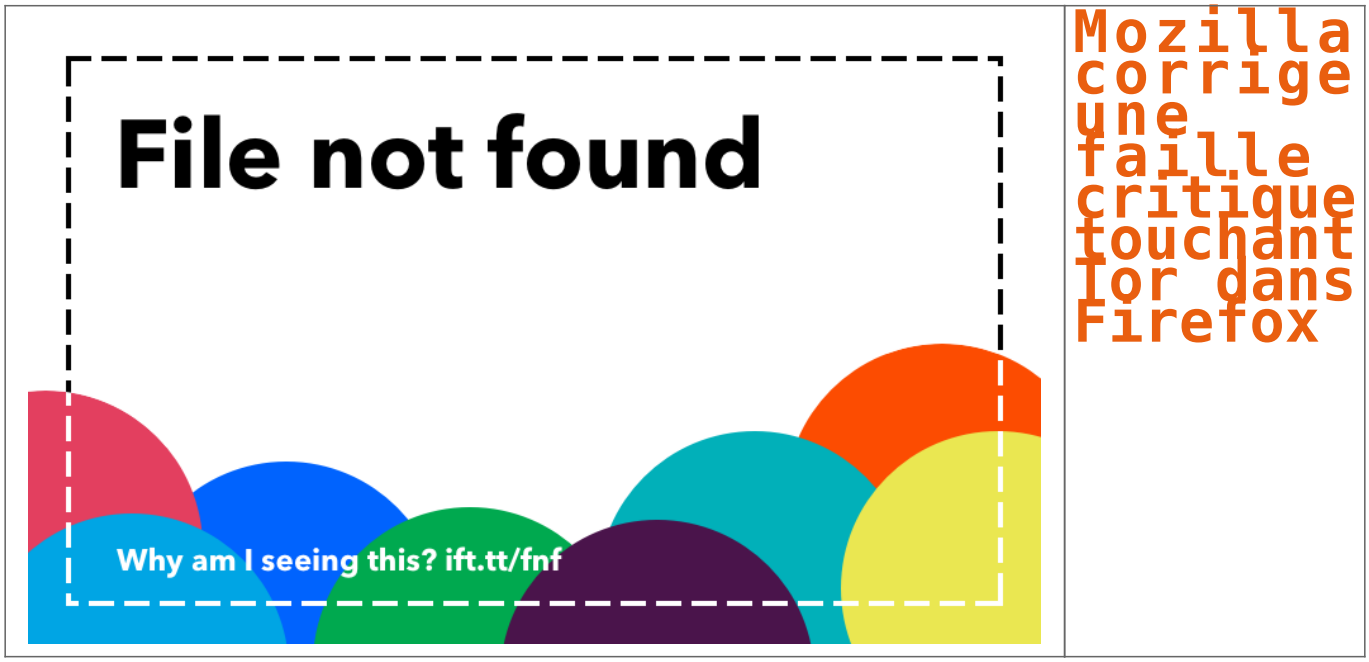
# Mozilla corrige une faille critique touchant Tor dans Firefox

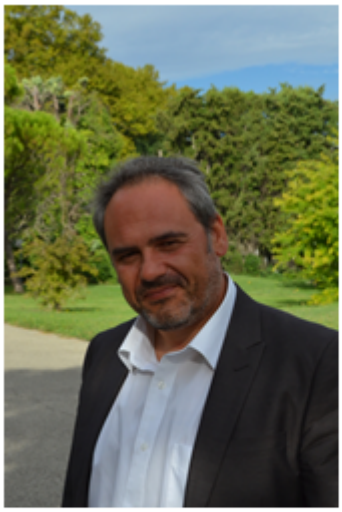



**« Mozilla a publié une mise à jour de Firefox contenant un correctif pour une vulnérabilité signalée comme étant activement utilisée pour désanonymiser les utilisateurs de Tor Browser.…**[Lire la suite ]

---

Denis JACOPINI Expert en cybercriminalité et en protection des données personnelles réalise des audits sécurité, vous explique comment vous protéger des pirates informatiques et vous aide à vous mettre en conformité avec le règlement Européen sur la protection des données personnelles. Audits sécurité, animations de formations en cybercriminalité et accompagnement à la mise en conformité avec le règlement sur la protection des données personnelles.. (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

---

# AirDroid : une faille de sécurité critique vient d'être découverte

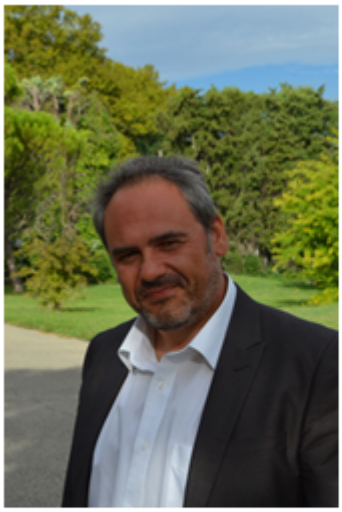
# AirDroid : une faille de sécurité critique vient d'être découverte

**AirDroid fait la une de tous les médias depuis quelques heures, et pas forcément pour les bonnes raisons. Des experts en sécurité ont effectivement trouvé une nouvelle faille critique en examinant la solution.…**[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.

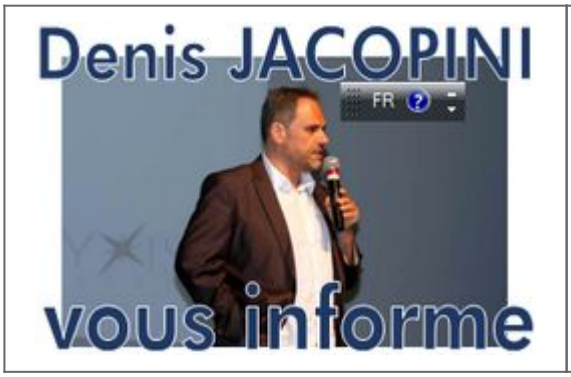
Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

---

# 900 000 routeurs de Deutsche Telekom infectés par un malware

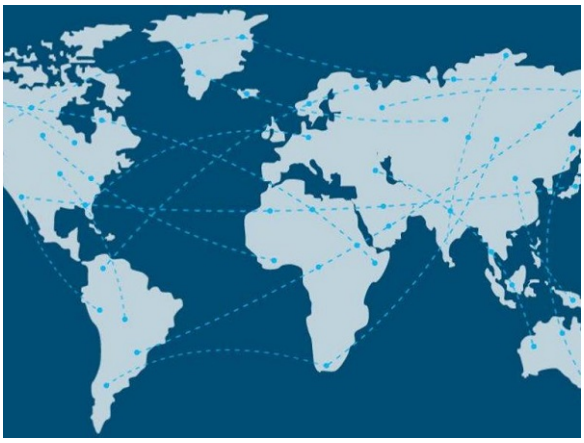



900 000 routeurs de Deutsche Telekom infectés par un malware

---

**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

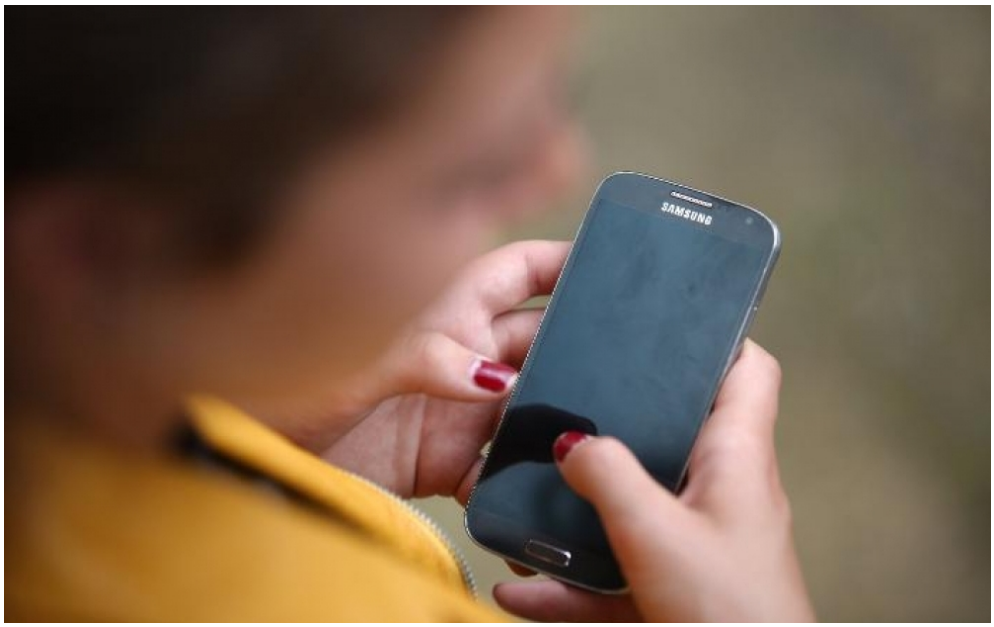
Contactez-nous

Réagissez à cet article

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

---

# 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]

---



---

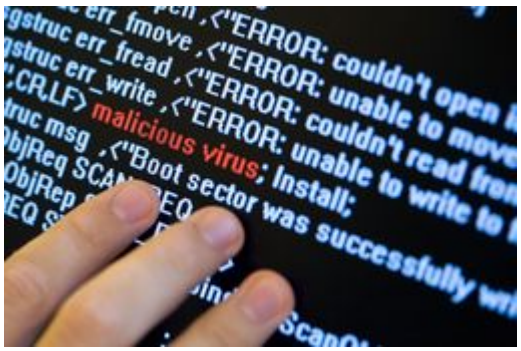


Réagissez à cet article

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

---

# 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

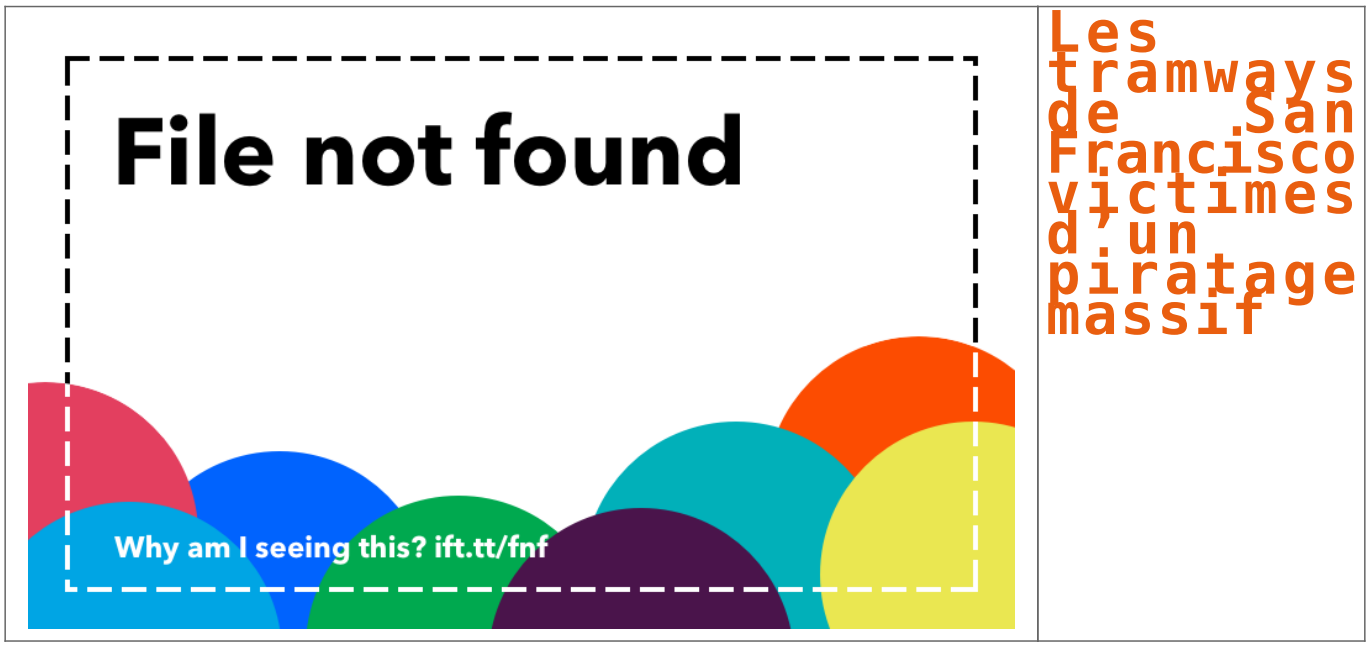
Contactez-nous

Réagissez à cet article

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

---

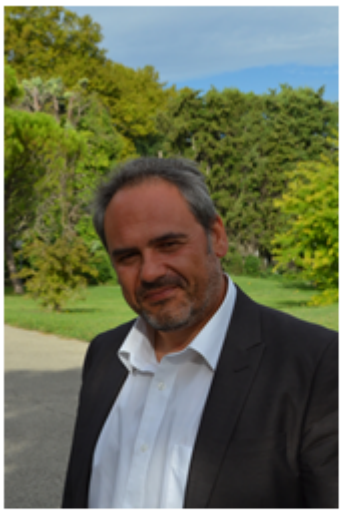
# Les tramways de San Francisco victimes d'un piratage massif




**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.

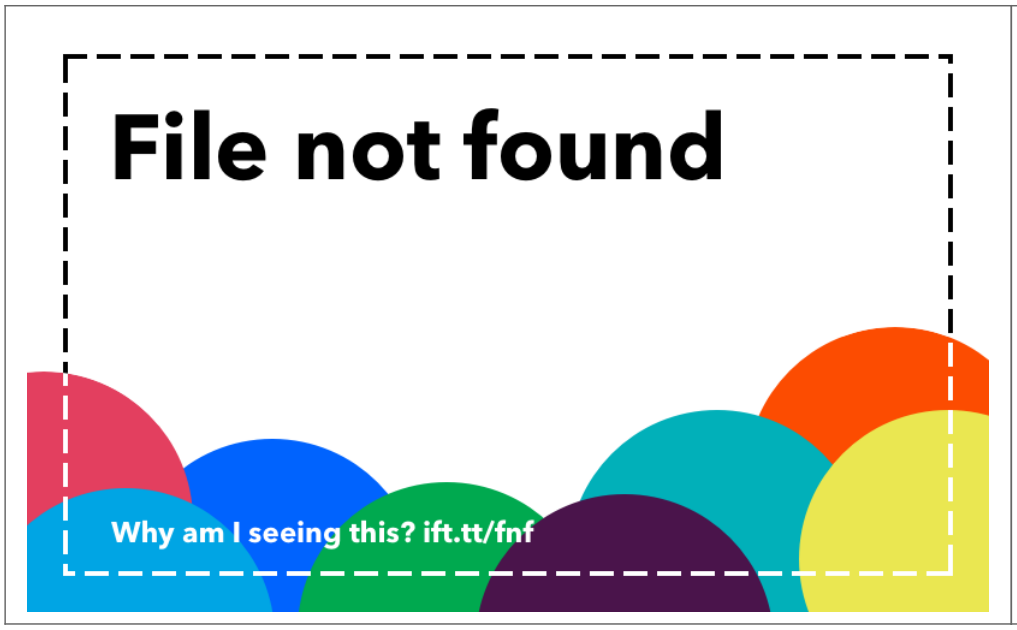
- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation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



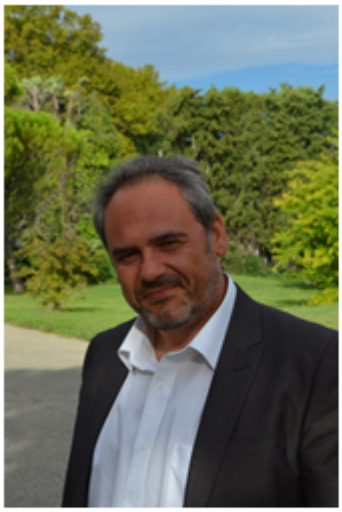

# La Commission européenne mise à terre par une attaque DDoS

**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.

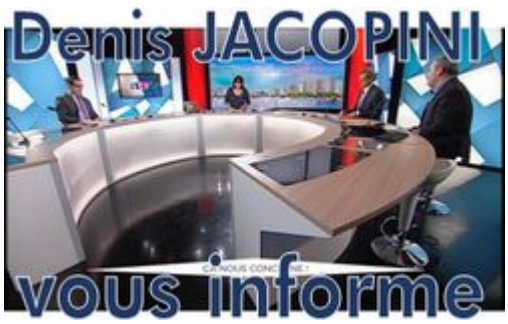
Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

---

# Intervention de la CNIL à l'encontre du site Alainjuppe2017




Intervention de la CNIL à l'encontre du site Alainjuppe2017

---

**La CNIL intervient pour faire corriger une fuite de données concernant le site Internet de l'ancien candidat aux présidentielles françaises, alainjuppe2017.fr.**

L'information est restée confidentielle le temps des primaires de la droite. Il fallait surtout que la faille concernée soit corrigée et la fuite en résultant bouchée. Il y a quelques jours, un internaute anonyme a fait appel au protocole d'alerte de ZATAZ pour faire corriger un bug qui permettait en quelques clics de souris d'accéder à plus de 20.000 profils d'internautes inscrits sur le site alainjuppe2017.fr.
Une porte ouverte présidentielle possible en raison d'un oubli interne. L'un des gestionnaires de l'espace politique avait oublié… de retirer le debug du site ! Bilan, la moindre erreur dans l'espace numérique de soutien à Alain Juppé, via l'espace « Mobilisation », permettait d'accéder à des informations privées et sensibles !…[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 : ZATAZ Protocole d'alerte ZATAZ : intervention de la CNIL à l'encontre du site Alainjuppe2017 – ZATAZ

# Hôtels et chambres d’hôtes, sensibilisez votre personnel contre les hackers

| | |
|---|---|
| | Hôtels et chambres d’hôtes, sensibilisez votre personnel contre les hackers |

**Si vous suivez un tantinet soit peu l'actualité de la sécurité informatique, le groupe de hackers Carbanak doit vous dire quelque chose. En effet, après avoir pendant de longs mois attaqué les banques en recourant à des malwares conçus spécifiquement en ce sens, voilà qu'il s'en prend désormais aux hôtels en utilisant des techniques dites de « social engineering ».**

## Les techniques de social engineering, nouvelles armes de Carbanak ?

L'an passé, les pirates informatiques du groupe Carbanak ont frappé fort en parvenant à dérober près d'un milliard de dollars à différents établissements bancaires.
Eh bien, le gang a changé de cibles mais il est toujours prêt à frapper très fort. Désormais, ce sont les hôtels qui sont dans son collimateur et pour mener ces actions, Carbanak a recours aux techniques de « social engineering ».
Autrement dit, il se fait passer pour des clients d'un hôtel rencontrant des difficultés à réserver sur le système en ligne proposé par l'hôtelier et propose d'envoyer ses informations de réservation par mail laissant alors le piège se refermer sur l'établissement.
En effet, ce mail contient également un malware qui va infecter le système de l'hôtelier. Bien évidemment, en pirates expérimentés, ceux de Carbanak savent ne laisser planer aucun doute quant à leur identité et il est quasiment impossible pour le personnel d'un hôtel de se rendre compte que leur interlocuteur est là pour leur causer du tort.

## Un malware voleur de données et aux effets dévastateurs

Dès lors que le malware a pénétré le système informatique d'un établissement hôtelier, ce dernier télécharge tout un panel de logiciels malveillants qui vont permettre de voler discrètement de nombreuses données.
S'il sera possible de dérober les données d'identité, les coordonnées postales ou les adresses électroniques, ce sont aussi les informations des cartes de crédit qui seront accessibles…[lire la suite]

---

Notre métier : Sensibiliser et former 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

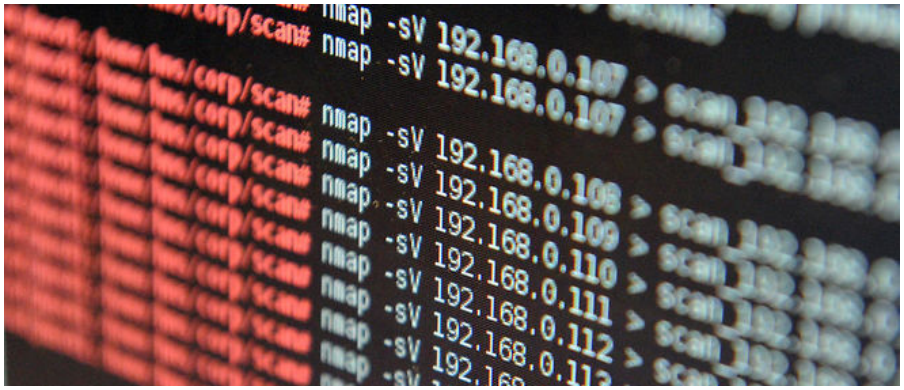
Contactez-nous

Réagissez à cet article

Original de l’article mis en page : Les hôtels, nouvelles cibles des hackers de Carbanak

---

# 14 millions de Français victimes des pirates Informatiques en 2016




14 millions de Français victimes des pirates Informatiques en 2016

---

**La prolifération des cyberattaques a un corollaire : aucune classe d'âge et aucune profession ne sont aujourd'hui épargnées. Explications.**

Dans un rapport publié mercredi 16 novembre, l'éditeur d'antivirus Symantec-Norton pointe l'ampleur que le phénomène « cybercriminel » a prise en 2016. Selon cette étude, 13,7 millions de Français auront été victimes d'attaques informatiques cette année. Le fait d'avoir baigné dans l'univers numérique depuis sa naissance ne change rien à la donne. Les « digital natives » (comme les experts désignent les jeunes qui manipulent des ordinateurs depuis le berceau) sont aussi démunis face à cette menace que leurs aînés.
La génération Y, celle des 18-34 ans, fait ainsi partie des plus touchées par le problème. Il faut dire que cette catégorie de population se comporte sur le Web de manière particulièrement risquée. Or, pour les professionnels de la cybersécurité, la négligence des internautes serait en cause dans la plupart des attaques informatiques dont ils sont victimes.

## Des internautes imprudents

Bien que 77 % des Français sachent qu'ils doivent protéger leurs données en ligne, les utilisateurs gardent de mauvaises habitudes sur le Web. Les réflexes d'élémentaire prudence sont de peu de poids face à l'attrait de certains liens… même d'origine douteuse. Ainsi, 65 % des Français reconnaissent avoir déjà ouvert une pièce jointe postée d'un expéditeur inconnu. Et quasiment un internaute sur cinq partage ses mots de passe avec d'autres utilisateurs. Faut-il, dès lors, s'étonner qu'un Français sur deux se résigne à l'idée qu'il est désormais plus probable qu'une personne accède frauduleusement à ses appareils domestiques connectés qu'à son logement ?
D'après Laurent Heslault, directeur des stratégies numériques chez Symantec, les internautes ont bien conscience des dangers mais « n'ont pas envie de prendre les précautions adéquates pour assurer leur sécurité ». Alors que les cybercriminels, eux, disposent de techniques de plus en plus recherchées pour arriver à leurs fins.
Il ne s'agit pas seulement de paresse chez les internautes. 31 % d'entre eux sont dépassés par la quantité d'informations qu'ils ont à protéger. La plupart considèrent d'ailleurs que la question de la gestion sécurisée des données ne les concerne pas et qu'il appartient aux fournisseurs d'accès à Internet et aux entreprises du secteur des nouvelles technologies de résoudre ces problèmes.

## Un problème mondial

Une étude réalisée en octobre, par le Ponemon Institute pour le compte de l'éditeur de logiciels professionnels Varonis Systems, démontre qu'il ne s'agit pas d'un problème strictement hexagonal. Si 37 % (seulement !) des internautes français indiquent qu'ils prennent toutes les mesures appropriées pour protéger les données auxquelles ils accèdent et qu'ils utilisent, la même réponse est donnée par 50 % chez les collaborateurs allemands, 39 % des employés britanniques et 35 % des employés américains.
Le nombre d'entreprises ayant fait l'expérience des ransomwares l'an dernier est en hausse constante. Ces logiciels rançonneurs, dont le FBI a révélé qu'ils avaient généré, au premier semestre 2016, plus de 209 millions de dollars de butin, ont infecté les serveurs de 12 % des entreprises allemandes, contre 17 % aux États-Unis, 16 % en France et 13 % au Royaume-Uni. Le nombre de cas de perte ou de vol de données au cours des deux dernières années a, lui aussi, explosé… Et l'on ne compte plus les cyberbraquages signalés chaque semaine à travers la planète.
De quoi inciter les États à renforcer leur arsenal pour lutter plus efficacement contre les gangs à l'oeuvre sur la Toile. Les 68 pays signataires de la convention de Budapest, le premier traité international abordant la question de la lutte contre la cybercriminalité adopté en 2001, se sont d'ailleurs réunis les 14 et 15 novembre derniers pour renforcer leur coopération en la matière. Un protocole additionnel à la convention sera adopté courant 2017 pour mettre en place un nouvel outil juridique permettant de collecter des preuves électroniques sur le « cloud », quelle que soit la localisation du serveur qui l'héberge… Preuve, s'il en était besoin, que les gouvernements du monde entier ont pris la mesure de la menace.

## Quels sont les cyberdélits les plus fréquents en France ?

• Le vol de mot de passe (14 %)
• le piratage électronique (11 %)
• le piratage des réseaux sociaux (10 %)
• la fraude à la carte de crédit (9 %)
• le ransomware ne représente que 4 % des actes de cybercriminalité contre les particuliers (mais 12 % des entreprises), soit environ 548 000 cas en 2015. 30 % des victimes de ransomware ont payé la rançon demandée et 41 % d'entre eux n'ont pas pu, malgré tout, récupérer leurs fichiers. [Article Original du Point]

---

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 : Cybersécurité : un Français sur cinq victime de hackers en 2016