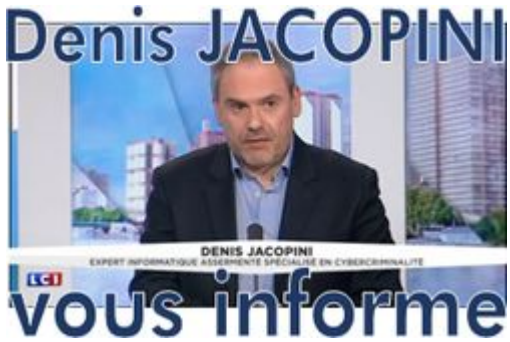
# Yahoo victime de millions de comptes volés




Yahoo victime de millions de comptes volés

**Selon la presse américaine, le portail web pourrait bientôt confirmer le vol de plus de 200 millions de comptes. Un hiatus dans la phase de rachat de Yahoo par Verizon.**

L'année 2012 a bel et bien été une annus horribilis pour les services web. Beaucoup de vols de données ont eu lieu cette année-là. Mais à l'époque, la plupart des services touchés avait relativisé, voire minimisé le nombre de comptes compromis.
Depuis quelques mois, le passé les rattrape et un pirate du nom de « Peace » égrène sur le Dark Web des paquets contenant des données sur des millions de comptes issues de vols de 2012. On pense notamment aux 167 millions de comptes de Linkedin, 360 millions de comptes pour MySpace et 65 millions de Tumblr. Des doutes subsistent sur Dropbox qui a demandé à ses abonnés antérieurs à 2012 de changer leur mot de passe.
Mais au mois d'août dernier, Motherboard avait repéré sur le Dark Web une nouvelle vente de « Peace » concernant 200 millions de comptes Yahoo. Ces données vendus 3 bitcoins (soit environ 1800 dollars) peuvent contenir les noms d'utilisateurs, les mots de passe hachés avec l'algorithme MD5. Mais aussi les dates de naissance et, parfois, une adresse e-mail de secours…[lire la suite]

---



---



Réagissez à cet article

Original de l'article mis en page : Yahoo va-t-il reconnaître le vol de 200 millions de comptes ?

# Les données de santé, la nouvelle cible des cybercriminels

| | |
|---|---|
|  | Les données de santé, la nouvelle cible des cybercriminels |

**Face au développement massif des nouvelles technologies, nos données personnelles sont aujourd'hui entièrement informatisées. De notre dossier médical jusqu'à nos données bancaires en passant par nos loisirs et notre consommation quotidienne, chaque minute de nos vies produit une trace numérique sans même que l'on s'en aperçoit.**

Pendant des années nos données de santé étaient éparpillées entre médecins, laboratoire d'analyses, hôpitaux, dentistes dans des dossiers cartonnés qui s'accumulaient au coin d'un bureau ou sur une étagère. En 2012 la loi « hôpital numérique » avait permis un premier virage en obligeant la numérisation des données de santé par tous les professionnels pour une meilleure transmission inter-service. Depuis un an, la loi « santé 2015 » oblige à une unification et une centralisation des données de santé dans des serveurs hautement sécurisés constituant ainsi le Big Data.

**Une centralisation des données qui n'est pas sans risque**

Appliqué à la santé, le Big Data ouvre des perspectives réjouissantes dans le croisement et l'analyse de données permettant ainsi d'aboutir à de véritables progrès dans le domaine médical. Mais cela n'est pas sans risque.

Le statut strictement confidentiel et extrêmement protégé donne à ces données une très grande valeur. Nos données médicales deviennent ainsi la cible d'une nouvelle cybercriminalité, cotées sur le Dark Web.

Le Dark Web ou Deep Web est l'underground du net tel qu'on le connait. Il est une partie non référencée dans les moteurs de recherche, difficilement accessible où le cybertrafic y est une pratique généralisée. Sur le Dark Web les données personnelles sont cotées et prennent ou non de la valeur selon leur facilité d'accès et leur rendement.

Là où les données bancaires détournées sont de plus en plus difficiles à utiliser suite aux nombreuses sécurisations mise en place par les banques, l'usurpation d'identité et la récolte de données médicales prennent une valeur de plus en plus grande. Selon Vincent TRELY, président-fondateur de l'APSSIS, Association pour la Sécurité des Systèmes d'information, interviewer sur France Inter le 8 septembre 2016, le dossier médical d'une personne aurait une valeur actuelle qui peut varier entre 12 et 18 $.

Si l'on rapporte cette valeur unitaire au nombre de dossiers médicaux abrités par un hôpital parisien, on se rend compte que ceux-ci abritent une potentielle fortune pouvant aller jusqu'à des millions de dollars. Aussi pour protéger ces données, les organismes de santé se tournent vers des sociétés certifiées proposant un stockage dans des Datacenters surveillés, doublement sauvegardés, ventilés avec une maintenance 24h/24. Le stockage a donc un coût qui peut varier entre quelques centaines d'euros jusqu'à des centaines de milliers d'euros pour un grand hôpital. Le coût d'hébergement peut alors devenir un vrai frein pour des petites structures médicales où le personnel présent est rarement qualifié pour veiller à la sécurité numérique des données. Et c'est de cette façon que ces organismes deviennent des cibles potentielles pour les cybercriminels.

Des exemples il en existe à la Pelle. Le laboratoire Labio en 2015 s'est vu subtilisé une partie des résultats d'analyse de ses patients, pour ensuite devenir la victime d'un chantage. Les cybercriminels demandaient une rançon de 20 000 euros en échange de la non divulgation des données. Peu de temps après c'est le service de radiologie du centre Marie Curie à Valence qui s'est vu refuser l'accès à son dossier patients bloquant ainsi toute une journée les rendez-vous médicaux initialement fixés. Peu de temps avant, en janvier 2015, la Compagnie d'Assurance Américaine Anthem a reconnu s'être fait pirater. Toutes ses données clients ont été cryptées en l'échange d'une rançon.

Ces pratiques étant nouvelles, on peut s'attendre à une recrudescence de ce type de criminalité dans l'avenir selon les conclusions en décembre 2014 de la revue MIT Tech Review…[lire la suite]

---

Denis Jacopini anime des **conférences et des formations** et est régulièrement invité à des **tables rondes en France et à l'étranger** pour sensibiliser les décideurs et les utilisateurs aux **CyberRisques** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).

Nous animons **conférences et formations** pour sensibiliser décideurs et utilisateurs **aux risques en informatique**, découvrir et comprendre les **arnaques** et les **piratages informatiques** pour mieux s'en protéger et se **mettre en conformité avec la CNIL** en matière de **Protection des Données Personnelles**. Nos actions peuvent être personnalisées et organisées dans votre établissement.

Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet…) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

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

Contactez-nous

Réagissez à cet article

# Original de l'article mis en page : Les données de santé, le nouvel El-Dorado de la cybercriminalité

# Même le FBI vous recommande très fortement de faire cela sur votre ordinateur !! Suivez leurs conseils !

| | |
|---|---|
|  | Même le FBI vous recommande très fortement de faire cela sur votre ordinateur !! Suivez leurs conseils ! |

**C’est lors d’une conférence organisée à Washington que le directeur du Bureau fédéral d’enquête (FBI), James Comey, a évoqué la question de la cybersécurité.**

C’était le 14 Septembre dernier. Et il a donné un conseil très précieux que nous devrions tous appliquer : « *Si vous allez dans n’importe quel bureau du gouvernement, vous verrez ces petites caméras au-dessus des écrans. Toutes ont un petit cache placé dessus. On fait ça pour éviter que des gens qui n’y sont pas autorisés ne nous regardent.* […] *Je pense que c’est une bonne chose.* »

**Effectivement, même si vous êtes un simple particulier, vous n’êtes pas à l’abri qu’un hacker prenne la main sur votre ordinateur et accède à votre webcam et votre micro.** Etre écouté et observé dans son intimité ? Non merci sans façon ! Alors on vous conseille d’aller vite mettre un petit bout d’adhésif sur votre ordi…Question de précaution !

Beaucoup de gens le font déjà, rappelez vous au mois de Juin, nous vous avions parlé de **cette photo de Mark Zuckerberg où l’on peut voir son ordinateur avec la cam et le micro protégés …**

---

Denis Jacopini anime des **conférences et des formations** et est régulièrement invité à des **tables rondes en France et à l’étranger** pour sensibiliser les décideurs et les utilisateurs aux **CyberRisques** (Autorisation de la Direction du travail de l’Emploi et de la Formation Professionnelle n°93 84 03041 84).
Nous animons **conférences et formations** pour sensibiliser décideurs et utilisateurs **aux risques en informatique**, découvrir et comprendre les **arnaques** et les **piratages informatiques** pour mieux s’en protéger et se **mettre en conformité avec la CNIL** en matière de **Protection des Données Personnelles**. Nos actions peuvent être personnalisées et organisées dans votre établissement.
Plus d’informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

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

Contactez-nous

Réagissez à cet article

Original de l’article mis en page : Le FBI vous recommande très fortement de faire cela sur votre ordinateur !! Suivez

leurs conseils !

---

# 10 point importants avant de faire le pas vers le Cloud hybride

9


10 point importants avant de faire le pas vers le Cloud hybride

---

**Les entreprises semblent adopter pleinement le cloud computing hybride. Mais comment y aller de la bonne façon ? Voici quelques grands points auxquels il faut faire attention dans la conception de ce type de projet.**

## 1. Complexité de l'architecture et ressources adéquates

Un environnement de cloud computing hybride est une architecture informatique extrêmement complexe qui implique différentes combinaisons de cloud computing public et privé et d'informatique sur site. Il faut un personnel informatique aguerri pour structurer et gérer une infrastructure de bout en bout qui doit prendre en charge des transferts de données continus entre toutes ces plates-formes…[lire la suite]

## 2. Coordination des achats de cloud computing et des besoins des utilisateurs finaux

La pire façon de se lancer dans une stratégie de cloud computing hybride est de le faire au petit bonheur la chance. Ces situations se produisent lorsque les départements métiers et le département informatique souscrivent indépendamment à des services de cloud computing…[lire la suite]

## 3. Bien gérer la complexité de la gestion des données

De plus en plus d'entreprises utilisent des systèmes automatiques dans leurs centres de données pour acheminer les données vers différents niveaux de stockage (rapides, moyens ou rarement utilisés), et ce en fonction du type de données et des besoins d'accès aux données…[lire la suite]

## 4. Sécurité et confidentialité des données

La sécurité et la confidentialité des données s'améliorent dans le cloud, mais cela ne change rien au fait que le département informatique d'entreprise a un contrôle direct sur la gouvernance, la sécurité et la confidentialité des données que l'entreprise conserve dans son propre centre de traitements, alors qu'il n'a pas ce contrôle direct dans le cloud computing…[lire la suite]

## 5. Débit et latence, deux points critiques

L'accès au cloud computing peut se faire via un réseau privé sécurisé ou, plus souvent, via Internet. Cela signifie que la gestion du débit et le risque de latence pour les flux de données en temps réel et les transferts de données en masse deviennent plus risqués que lorsqu'ils se produisent au sein du propre réseau interne de l'entreprise…[lire la suite]

## 6. Reprise après sinistre et reprise à chaud

Les entreprises qui transfèrent des données et des applications vers le cloud computing doivent demander à voir les plans de reprise après sinistre et les engagements de reprise après sinistre et reprise à chaud des fournisseurs de cloud computing…[lire la suite]

## 7. Changement de fournisseur

Pourrez-vous facilement changer de fournisseur de cloud computing si tel est votre choix ? Si cette opération peut être facile sur le plan technique, elle pourrait être plus compliquée d'un point de vue contractuel ou de la coopération…[lire la suite]

## 8. Gestion des contrats et des licences sur site

Si vous transférez des applications sur site vers le cloud computing, la coordination sera optimale si vous parvenez à opérer cette transition au moment où vos licences logicielles sur site expirent. La migration vers le cloud n'est généralement pas un problème si vous conservez le même fournisseur, mais elle peut le devenir si vous quittez un fournisseur pour un autre…[lire la suite]

## 9. SLA des fournisseurs

De nombreux fournisseurs de cloud computing ne publient pas de contrats de niveau de service (SLA) et ne les incluent non plus dans leurs contrats. Si vous prévoyez de migrer vers un environnement de cloud computing public ou un environnement de cloud privé hébergé par un fournisseur extérieur, les SLA de base que vous devez exiger de la part de votre fournisseur concernent le temps de disponibilité, le délai moyen de réponse, le délai moyen de résolution des problèmes et le délai de reprise après sinistre…[lire la suite]

## 10. Gestion du risque et responsabilité du fournisseur

Quelle est la responsabilité du fournisseur en cas de sinistre (et de temps d'arrêt) d'un service qui nuit à votre entreprise ? Que se passe-t-il si le fournisseur n'a pas de contrôle sur les circonstances qui ont conduit au problème ? (Cela peut être le cas si le fournisseur de cloud ne possède pas ses propres centres de traitements et les loue à des tiers et que le problème provient d'un de ces centres de traitements.) Qu'en est-il si une brèche de sécurité touche vos données dans le cloud ?…[lire la suite]

---

Denis Jacopini anime des **conférences et des formations** et est régulièrement invité à des **tables rondes en France et à l'étranger** pour sensibiliser les décideurs et les utilisateurs aux **CyberRisques** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Nous animons **conférences et formations** pour sensibiliser décideurs et utilisateurs **aux risques en informatique**, découvrir et comprendre les **arnaques** et les **piratages informatiques** pour mieux s'en protéger et se **mettre en conformité avec la CNIL** en matière de **Protection des Données Personnelles**. Nos actions peuvent être personnalisées et organisées dans votre établissement.
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

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

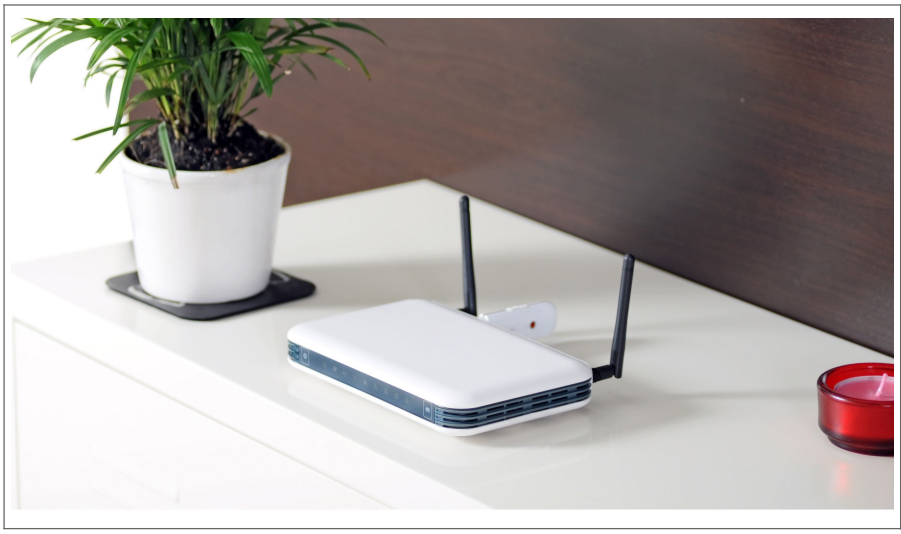
Contactez-nous

Réagissez à cet article

Original de l’article mis en page : Cloud hybride : 10 points de vigilance à bien noter – ZDNet

---

# Professionnels, ne pas fermer votre Wi-Fi pourrait vous coûter cher



Professionnels, ne pas fermer votre Wi-Fi pourrait vous coûter cher

---

**En jugeant que les titulaires de droits d'auteur pouvaient exiger des professionnels qu'ils recueillent l'identité de quiconque utiliserait leur réseau Wi-Fi, la CJUE a prévenu qu'ils pourraient se faire rembourser l'intégralité des frais de justice engagés.**

Jeudi, nous rapportions qu'avec sa décision *Tobias Mc Fadden* prise pour une affaire de piratage de fichiers MP3, la Cour de justice de l'Union européenne (CJUE) a véritablement condamné à mort les réseaux Wi-Fi ouverts, en exigeant que les professionnels qui offrent un tel service recueillent l'identité des internautes qui s'y connectent, et conservent un journal de leurs connexions. Ceux qui ne le font pas s'exposeront à des conséquences financières, alors-même que la Cour estime qu'ils ne sont pas responsables des téléchargements illégaux effectués avec leur connexion.

**Pour comprendre ce paradoxe apparent, il faut revenir sur le raisonnement juridique de la CJUE.**
Tout d'abord, les juges reconnaissent que le professionnel qui met à disposition de ses clients ou prospects un réseau Wi-Fi est assimilable à un « fournisseur d'accès à un réseau de communication », autrement dit à un FAI. En conséquence, ils déduisent que la jurisprudence de la Cour qui interdit d'imposer le filtrage à un FAI s'applique, et que le fournisseur du Wi-Fi ne peut pas être tenu pour responsable de l'utilisation qui est faite par les utilisateurs.
Dès lors, « *il est en toute hypothèse exclu que le titulaire d'un droit d'auteur puisse demander à ce prestataire de services une indemnisation au motif que la connexion à ce réseau a été utilisée par des tiers pour violer ses droits* », juge la Cour…[lire la suite]

---

Denis Jacopini anime des **conférences et des formations** et est régulièrement invité à des **tables rondes en France et à l'étranger** pour sensibiliser les décideurs et les utilisateurs aux **CyberRisques** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Nous animons **conférences et formations** pour sensibiliser décideurs et utilisateurs **aux risques en informatique**, découvrir et comprendre les **arnaques** et les **piratages informatiques** pour mieux s'en protéger et se **mettre en conformité avec la CNIL** en matière de **Protection des Données Personnelles**. Nos actions peuvent être personnalisées et organisées dans votre établissement.
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

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

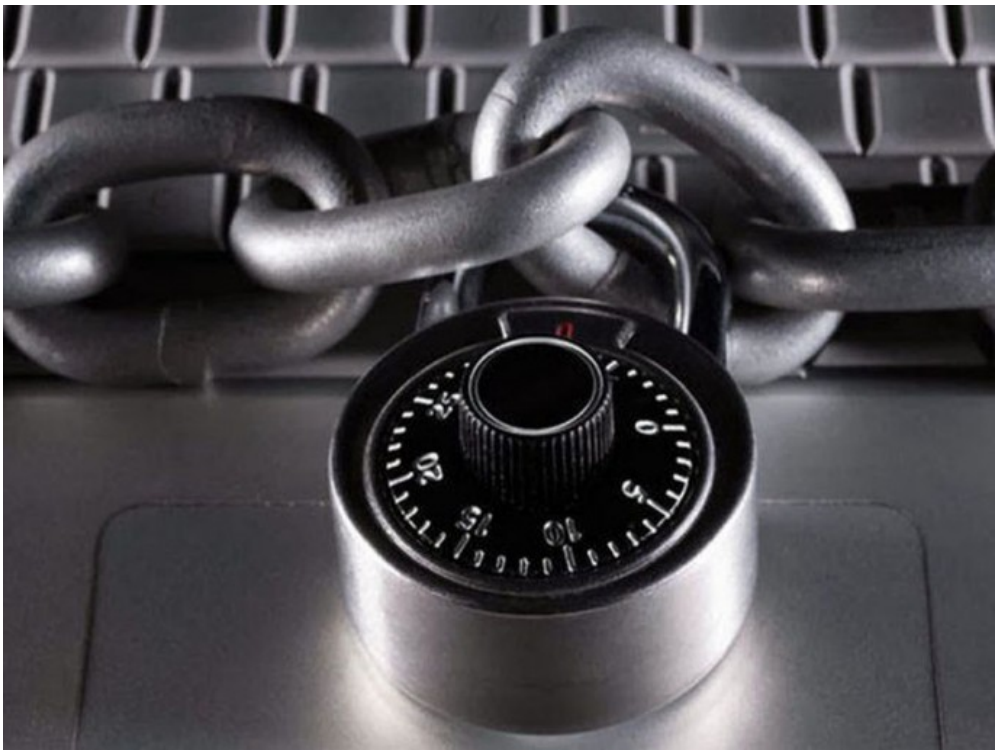
Contactez-nous

Réagissez à cet article

Original de l’article mis en page : Professionnels, ne pas fermer votre Wi-Fi pourrait vous coûter cher – Politique – Numerama

---

# Alerte : Le ransomware Locky passe en mode autopilote



Alerte : Le ransomware Locky passe en mode autopilote

---

**Une nouvelle variante de Locky ajoute un mode autopilote qui proscrit les connexions aux serveurs de commandes et contrôles. Un mode toujours plus discret.**
Il n'y a pas que les voitures autonomes qui se pilotent toutes seules (parfois avec des conséquences dramatiques). Les malwares aussi (avec des conséquences moins dramatiques humainement mais qui peuvent s'avérer aussi ennuyeuses qu'onéreuses). Locky, l'un des ransomwares les plus actif et tristement célèbre, connaît une nouvelle évolution. Il vient de passer en mode d'auto-pilotage. Autrement dit, l'agent malveillant n'a plus besoin de se connecter à un serveur distant de contrôle et commandes (C&C) pour engager le chiffrement des fichiers victimes de son attaque. C'est du moins ce qu'ont découvert les chercheurs en sécurité de l'éditeur Avira.

**Locky en mode furtif**
L'autopilotage permet désormais à Locky d'opérer en mode furtif. « Avec cette étape, [les attaquants] n'ont plus à jouer au chat et à la souris avec la mise en place incessante de nouveaux serveurs avant qu'ils ne soient blacklistés ou fermés », commente Moritz Kroll, spécialiste des logiciels malveillants au Protection Labs d'Avira. Il rappelle en effet que, précédemment, la configuration de Locky comprenait des URL pointant vers des serveurs de C&C ainsi qu'un algorithme de génération de domaines pour créer des liens supplémentaires vers des serveurs de commande et contrôle.
En se libérant de cette dépendance, le mode Autopilote du malware permet à ses auteurs (ou utilisateurs) d'économiser des coûts d'infrastructure et optimiser ainsi la rentabilité de leurs opérations. « Les cybercriminels affinent le mode d'infection 'hors-ligne', ajoute le chercheur d'Avira. En réduisant au minimum les activités en ligne de leur code, ils n'ont pas à payer pour autant de serveurs et de domaines supplémentaires. » Et si ce mode de fonctionnement déconnecté ne leur permet plus de remonter les statistique des infections en cours, il présente l'avantage de se montrer plus discret aux yeux des responsables du réseau. « Auparavant, les administrateurs systèmes pouvaient bloquer les connexions aux serveurs C&C et se prémunir des opérations de chiffrement de Locky. Ces jours sont désormais révolus, prévient Moritz Kroll. Locky a réduit les chances des victimes potentielles d'éviter une catastrophe de chiffrement. »…[lire la suite]

---



---



Réagissez à cet article

Original de l’article mis en page : Ransomware : Locky active le mode pilotage automatique

---

# Alerte : Des bases MySQL menacées par une faille zero-day


---

**Alors que les vulnerabilités zero-day sont de plus en plus fréquentes, voilà que l'une d'elles a été découverte pas n'importe où mais bel et bien dans la célèbre base de données MySQL. Rendue publique il y a quelques heures seulement, cette faille zero-day, si elle est exploitée, peut permettre à un attaquant d'exécuter du code malveillant.**

## Les serveurs MySQL exposés aux menaces

Il y a quelques heures, c'est le chercheur en sécurité Dawid Golunski qui a rendu public une drôle de découverte, à savoir une faille zero-day dans les bases de données MySQL.
Aussi, tous les serveurs MySQL paramétrés en configuration par défaut et les bases de données MariaDB et PerconaDB sont potentiellement exposés à des menaces. Eh oui, l'exploitation de la faille peut permettre assez simplement de modifier le fichier de configuration MySQL et donc d'exécuter une bibliothèque dont le pirate a préalablement pris le contrôle grâce aux privilèges « root ».
Cet exploit peut être exécuté dès lors que l'attaquant dispose d'une connexion authentifiée au service MySQL ou bien par injection SQL. Pourtant, il semblerait que la faille soit connue d'Oracle, qui a en charge le développement et le support de cette base de données, depuis maintenant plus d'un mois et demi.

## Une faille zero-day véritablement dangereuse ?

Comme à chaque fois qu'une faille zero-day est découverte, la première préoccupation est de savoir si la menace qu'elle fait naître est importante ou non. A cette question, les réponses divergent.
Il faut dire que tout le monde ne semble pas d'accord sur la nature même de la faille. Pour certains, il s'agirait d'une vulnérabilité par escalade de privilèges et pas, comme l'a décrit Dawid Golunski, d'une vulnérabilité par exécution de code à distance.
Ainsi, il semble exister des solutions temporaires pour protéger au moins partiellement les bases de données mais tout le monde est unanime pour dire que la livraison de correctifs par Oracle, et ce dans le meilleur délai possible, se fait attendre avec beaucoup d'impatience du côté des administrateurs serveurs…[lire la suite]

---



---

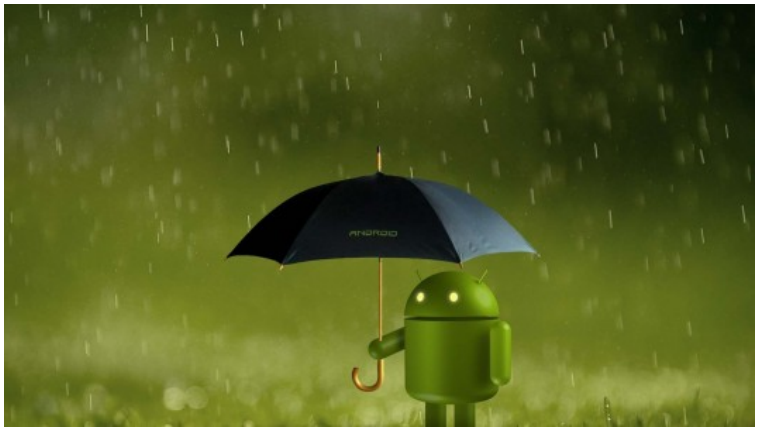


Réagissez à cet article

Original de l’article mis en page : Des bases MySQL menacées par une faille zero-day

---

# 8 failles critiques dans Android corrigées

| | |
|---|---|
|  | 8 failles critiques dans Android corrigées |

---

**Alors que Google s'était déjà illustré au mois de juin en apportant 28 corrections au système d'exploitation mobile Android, la firme de Mountain View a livré il y a quelques heures une nouvelle salve de correctifs. 8 failles critiques ont d'ailleurs été patchées !**

# Encore des corrections en masse pour Android

Souvent décrié en raison du nombre de failles qui affectent son célèbre système d'exploitation mobile, Google a une nouvelle fois livré un nombre (trop) important de patchs correctifs et le problème, c'est que plusieurs vulnérabilités corrigées sont estimées comme « critiques ».

Eh oui, aussi surprenant que cela puisse paraître, la société implantée à Mountain View vient bel et bien d'apporter 57 correctifs dont 8 ont servi à patcher des failles pouvant s'avérer être une vraie menace pour les terminaux.

# Trois sets de correctifs disponibles

Le premier set, disponible depuis le 1er septembre 2016, permet de combler 25 failles Android. Deux d'entre elles étaient critiques. L'une permettait d'exécuter du code distant via une attaque de type « dépassement de mémoire » au niveau du package libutils d'Android. L'autre donnait la possibilité d'exécuter du code distant dans les composants Mediaserver d'Android.

Le deuxième set, mis en ligne le 5 septembre 2016, propose quant à lui de corriger 30 failles exposant largement l'utilisateur. Les plus critiques permettent d'obtenir des privilèges système, d'accéder à un noyau de sous-système réseau, de netfilter ou encore de driver USB…[lire la suite]

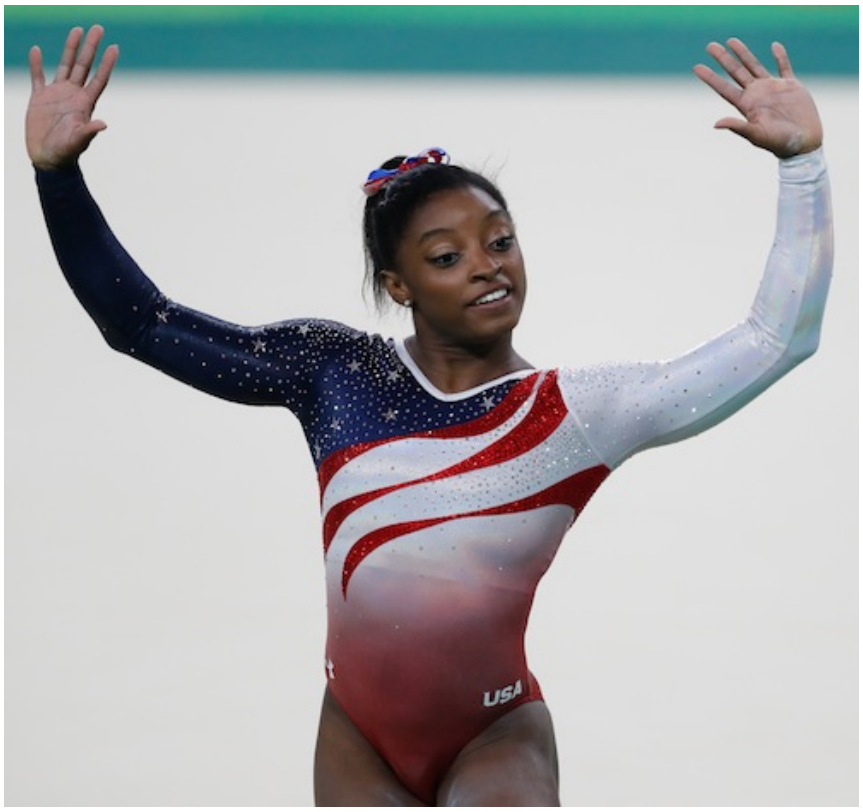
---



Réagissez à cet article

Original de l’article mis en page : Encore 8 failles critiques patchées dans Android

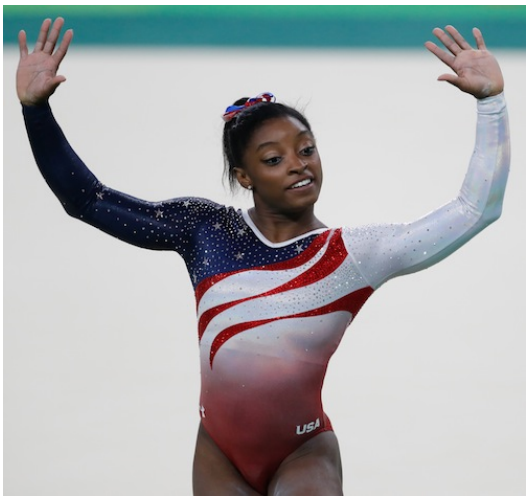
# L’Agence mondiale anti-dopage victime de piratage




L’Agence mondiale anti-dopage victime de piratage

**L'Agence mondiale anti-dopage (AMA ou WADA en anglais) a été victime d'un piratage. Un groupe de hackers a pu subtiliser les dossiers médicaux de quatre athlètes américaines et dévoiler des informations confidentielles. Surprise : les pirates sont russes !**

Les Russes l'auraient-ils mauvaise suite à la disqualification de la quasi-totalité de leurs athlètes lors des Jeux Olympiques de Rio ? Ce vaste « nettoyage » opéré par les fédérations sportives internationales faisait suite au scandale sur le dopage d'Etat généralisé en Russie. Toujours est-il que le groupe russe Tsar Team (APT28), Fancy Bear pour les intimes, a piraté une base de données de l'AMA.
La date exacte de l'attaque n'est pas connue. Les hackers ont vraisemblablement obtenu l'accès aux serveurs de l'Agence en obtenant par phishing des mots de passe ADAMS (pour Anti-Doping Administration and Management System, le SI de l'AMA), via un compte du Comité International Olympique créé à l'occasion des JO de Rio. Ils ont ainsi pu dérober les données relatives à quatre athlètes américaines, notamment leurs dossiers médicaux détaillés.



*Simone Biles, quadruple championne olympique en athlétisme*

Sur les réseaux sociaux, Fancy Bear a divulgué une partie de ces informations, pointant du doigt des « *analyses anormales* » dans les dossiers des joueuses de tennis Venus et Serena Williams, de la basketteuse Elena Delle Donne et de la gymnaste Simone Biles. L'AMA a pris la défense des athlètes mises en cause, expliquant qu'elles bénéficient d'exemptions thérapeutiques. Dans le cas de Simone Biles, par exemple, il s'agit d'un traitement pour trouble du déficit de l'attention, dont il avait déjà été question lors des JO. Mais les hackers promettent bien d'autres révélations.

## « Miner le système anti-dopage mondial ».

Le CIO a condamné cette attaque, « *destinée à salir la réputation d'athlètes propres* ». L'AMA elle aussi condamne, et y voit une tentative de « *miner le système anti-dopage mondial* »…[lire la suite]

---

Denis Jacopini anime des **conférences et des formations** et est régulièrement invité à des **tables rondes en France et à l'étranger** pour sensibiliser les décideurs et les utilisateurs aux **CyberRisques** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Nous animons **conférences et formations** pour sensibiliser décideurs et utilisateurs **aux risques en informatique**, découvrir et comprendre les **arnaques** et les **piratages informatiques** pour mieux s'en protéger et se **mettre en conformité avec la CNIL** en matière de **Protection des Données Personnelles**. Nos actions peuvent être personnalisées et organisées dans votre établissement.
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet…) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

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

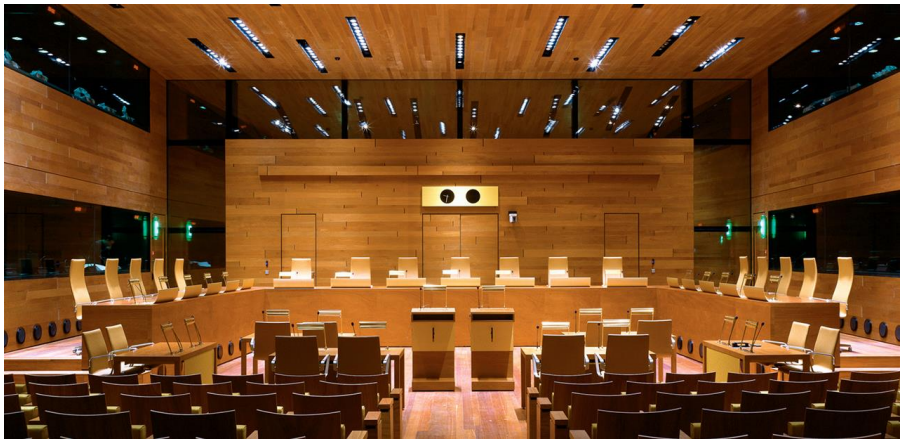
Contactez-nous

Réagissez à cet article

Original de l’article mis en page : Des hackers russes derrière le piratage de l’Agence mondiale anti-dopage

---

# L’exploitant professionnel d’un hotspot Wi-Fi n’est pas responsable des contrefaçons



L’exploitant professionnel d’un hotspot Wi-Fi n’est pas responsable des contrefaçons

---

**Cour de justice de l'Union européenne a jugé aujourd'hui qu'un fournisseur de hotspot n'était pas responsable des contrefaçons réalisées par ses utilisateurs. Cependant, cet acteur pouvait se voir enjoindre d'exiger un mot de passe par une juridiction ou une autorité administrative nationale.**

Le litige est né en 2010 : Sony Music avait adressé une mise en demeure à Thomas Mc Fadden. Cet exploitant d'une entreprise de sonorisation outre-Rhin avait laissé son réseau Wi-Fi ouvert sans mot de passe. Or, un tiers a pu mettre à disposition une œuvre du catalogue de la major. L'affaire était remontée jusqu'à la CJUE où les juridictions allemandes ont déversé une série de questions préjudicielles.

## FAI ou exploitant de hotspot Wi-Fi, même combat

Dans son arrêt (PDF) du jour, la Cour va d'abord considérer que la fourniture d'un tel accès Wi-Fi relève de la fourniture d'un service de la société de l'information, à l'instar donc des prestations d'un FAI (article 12 de la directive de 2000). Cela implique cependant que l'exploitant du hotspot ait un rôle « *purement technique, automatique et passif* » et qu'il n'a ni la connaissance ni le contrôle des informations transmises.

Ceci vérifié, la Cour rappelle qu'un tel prestataire n'est alors pas responsable des contenus qui passent dans ses tuyaux à la triple condition :

1. de ne pas être à l'origine d'une telle transmission,
2. de ne pas sélectionner le destinataire de cette transmission et
3. de ne ni sélectionner ni modifier les informations faisant l'objet de ladite transmission.

Si ces conditions sont remplies, alors un titulaire de droit ne peut demander la moindre indemnisation à cet intermédiaire ou le remboursement de ses frais…[lire la suite]

Qu'en est-il des professionnels de l'hôtellerie qui mettent à disposition de leurs clients du Wifi ? Réagissez

---

Denis Jacopini anime des **conférences et des formations** et est régulièrement invité à des **tables rondes en France et à l'étranger** pour sensibiliser les décideurs et les utilisateurs aux **CyberRisques** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).

Nous animons **conférences et formations** pour sensibiliser décideurs et utilisateurs **aux risques en informatique**, découvrir et comprendre les **arnaques** et les **piratages informatiques** pour mieux s'en protéger et se **mettre en conformité avec la CNIL** en matière de **Protection des Données Personnelles**. Nos actions peuvent être personnalisées et organisées dans votre établissement.

Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

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

Contactez-nous

Réagissez à cet article

Original de l’article mis en page : CJUE : l’exploitant professionnel d’un hotspot Wi-Fi n’est pas responsable des contrefaçons