La France se prépare à une cyberattaque de grande envergure

La France se prépare à une cyberattaque de grande envergure

En France, l'Agence nationale de la sécurité des systèmes d'information (ANSSI), qui surveille les réseaux informatiques gouvernementaux ou ceux des entreprises les plus sensibles, comme EDF ou la SNCF, révèle avoir détecté ces derniers mois, des intrusions dans les ordinateurs de certaines sociétés, mais de manière étrange, aucune donnée n'ayant été volée.

Ce qui laisse craindre des préparatifs en vue de tentatives de sabotages ou d'attaques terroristes. En France, la lutte contre la piraterie informatique est désormais inscrite dans la Loi de programmation militaire (LPM) 2014-2019. Les différents secteurs d'importance vitale ont pour obligation légale de se protéger.

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 : La France se prépare à une cyberattaque de grande envergure – RFI

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

La détection des cyberattaques des OIV passe sous le contrôle de l´Etat

La détection des attaques des OIV sous le contrôle de lEtat

Pour superviser leur sécurité, les Opérateurs d'importance vitale (OIV) devront avoir recours à des prestataires certifiés PDIS. Une habilitation que l'Anssi est en train de tester avec une poignée de sociétés.

L'Anssi (Agence nationale pour la sécurité des systèmes d'information) serre peu à peu la vis aux OIV (Opérateurs d'importance vitale), environ 250 organisations dont le bon fonctionnement est jugé essentiel au fonctionnement de la Nation. Après les premiers arrêtés sectoriels (sortis en juin et en août) encadrant la sécurité informatique de ces entités, l'agence s'attaque à un élément clef de son dispositif découlant de l'article 22 de la Loi de programmation militaire (LPM), votée fin 2013 : la notification d'incidents.
Rappelons que, pour les systèmes d'information dits d'importance vitale – que chaque entreprise doit définir par elle-même -, « les opérateurs (d'importance vitale, NDLR) communiquent les informations dont ils disposent dès qu'ils ont connaissance d'un incident et les complètent au fur et à mesure de leur analyse de l'incident », précise un décret paru en mars 2015. Et, pour ce faire, ils devront faire appel à des prestataires certifiés, les PDIS (Prestataires de détection d'incidents de sécurité). « Au sein des OIV, trois niveaux de sécurité sont définis. Le plus élevé – C3 – devra être protégé par une société habilitée », précise Denis Attal, directeur technique de Thales Critical Information Systems (CIC), une des sociétés engagées dans cette certification…[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 : OIV : la détection des attaques passe sous le contrôle de lEtat

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

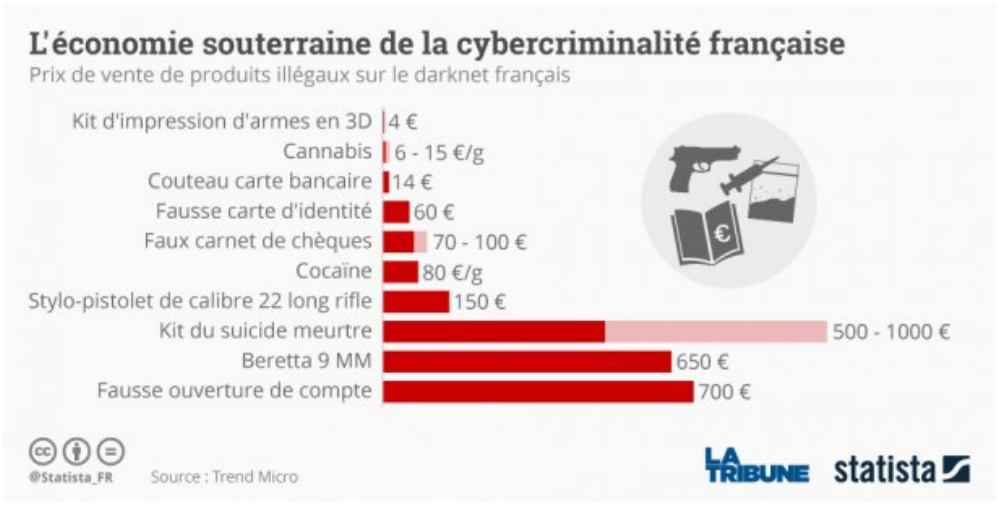
Contactez-nous

Réagissez à cet article

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

---

Qui sont les escrocs du darknet français ?



Qui sont les escrocs du darknet français ?

Pour la première fois, une étude, réalisée par la société de cybersécurité Trend Micro, s'est penchée sur l'organisation de la sphère cybercriminelle française. D'après ses estimations, 40.000 escrocs réalisent un chiffre d'affaires compris entre 5 et 10 millions d'euros par mois.

À quoi ressemble l'économie souterraine de la cybercriminalité française ? Combien de hackers malveillants y prospèrent ? Comment s'organisent-ils, que vendent-ils et combien gagnent-ils ? Pour la première fois en France, une étude, réalisée par l'entreprise de cybersécurité Trend Micro et publiée ce mercredi, donne des réponses. Pendant un an, ses équipes de R et D ont scruté les marchés souterrains nationaux et compris ses spécificités.
Le panorama dressé, plutôt inquiétant, révèle les dessous du « web underground » français. Un écosystème criminel qui prospère dans le *darknet* (l'internet caché), mais qui apparaît très bien organisé, en pleine professionnalisation et… en pleine croissance.

40.000 cybercriminels dans une centaine de places de marché

Selon les estimations de l'auteur de l'étude, qui souhaite rester anonyme, le cybercrime français se compose de 40.000 individus. Un chiffre « relativement faible » par rapport aux marchés plus importants comme la Russie ou les États unis, mais comparable à celui de l'Allemagne. Ce chiffre a été obtenu en compilant et en pondérant le nombre de membres de la centaine de « marketplaces » du *darknet*, c'est-à-dire les forums de discussions qui sont indispensables aux hackers pour organiser leurs fraudes.
Quel est le profil de ces cybercriminels ? Bien évidemment, tout le monde utilise un ou plusieurs pseudo, des plus loufoques aux plus lyriques. Mais les connaisseurs de ce milieu estiment qu'il s'agit surtout d'hommes jeunes, entre 20 et 30 ans. Au regard de leurs compétences techniques, certains sont « *certainement des développeurs professionnels*« . On assiste aussi au retour en force des anciens « spammers nigérians », les escrocs qui envoyaient des courriels pour demander de l'aide dans les années 1990 et 2000, et qui se reconvertissent désormais dans les virus informatiques.
Relatif soulagement : la plupart des 40.000 cybercriminels français ne vivent pas exclusivement de cette activité. Seule une petite centaine d'entre eux seraient « de vrais pros ». Les autres sont plutôt à la recherche d'un complément de revenus. Mais cela n'empêche pas cet écosystème de prospérer. D'après les données de la Gendarmerie nationale et de la Police nationale, la cybercriminalité française générerait entre 5 et 10 millions d'euros de chiffre d'affaires tous les mois.

Armes, drogues, données bancaires

Les places de marché, qui attirent au moins plusieurs milliers, voire une dizaine de milliers d'utilisateurs chacune (la plupart du temps, les hackers sont membres de plusieurs forums) sont très bien structurées, avec des sous-sections clairement identifiées en fonction des « besoins » : armes, logiciels malveillants, drogues…
Comment s'organise ce commerce ? « *Généralement, il existe trois canaux de vente de biens et de services illégaux au sein de l'underground français* », décrypte l'étude. Certains fraudeurs font la promotion de leurs produits directement sur les places de marchés. D'autres, plus paranoïaques, guettent les messages et contactent eux-mêmes leurs clients. Enfin, il existe aussi des « autoshops », c'est-à-dire de véritables boutiques gérées par les vendeurs eux-mêmes, dont beaucoup sont accessibles depuis les forums. C'est même la grande spécialité française.
Les vendeurs proposent un catalogue impressionnant de produits illégaux, à des prix très compétitifs. On y trouve des armes discrètes (poings américains, couteaux de petits formats, stylo-pistolets de calibre 22 long rifle), vendues entre 10 et 150 euros. Mais aussi des armes lourdes, vendues entre 650 et 1.800 euros, ainsi que des kits d'impression d'armes en 3D, que l'on peut acquérir pour une poignée d'euros.
Au rayon des stupéfiants, le cannabis se vend entre 6 et 15 euros le gramme, mais on trouve aussi de la cocaïne, de l'héroïne, de la MDMA, du LSD et autres champignons. »*Les dealers ne vendent qu'en France pour ne pas se faire détecter lors des transactions transfrontalières* », note l'étude. Les autoshops proposent également des fichiers comportant des bases de données personnelles (comme des numéros de carte bancaire) pour environ 400 euros…[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 : Cybercriminalité : qui sont les escrocs du darknet français ?

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

---

Peut-on être condamné pour avoir visité des sites djihadistes ?

Peut-on être condamné pour avoir visité des sites djihadistes ?

Un jeune homme de 28 ans, qui était surveillé par les services de renseignement pour des velléités de départ vers la Syrie, a été condamné à deux ans de prison par le tribunal correctionnel de Marseille, pour avoir régulièrement visité des sites djihadistes à la bibliothèque municipale.

Jeudi, le tribunal correctionnel de Marseille a condamné un Marseillais de 28 ans à deux ans de prison, parce qu'il avait consulté à de nombreuses reprises des sites de propagande terroriste, et notamment regardé des scènes d'exécutions.
La justice a fait une pleine application des nouvelles dispositions du code pénal introduites par la loi Urvoas du 3 juin 2016, qui punissent d'un maximum de deux ans de prison « *le fait de consulter habituellement un service de communication au public en ligne mettant à disposition des messages, images ou représentations soit provoquant directement à la commission d'actes de terrorisme, soit faisant l'apologie de ces actes lorsque, à cette fin, ce service comporte des images ou représentations montrant la commission de tels actes consistant en des atteintes volontaires à la vie* ».
Seule la démonstration de la bonne foi de l'internaute pouvait l'exonérer d'une condamnation. Mais en l'espèce, et même s'il a tenté de plaider qu'il faisait un travail d' « apprenti journaliste » avec un « programme de recherches », les éléments contextuels rapportés par l'AFP permettaient difficilement de croire à une simple volonté de s'informer :
De janvier à août, il s'était connecté à 143 reprises pour visionner écrits et vidéo faisant l'apologie du terrorisme. Il a été interpellé le 9 août alors qu'il faisait des recherches sur le moyen de gagner la Libye via l'Espagne. Jugé en comparution immédiate, il avait été placé en détention dans l'attente de son procès. Hospitalisé en 2012 en psychiatrie à Avignon où il dit s'être converti à l'islam, le jeune homme était surveillé par les services du renseignement depuis l'été 2015, date à laquelle son père avait alerté les autorités sur les velléités de départ en Syrie de son fils.
Ce signalement avait provoqué une interdiction administrative de quitter le territoire pour six mois. Son téléphone portable contenait plus de 100 vidéos dont l'une de 21 minutes montrant la décapitation de quatre hommes.
Ce n'est pas la première condamnation du genre depuis que le législateur a fait de la seule consultation des sites terroristes une infraction pénale en elle-même (auparavant, il fallait que d'autres éléments matériels viennent en soutien). Mais cette affaire est intéressante à un autre titre…[lire la suite]

Réagissez à cet article

Original de l’article mis en page : Un homme condamné pour avoir visité des sites djihadistes à la bibliothèque – Politique – Numerama

---

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