Signes indiquant qu’un compte a été piraté et procédure à suivre

Signes indiquant qu’un compte Yahoo a été piraté et procédure à suivre

Nous espérons que vous n'aurez jamais à craindre qu'une autre personne accède à votre compte sans votre autorisation, mais vous ne pouvez jamais être sûr à 100 % de la sécurité de votre compte. Voici comment déterminer si une autre personne s'est connectée à votre compte Yahoo et les étapes à suivre pour récupérer l'accès à celui-ci.

Quelle que soit la situation, si vous pensez qu'une autre personne a accédé à votre compte sans votre autorisation, **changez votre mot de passe immédiatement**. Si vous n'avez pas accès à votre compte, utilisez l'aide relative aux mots de passe pour le récupérer.

Signes indiquant que votre compte a été piraté

• Vos informations de compte ont été modifiées à votre insu.
• Des connexions ont été établies depuis des endroits que vous ne reconnaissez pas sur la page de vos activités de connexion.
• Vous ne recevez pas des e-mails que vous attendiez.
• Votre compte Yahoo Mail envoie des spams

Ce que vous devez faire

Bloquer l'envoi de spam depuis votre compte

Recevoir des spams est une chose. Recevoir des rapports de spam provenant de votre compte en est une autre. Si votre compte a été piraté de sorte qu'il envoie des spams, vous pouvez résoudre ce problème ! Le moyen le plus rapide de bloquer l'envoi de spams depuis votre compte consiste à sécuriser votre compte en créant un nouveau mot de passe fiable ou activer la clé de compte.

Signaler un mail falsifié (usurpé)

Les messages falsifiés sont des mails qui semblent avoir été envoyés depuis votre adresse mail, mais qui en réalité ont été envoyés depuis un compte de messagerie complètement différent. Si votre Yahoo Mail est sécurisé, mais que vos contacts reçoivent toujours des spams qui semblent provenir de votre adresse, il s'agit probablement d'un mail falsifié ou « usurpé ».

1. Affichez l'en-tête complet du mail en question.
2. Dans la dernière ligne Reçu de l'en-tête complet, notez l'adresse IP d'où provient le mail.
– Cela correspond au fournisseur d'accès Internet (FAI) de l'expéditeur.
3. Effectuez une recherche par adresse IP sur un site tel que WhoIs.net pour déterminer le fournisseur d'accès Internet de l'expéditeur.
4. Contactez le fournisseur d'accès Internet de l'expéditeur pour demander que l'action appropriée soit entreprise.

Les fournisseurs de messagerie ne peuvent pas empêcher ces contrefaçons, mais si la fraude est identifiée, il est possible d'entreprendre une action.

Examinez les paramètres Yahoo Mail

• Supprimez les contacts mail inconnus.
• Supprimez les comptes Mail liés que vous ne reconnaissez ou ne contrôlez pas.
• Changer votre mot de passe sur les comptes liés que vous contrôlez.
• Vérifiez que votre réponse automatique de congés est désactivée.
• Découvrez si une autre personne a accédé à votre compte.

Autres paramètres de compte Yahoo Mail habituellement modifiés :

• Signature
• Nom d'expéditeur
• Adresse de réponse
• Transfert de mails
• Filtres
• Adresses interdites

Restaurer les mails, messages instantanés et contacts manquants

Si des mails, des messages instantanés ou des contacts sont manquants, vous pouvez restaurer les mails ou messages instantanés perdus ou supprimés. Vous pouvez également récupérer les contacts perdus.

Empêchez d'autres personnes d'accéder à nouveau à votre compte, même après avoir modifié votre mot de passe. Assurez-vous que votre compte reste protégé.

Recherchez la présence de logiciel malveillant sur votre ordinateur

Les logiciels malveillants peuvent corrompre votre système et collecter des informations sensibles, telles que des mots de passe et des coordonnées bancaires. Plusieurs programmes anti-logiciel malveillant sont disponibles sur Internet et permettent de détecter et de supprimer les logiciels malveillants sur les Mac et PC.

Réagissez à cet article

Original de l'article mis en page : Signes indiquant qu'un compte a été piraté et procédure à suivre | Yahoo Aide – SLN2090

Toutes les 4 secondes, un nouveau malware téléchargé

Toutes les 4 secondes, un nouveau malware est téléchargé

Selon Check Point, les téléchargements de logiciels malveillants inconnus ont été multipliés par 9 dans les entreprises. La faute aux employés ?

Dans leur rapport de sécurité 2016, les chercheurs de Check Point ont analysé plus de 31 000 incidents cyber touchant plusieurs milliers d'entreprises dans le monde. Résultat des courses : les téléchargements de logiciels malveillants explosent dans les entreprises.
L'an dernier, les téléchargements de malwares encore « inconnus » des systèmes de sécurité d'organisations ont été multipliés par 9, passant de 106 à plus de 970 téléchargements par heure, selon Check Point. En moyenne, un nouveau programme malveillant inconnu est téléchargé toutes les quatre secondes. Et les employés sont présentés comme le maillon faible dans ce domaine.

Maillon faible

Les malwares « connus » font également des dégâts (un téléchargement toutes les 81 secondes en moyenne) lorsque les systèmes sont irrégulièrement mis à jour et que les correctifs de sécurité font défaut. Une variante d'un programme malveillant peut aussi confondre un antivirus, au risque d'exposer les systèmes et réseaux d'une entreprise à l'espionnage et au vol de données…[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 : Un nouveau malware téléchargé toutes les 4 secondes

Comment Facebook manipule le contenu qu’il nous affiche ?

Comment Facebook manipule le contenu qu’il nous affiche ?

Censure d'une photo historique, choix d'articles qui renforcent les partis pris: les centaines de millions d'internautes qui s'informent via leurs «amis» sur Facebook, plutôt que par les médias classiques, courent le risque d'une information biaisée, selon des experts.

Dernier exemple en date, la censure par Facebook la semaine dernière de la célèbre photo d'une petite Vietnamienne nue brûlée au napalm, au nom de sa politique contre la nudité des enfants. Critiqué dans le monde entier, le groupe américain a rétabli la photo et promis de tenir compte à l'avenir du «statut d'icône» des clichés historiques.
Cette polémique a révélé l'importance prise par Facebook comme source d'information pour une majorité d'internautes dans le monde.
Un sondage international du Reuters Institute montre que 51% des personnes interrogées dans 26 pays s'informent par les réseaux sociaux, dont 44% par Facebook, et que 12% en ont fait leur première source d'information. En France, un Français sur deux consulte Facebook, surtout sur mobile, et peut y passer plusieurs heures par semaine.
Aucun des 1,7 milliard d'utilisateurs ne voit les mêmes informations dans son «newsfeed» (fil d'actualités), qui compile les messages de ses «amis»: un mélange de commentaires personnels et d'articles partagés, provenant aussi bien de grands médias que de blogues inconnus.
Entre les milliers de messages produits par ses amis, impossible de tout lire: c'est l'algorithme de Facebook qui, pour chacun, classe ceux placés en haut de page. Et donc ceux qui seront vus, car en moyenne l'utilisateur ne lit que 200 des 2000 messages de son fil.
Les utilisateurs ignorent le plus souvent l'existence et les critères de ce tri, qui ont changé sans cesse en 10 ans d'existence. En juin, Facebook a brusquement décidé de privilégier les messages personnels au détriment des partages d'articles, diminuant la place des médias classiques…[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 : Comment Facebook filtre notre connaissance du monde | Laurence BENHAMOU | Internet

---

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 ?

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

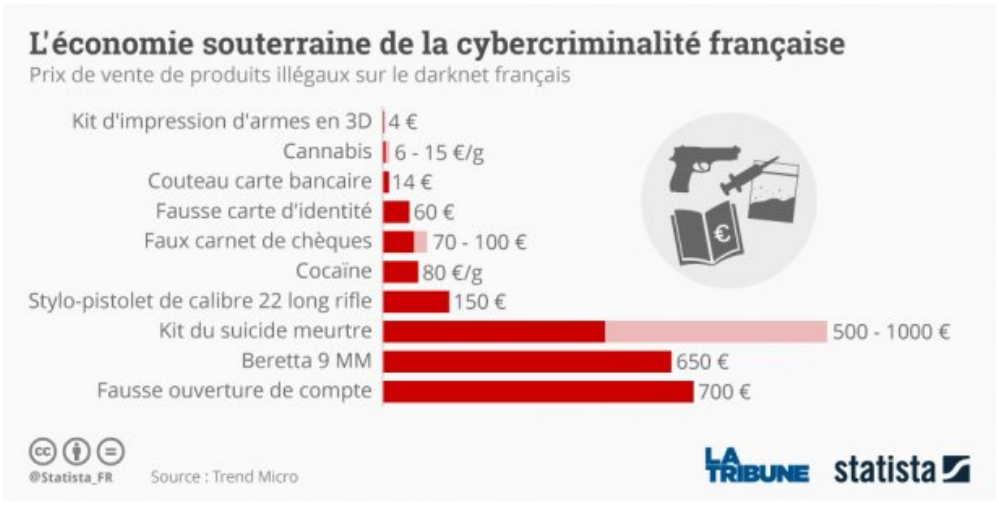
Contactez-nous

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 ?