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]

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

---

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

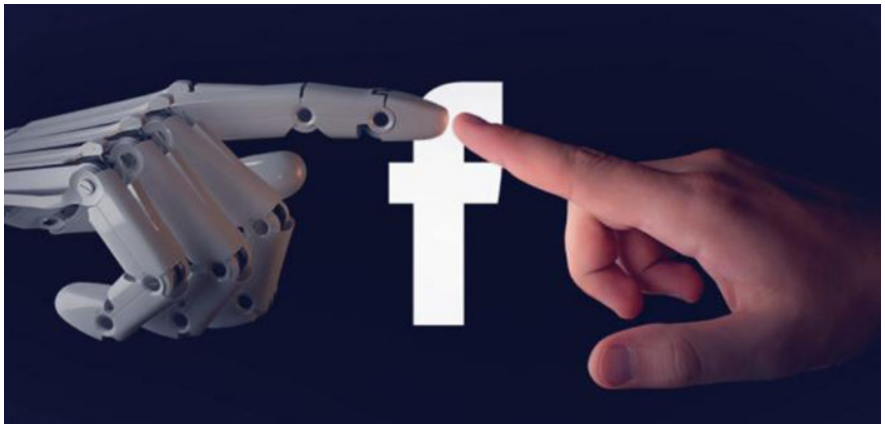
Contactez-nous

Réagissez à cet article

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

---

L’intelligence artificielle (IA) de Facebook sur le point d’être dévoilée

	L’intelligence artificielle (IA) de Facebook sur le point d’être dévoilée

---

Nous le répétons souvent au sein de nos articles, Facebook Inc. n'est plus seulement la première plateforme sociale au monde, c'est avant tout une société créant des technologies. Des technologies dont Facebook est l'édifice principale qui rend le groupe si rentable. Mais Mark Zuckerberg voit beaucoup plus loin et il a pour habitude de dévoiler ses futurs défis. Celui de cette année concerne l'élaboration d'une intelligence artificielle, rien que ça…

En janvier, Mark Zuckerberg présentait, dans une de ses publications Facebook, son nouveau challenge : « construire une intelligence artificielle comme Jarvis pour Iron Man ». Dans ces paroles, qui sont les siennes et au-delà de la référence au Comics, c'est la vision de Facebook qui s'éclaire.

Depuis le début de l'année, l'intelligence artificielle semble présentable pour Facebook. Dans un de ses récents Facebook Live à Rome, Zuckerberg a évoqué le sujet en annonçant une présentation dès septembre soit demain…

Mais à quoi consisterait cette intelligence artificielle ?
Celle-ci servirait comme un assistant pour une maison : paramétrer le réveil selon son agenda, préparer les toasts au petit-déjeuner selon une présence humaine ou non, ouvrir la porte d'entrée à des individus pré-sélectionnés par la reconnaissance faciale, augmenter la température intérieure selon la météo et une présence et on imagine bien d'autres choses. Vous me direz qu'au niveau de la domotique, il y a déjà eu de belles avancées et que programmer une cafetière ou un toast n'est pas compliqué… Mais là où Facebook veut progresser, c'est l'élaboration d'une perception artificielle capable d'entendre, de voir et d'interpréter un langage. Nous avons hâte d'avoir plus d'informations officielles de la part de la firme dès la rentrée !…[lire la suite]

Réagissez à cet article

Original de l’article mis en page : L’intelligence artificielle de Facebook prête à être dévoilée

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

---

Comment préparer les enfants aux Réseaux Sociaux ?

Comment préparer les enfants aux Réseaux Sociaux ?

Dangers de l'Internet au-delà de logiciels malveillants, ou l'enlèvement des données par des ransomware. Sur le Net, le respect de la vie privée est mis à mal par les réseaux sociaux, les moteurs de recherche et la publicité. Dans le cas des mineurs, il y a des risques plus inquiétants, dont ils ne sont pas pleinement conscients, mais leurs parents, les enseignants et la société doivent assurer leur sécurité. Une étude récente, appelé Kids Connected, et menée par la firme de sécurité Kaspersky Lab avec iconKids et jeunesse, révèle des faits troublants sur la façon dont les enfants se comportent en ligne. Comportements qui peuvent conduire à provoquer plus de crainte.

Ce rapport montre que **les enfants âgés de 8 à 16 ans sont accros aux réseaux sociaux**. En outre, l'activité peut les mettre en danger, eux et leurs **familles**. 35% des enfants disent qu'ils ne veulent pas être sans réseaux sociaux, et sont désireux de rejoindre des groupes en leur sein, ils sont en mesure de partager beaucoup d'informations personnelles. **Le problème** est qu'ils le font sans avoir conscience que les données qu'ils partagent sont vues par de nombreux utilisateurs et peuvent être utilisées par des personnes potentiellement dangereuses.

Trop d'informations personnelles

Mais **qu'est-ce que les mineurs partagent le plus** ? La plupart des enfants, 66%, **montrent l'école** où ils étudient, 54% **des lieux qu'ils visitent**, et 22% partagent même **la gestion de leurs maisons**. Mais, 33% des enfants donnent également des **informations sur les effets de leur famille et de leurs parents**, sur leur travail (36%) ou sur **ce que leurs parents facturent** (23% des enfants).
Mais, outre le partage des données réelles, **les mineurs sont également prêts à mentir sur le réseau**, et ils le font surtout **si ça peut leur ouvrir des portes**. Un tiers des enfants est prêt à mentir au sujet de l'âge. 17% des enfants font semblant d'être plus âgés, et de modifient leur âge en fonction du web ou le service qu'ils veulent utiliser, étant donné que beaucoup d'entre eux ont des restrictions (très facile à sauter) d'âge.
Avec ces données, **les cybercriminels disposent d'informations suffisantes pour être utilisés à des fins malveillantes**. Parmi les activités criminelles qu'ils pourraient commettre, ils trouvent l'emplacement physique des mineurs. **Tous les enfants doivent apprendre à un âge précoce ce qu'ils devraient partager en ligne**, ou non. Et connaître les paramètres des réseaux sociaux de la vie privée, de sorte que seuls leurs amis peuvent voir leurs publications et leurs données.

Comprendre quelles sont vos données et la façon de les protéger

Tous les enfants et leurs parents doivent comprendre ce que sont les données personnelles, et **la façon dont on peut les protéger**. "Ceci est comparable aujourd'hui à lire et à écrire», dit Janice Richardson, consultant senior chez European Schoolnet, qui explique que **«les enfants ont besoin d'apprendre à un âge précoce que la vie privée est votre bien le plus précieux, et un droit fondamental ».**
Comme des **conseils de base** qui sont donnés par Kaspersky Lab afin d'éviter autant que possible les risques:
• Une bonne **communication est essentielle**. Il faut parler aux enfants au sujet de leurs expériences et préoccupations.
• **Réalisez les premières étapes dans les réseaux sociaux avec eux** pour créer le profil, activez les options de confidentialité, publiez votre premier poste …
• Les réseaux sociaux ont des **restrictions d'âge**. La plupart sont fixée à 13 ans. À cet âge, il est commode d'en profiter pour leur parler et leur expliquer leurs droits, les responsabilités et les préparer à l'entrée dans le monde numérique.
• Cela peut **devenir un jeu**, quelque chose que vous faites en famille: par exemple, l'impression de leur profil, accroché au mur, leurs postes … Ils pourront visualiser le public à qui est destiné chaque contenu.
• **Établir des règles** pour leur utilisation.
• **Encourager les enfants à communiquer avec vous**, ils vous apprendront de nouvelles applications récemment installées, les services qu'ils utilisent … Si cela devient une habitude depuis le début, il sera plus facile de partager des informations et de leur **parler de la vie privée et de sécurité**.

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 situation préoccupante des enfants dans le réseau: mentir pour accéder aux réseaux sociaux et y donner trop d’informations

---

Trend Micro ausculte la cybercriminalité underground en France

	A quoi ressemble de DarkNet ?

L'éditeur de sécurité a dressé un état des lieux de l'underground de la cybercriminalité en France. Méfiance, bitcoins et forte orientation vers les falsifications des documents sont les maîtres mots.
Un chercheur de Trend Micro s'est livré à un exercice délicat : plonger dans l'univers de la cybercriminalité souterraine en France. Connu sous le vocable « underground », cette partie du web accueille des places de marchés, des forums où s'achètent contre monnaie virtuelle des armes, de la drogue, des faux documents, mais aussi des malwares.
Dans son étude, l'éditeur japonais précise que le tréfonds du web français reste relativement modeste par rapport à d'autres pays comme la Chine ou la Russie. Néanmoins, il recense 40 000 cybercriminels sur l'underground hexagonal ayant des compétences hétérogènes (expert à novice). Ce foyer génère entre 5 à 10 millions d'euros par mois.

Une prudence de sioux
Un des leitmotiv des cybercriminels français est la prudence. Pour approcher ce monde souterrain, il faut montrer patte blanche. L'objectif est d'éviter de se faire coincer par les forces de l'ordre. Le climat de méfiance règne donc allant jusqu'à la délation (signalement des actes malhonnêtes et frauduleux) et jusqu'à l'affrontement (les places de marché se piratent mutuellement pour se piquer des clients).
L'acceptation sur les forums fait par cooptation, par évaluation de la réputation. Mais ce qui distingue le Dark Net Français, c'est le recours à des tiers de confiance (escrow en anglais). Ils jouent un rôle d'intermédiaire dans la transaction entre les deux parties pour s'assurer que chacun récupère son dû. Ces intermédiaires prennent une commission (entre 5 et 7%) sur la transaction. Certaines places de marché ont même créé leurs propres plateformes de tiers de confiance (mais faut-il encore avoir confiance ?).
La disparition des forums est aussi un grand classique, comme le précise le chercheur de Trend Micro. « Un des forums les plus en vue du French Dark Net qui recensait 40 000 utilisateurs avec la possibilité de gérer leurs transactions a fermé du jour au lendemain et les administrateurs se sont enfuis avec la caisse. Le préjudice est estimé à 180 000 euros. » Et d'ajouter que les mêmes administrateurs ont créé une nouvelle structure dans les jours suivant. Rien ne se perd, tout se crée.

Chiffrement et bitcoin de rigueur
Parmi les autres enseignements, l'underground français n'échappe pas à la vague du chiffrement des communications. Logique, avec un degré de méfiance qui frise la paranoïa, les conversations sont chiffrées et plutôt fortement, assure Trend Micro. « On est principalement sur du PGP. » De même, l'usage de Tor s'est banalisé. Pour trouver les forums ou les places de marché, il est quasiment impossible de les repérer sur le web normal. Les sites se terminent par .onion indiquant son appartenance au réseau anonymisé Tor.
Le Bitcoin et les cartes prépayées sont les moyens de paiement préférés sur l'underground français. La crypto-monnaie est traditionnellement utilisée dans ce genre de secteur. Mais la carte prépayée PCS est une spécificité française. « Elles sont devenues si populaires que certains cybercriminels vendent ce type de cartes avec de faux papiers d'identité et des fausses informations personnelles comme adresse physique, e-mail et carte SIM. L'objectif est de déverrouiller le plafond de paiement pour atteindre jusqu'à 3000 euros. L'opération coûte à peu près 60 euros », souligne Trend Micro.

Le royaume des faux documents officiels et Pass PTT
Héritage du système jacobin et du régime napoléonien, la France est la partie des papiers administratifs. On ne s'étonnera donc pas que les propositions commerciales sur le Dark Net hexagonal concernent la fraude aux documents administratifs. Fausse carte d'identité, carte grise (500 euros), carte PMR (mobilité réduite pour 40 euros), justificatif de domicile (utile pour certaines démarches), vente de points pour le permis de conduire, ouverture d'un compte bancaire (700 euros).
Autre élément typiquement français, le pass PTT. Il s'agit d'une clé dont dispose les livreurs pour ouvrir l'ensemble des boîtes aux lettres d'un immeuble. Les personnes peuvent ainsi chercher des plis contenant de l'argent, des chéquiers ou des clés de maison. Ces pass PTT sont disponibles sur les forums underground à des tarifs abordables. Un vendeur proposait 25 clés pour 220 euros, un autre vendait à l'unité au tarif de 15 euros et un troisième livrait un fichier d'impression 3D de la dite clé, rapporte l'éditeur de sécurité…[lire la suite]

Réagissez à cet article

Original de l’article mis en page : Trend Micro ausculte la cybercriminalité underground en France