

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

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

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

Les techniques de social engineering, nouvelles armes de Carbanak ?

L'an passé, les pirates informatiques du groupe Carbanak ont frappé fort en parvenant à dérober près d'un milliard de dollars à différents établissements bancaires.

Eh bien, le gang a changé de cibles mais il est toujours prêt à frapper très fort. Désormais, ce sont les hôtels qui sont dans son collimateur et pour mener ces actions, Carbanak a recours aux techniques de « social engineering ».

Autrement dit, il se fait passer pour des clients d'un hôtel rencontrant des difficultés à réserver sur le système en ligne proposé par l'hôtelier et propose d'envoyer ses informations de réservation par mail laissant alors le piège se refermer sur l'établissement.

En effet, ce mail contient également un malware qui va infecter le système de l'hôtelier. Bien évidemment, en pirates expérimentés, ceux de Carbanak savent ne laisser planer aucun doute quant à leur identité et il est quasiment impossible pour le personnel d'un hôtel de se rendre compte que leur interlocuteur est là pour leur causer du tort.

Un malware voleur de données et aux effets dévastateurs

Dès lors que le malware a pénétré le système informatique d'un établissement hôtelier, ce dernier télécharge tout un panel de logiciels malveillants qui vont permettre de voler discrètement de nombreuses données.

S'il sera possible de dérober les données d'identité, les coordonnées postales ou les adresses électroniques, ce sont aussi les informations des cartes de crédit qui seront accessibles...[lire la suite]

Notre métier : Sensibiliser et former les décideurs et les utilisateurs aux risques liés à la **Cybercriminalité** et à la **Protection des Données Personnelles** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).

Denis JACOPINI anime dans toute la France et à l'étranger des conférences, des tables rondes et des formations pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles (Mise en Place d'un Correspondant Informatique et Libertés (CIL) dans votre établissement.

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



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

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



[Contactez-nous](#)

Réagissez à cet article

Les États... unis contre la cybercriminalité



La convention de Budapest sur la cybercriminalité fête ses quinze ans en 2016. À cette occasion, une conférence se tient du 16 au 18 novembre à Strasbourg...[Lire la suite]

Denis JACOPINI anime des **conférences, des formations** en Cybercriminalité et est régulièrement invité à des **tables rondes en France et à l'étranger** pour sensibiliser les décideurs et les utilisateurs aux **Dangers liés à la Cybercriminalité (Arnaques, Piratages...)** pour mieux s'en **protéger** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).

Plus d'informations sur sur cette page.



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

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



[Contactez-nous](#)

Réagissez à cet article

Le cyberharcèlement n'épargne pas les enseignants



Dans une société hyperconnectée, où plus de 8 Français sur 10

fréquentent Internet, l'école entend tirer parti des nouvelles technologies....[Lire la suite]

Denis JACOPINI anime des **conférences, des formations** en Cybercriminalité et est régulièrement invité à des **tables rondes en France et à l'étranger** pour sensibiliser les décideurs et les utilisateurs aux **Dangers liés à la Cybercriminalité (Arnaques, Piratages...)** pour mieux s'en **protéger** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Plus d'informations sur sur cette page.



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

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



[Contactez-nous](#)

Réagissez à cet article

De l'intelligence artificielle pour épauler les experts en cybersécurité



Arrêtons de taper tout le temps sur la tête des utilisateurs et de citer la faiblesse de l'humain comme la principale faille en matière de cybersécurité....[Lire la suite]

Denis JACOPINI anime des **conférences, des formations** en Cybercriminalité et est régulièrement invité à des **tables rondes en France et à l'étranger** pour sensibiliser les décideurs et les utilisateurs aux **Dangers liés à la Cybercriminalité (Arnaques, Piratages...)** pour mieux s'en **protéger** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Plus d'informations sur sur cette page.



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

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



[Contactez-nous](#)

Réagissez à cet article

De l'intelligence artificielle pour épauler les experts en cybersécurité



Arrêtons de taper tout le temps sur la tête des utilisateurs et de citer la faiblesse de l'humain comme la principale faille en matière de cybersécurité....[Lire la suite]

Denis JACOPINI anime des **conférences, des formations** en Cybercriminalité et est régulièrement invité à des **tables rondes en France et à l'étranger** pour sensibiliser les décideurs et les utilisateurs aux **Dangers liés à la Cybercriminalité (Arnaques, Piratages...)** pour mieux s'en **protéger** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Plus d'informations sur sur cette page.



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

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



[Contactez-nous](#)

Réagissez à cet article

Un collégien sur cinq est victime de cyberharcèlement

 **Un collégien sur cinq est victime de cyberharcèlement**

Longtemps accusé de ne pas faire grand-chose pour lutter contre les messages de haine sur son réseau social, Twitter a décidé de réagir. Zoom sur le cyberharcèlement à l'école en Haute-Loire. Insultes, menaces, racisme... Twitter fait maintenant la guerre au harcèlement...[Lire la suite]

Denis JACOPINI anime des **conférences, des formations** en Cybercriminalité et est régulièrement invité à des **tables**

rondes en France et à l'étranger pour sensibiliser les décideurs et les utilisateurs aux **Dangers liés à la Cybercriminalité (Arnaques, Piratages...)** pour mieux s'en protéger (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Plus d'informations sur sur cette page.



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

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



[Contactez-nous](#)

Réagissez à cet article

**Vos médias sociaux
personnalisent ce ransomware
pour mieux vous piéger**

Balliffs Service
Department of pre-trial settlement
Date of issue: Oct 26, 2016
Ref. #: 10/26/2016-200

PENALTY NOTICE

PENALTIES DETAILS

Amount: \$100
Due date: Oct 27, 2016
Remaining:

WE HEREBY INFORM YOU THAT ON YOUR PC FOUND

ALL ACTIVITY OF THIS PC IS BEING RECORDED
USING AUDIO, VIDEO AND OTHER DEVICES

REC



00:00:00
SAVED DATA WILL BE USED FOR IDENTIFICATION
AND WILL BE SENT TO GOVERNMENT AGENCIES

1. CHILD SEXUAL ABUSE MATERIALS

We would like to inform you that pursuant to the provisions of 18 U.S. Code § 1466A and 18 U.S. Code § 2252A, any person shall be fined up to \$200,000 and imprisoned for not less than 15 years not more than 40 years.

\$200,000
40 years in prison

2. MATERIALS THAT VIOLATE THE INTELLECTUAL PROPERTY RIGHTS

We would like to inform you that pursuant to the provisions of 17 U.S. Code § 504, willful copyright infringement carries a penalty up to \$150,000 per instance.

\$150,000
per instance

3. SUSPICIOUS ACTIVITY

We would like to inform you that pursuant to the provisions of 18 U.S. Code § 1030, any person shall be fined up to \$100,000, imprisoned for not more than 10 years, or both.

\$100,000
10 years in prison

In the course of pre-trial settlement, in case of removal of all detected violations, and payment of the fine within 3 hours since the receipt of this notice,

ALL ACTIONS WILL BE STOPPED AND THE PROCEEDINGS WILL BE CEASED!
(ALL MONEY WILL BE REFUNDED TO YOU IF YOU ARE NOT CAUGHT AGAIN WITHIN 180 DAYS)

You must pay penalty within 3 hours to settle the case out of court. In case of failure to comply claims

ALL COLLECTED DATA WILL BE MADE PUBLIC AND THE CASE GOES TO TRIAL!

Please note:

You must pay penalty within 3 hours
to settle the case out of court!

**PAY A PENALTY OF \$100
TO SETTLE THE CASE OUT OF COURT**

criminal-report.com

CRIMINAL CASE HAS BEEN INITIATED!

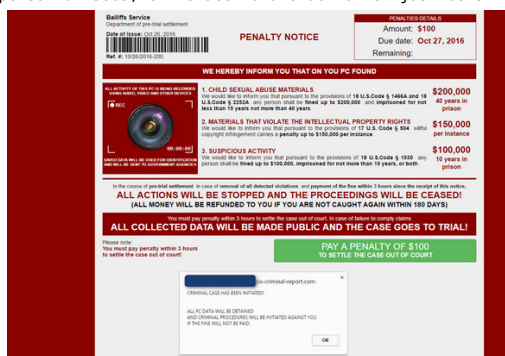
ALL PC DATA WILL BE DETAINED
AND CRIMINAL PROCEDURES WILL BE INITIATED AGAINST YOU
IF THE FINE WILL NOT BE PAID.

OK

Un
Ransomware
utilise
vos media
sociaux
pour mieux
vous
piéger

Ransoc utilise les médias sociaux pour personnifier la menace et tenter d'attendrir ses victimes. Car rien ne vaut les détails personnels pour faire peur.

Une nouvelle forme de ransomware utilise les comptes des médias sociaux et les fichiers locaux des victimes afin de créer des demandes personnalisées, et menacer d'une action en justice si la rançon n'est pas payée.



Nommé Ransoc par les chercheurs en cybersécurité de Proofpoint en raison de son lien avec les médias sociaux, y compris Facebook, LinkedIn et Skype, ce ransomware est une nouvelle évolution du logiciel malveillant qui s'est répandu cette année sur le Web. Ce n'est pas la première variante de ransomware à utiliser l'ingénierie sociale pour forcer les victimes à payer, mais Ransoc est unique par sa façon de retourner les fichiers des utilisateurs contre eux – surtout si ces fichiers sont téléchargés.

Pas de chiffrement, de la menace directe

Peut-être parce qu'il se concentre sur l'exploitation de cette peur, Ransoc ne chiffre pas les fichiers des victimes de la même manière qu'un ransomware comme Locky. Ransoc livre tout simplement ses exigences via le navigateur après avoir infecté le système via Internet Explorer sur Windows et Safari sur OS X.

Ce procédé pourrait paraître basique ou daté par rapport à des formes plus sophistiquées de ransomware – les ransomwares qui verrouillent les ordinateurs ont vu leur apogée entre 2012 et 2014 – mais Ransoc est construit de manière à pouvoir rechercher sur les disques durs de la victime et sur les médias sociaux les données qu'il va pouvoir ensuite utiliser. Ces données seront ensuite façonnées pour réaliser une demande de rançon sur mesure, en y incluant des images issues de comptes Facebook et LinkedIn.

Détection de matériel illégal

Les chercheurs de Proofpoint ont découvert qu'une variante de la demande de rançon n'est affichée que lorsque Ransoc soupçonne la victime de posséder des fichiers contenant des images illégales ou des fichiers multimédias téléchargés via un protocole torrent. Dans ce cas, Ransoc menace la victime d'une amende et de divulguer ces informations dans le cadre d'une action en justice.

Contrairement à la plupart des systèmes utilisés dans les ransomware, qui exigent des paiements intraquables en Bitcoin, les auteurs de Ransoc ont choisi de faire payer les victimes avec leur carte de crédit.

...[lire la suite]

Notre métier : Sensibiliser les décideurs et les utilisateurs aux risques liés à la **Cybercriminalité** et à la **Protection des Données Personnelles** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).

Denis JACOPINI anime dans toute la France et à l'étranger des conférences, des tables rondes et des formations pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles (Mise en Place d'un Correspondant Informatique et Libertés (CIL) dans votre établissement.

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



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

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

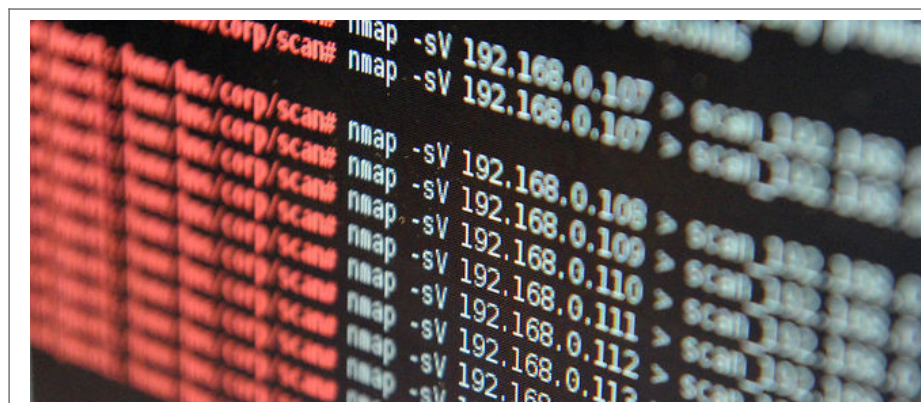


Contactez-nous

Réagissez à cet article

Original de l'article mis en page : Ce ransomware utilise vos profils de médias sociaux pour personnaliser ses demandes – ZDNet

14 millions de Français victimes des pirates Informatiques en 2016



14 millions
de Français
victimes des
pirates
Informatiques
en 2016

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

Dans un rapport publié mercredi 16 novembre, l'éditeur d'antivirus Symantec-Norton pointe l'ampleur que le phénomène « cybercriminel » a prise en 2016. Selon cette étude, 13,7 millions de Français auront été victimes d'attaques informatiques cette année. Le fait d'avoir baigné dans l'univers numérique depuis sa naissance ne change rien à la donne. Les « digital natives » (comme les experts désignent les jeunes qui manipulent des ordinateurs depuis le berceau) sont aussi démunis face à cette menace que leurs aînés.

La génération Y, celle des 18-34 ans, fait ainsi partie des plus touchées par le problème. Il faut dire que cette catégorie de population se comporte sur le Web de manière particulièrement risquée. Or, pour les professionnels de la cybersécurité, la négligence des internautes serait en cause dans la plupart des attaques informatiques dont ils sont victimes.

Des internautes imprudents

Bien que 77 % des Français sachent qu'ils doivent protéger leurs données en ligne, les utilisateurs gardent de mauvaises habitudes sur le Web. Les réflexes d'élémentaire prudence sont de peu de poids face à l'attrait de certains liens... même d'origine douteuse. Ainsi, 65 % des Français reconnaissent avoir déjà ouvert une pièce jointe postée d'un expéditeur inconnu. Et quasiment un internaute sur cinq partage ses mots de passe avec d'autres utilisateurs. Faut-il, dès lors, s'étonner qu'un Français sur deux se résigne à l'idée qu'il est désormais plus probable qu'une personne accède frauduleusement à ses appareils domestiques connectés qu'à son logement ?

D'après Laurent Heslault, directeur des stratégies numériques chez Symantec, les internautes ont bien conscience des dangers mais « n'ont pas envie de prendre les précautions adéquates pour assurer leur sécurité ». Alors que les cybercriminels, eux, disposent de techniques de plus en plus recherchées pour arriver à leurs fins.

Il ne s'agit pas seulement de paresse chez les internautes. 31 % d'entre eux sont dépassés par la quantité d'informations qu'ils ont à protéger. La plupart considèrent d'ailleurs que la question de la gestion sécurisée des données ne les concerne pas et qu'il appartient aux fournisseurs d'accès à Internet et aux entreprises du secteur des nouvelles technologies de résoudre ces problèmes.

Un problème mondial

Une étude réalisée en octobre, par le Ponemon Institute pour le compte de l'éditeur de logiciels professionnels Varonis Systems, démontre qu'il ne s'agit pas d'un problème strictement hexagonal. Si 37 % (seulement !) des internautes français indiquent qu'ils prennent toutes les mesures appropriées pour protéger les données auxquelles ils accèdent et qu'ils utilisent, la même réponse est donnée par 50 % chez les collaborateurs allemands, 39 % des employés britanniques et 35 % des employés américains.

Le nombre d'entreprises ayant fait l'expérience des ransomwares l'an dernier est en hausse constante. Ces logiciels rançonneurs, dont le FBI a révélé qu'ils avaient généré, au premier semestre 2016, plus de 209 millions de dollars de butin, ont infecté les serveurs de 12 % des entreprises allemandes, contre 17 % aux États-Unis, 16 % en France et 13 % au Royaume-Uni. Le nombre de cas de perte ou de vol de données au cours des deux dernières années a, lui aussi, explosé... Et l'on ne compte plus les cyberbraquages signalés chaque semaine à travers la planète.

De quoi inciter les États à renforcer leur arsenal pour lutter plus efficacement contre les gangs à l'oeuvre sur la Toile. Les 68 pays signataires de la convention de Budapest, le premier traité international abordant la question de la lutte contre la cybercriminalité adopté en 2001, se sont d'ailleurs réunis les 14 et 15 novembre derniers pour renforcer leur coopération en la matière. Un protocole additionnel à la convention sera adopté courant 2017 pour mettre en place un nouvel outil juridique permettant de collecter des preuves électroniques sur le « cloud », quelle que soit la localisation du serveur qui l'héberge... Preuve, s'il en était besoin, que les gouvernements du monde entier ont pris la mesure de la menace.

Quels sont les cyberdélicts les plus fréquents en France ?

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

Notre métier : Sensibiliser les décideurs et les utilisateurs aux risques liés à la **Cybercriminalité** et à la **Protection des Données Personnelles** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).

Denis JACOPINI anime dans toute la France et à l'étranger des conférences, des tables rondes et des formations pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles (Mise en Place d'un Correspondant Informatique et Libertés (CIL) dans votre établissement.

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



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

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



[Contactez-nous](#)

Réagissez à cet article

Original de l'article mis en page : Cybersécurité : un Français sur cinq victime de hackers en 2016

Une backdoor chinoise planquée dans des smartphones Android



Y a-t-il un espion dans plus de 700 millions de smartphones Android ? Oui, selon les chercheurs de la société Kryptowire, une start-up de sécurité soutenue par la DARPA et le Département américain de la sécurité intérieure, qui vient de rendre public ses travaux mettant en cause un firmwar...[Lire la suite]

Denis JACOPINI anime des **conférences, des formations** en Cybercriminalité et est régulièrement invité à des **tables rondes en France et à l'étranger** pour sensibiliser les décideurs et les utilisateurs aux **Dangers liés à la Cybercriminalité (Arnaques, Piratages...)** pour mieux **s'en protéger** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Plus d'informations sur sur cette page.



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

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



[Contactez-nous](#)

Réagissez à cet article

Un amateur de jeux vidéos derrière une cyberattaque



La cyberattaque géante qui a paralysé en octobre de nombreux sites internet aux Etats-Unis a probablement été perpétrée par un amateur de jeux vidéos en colère, a affirmé mercredi un expert en informatique proche du dossier....[Lire la suite]

Denis JACOPINI anime des **conférences, des formations** en Cybercriminalité et est régulièrement invité à des **tables rondes en France et à l'étranger** pour sensibiliser les décideurs et les utilisateurs aux **Dangers liés à la Cybercriminalité (Arnaques, Piratages...)** pour mieux s'en **protéger** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Plus d'informations sur sur cette page.



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

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



[Contactez-nous](#)

Réagissez à cet article