

Attention aux fausses sociétés d'assistance informatique !



Attention
aux fausses
sociétés
d'assistance
informatique
!

Les cybercriminels présentent la particularité d'être inventifs et très opportunistes. La médiatisation de la cyberattaque Wannacry a créé une peur que des hackers mal intentionnés ont parfaitement su utiliser.

Ainsi, les spams (courriels indésirables, généralement publicitaires) ont augmenté de 57% au deuxième trimestre 2017 d'après Kaspersky Lab. Avec une particularité : de nombreux courriels contenaient « *des offres de services de lutte contre Wannacry, des conseils pour éviter d'infection ainsi que des invitations à des séminaires de formation* ». Les escrocs en ont profité pour envoyer de fausses notifications, au nom d'éditeurs connus de logiciels, qui signalaient au destinataire que son ordinateur avait été infecté et qu'il fallait cliquer sur un lien pour installer une mise à jour. Problème : ce lien menait sur une page de *phishing*, c'est-à-dire un formulaire incitant les victimes à entrer des informations personnelles, utilisées ensuite pour effectuer une usurpation d'identité...[lire la suite]

NOTRE MÉTIER :

EXPERTISES / COLLECTE & RECHERCHE DE PREUVES : Nous mettons à votre disposition notre expérience en matière d'expertise technique et judiciaire ainsi que nos meilleurs équipements en vue de collecter ou rechercher des preuves dans des téléphones, ordinateurs et autres équipements numériques;

PRÉVENTION : Nous vous apprenons à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) sous forme de conférences, d'audits ou de formations ;

SUPERVISION : En collaboration avec votre société de maintenance informatique, nous assurons le suivi de la sécurité de votre installation pour son efficacité maximale ;

AUDITS CNIL / AUDIT SÉCURITÉ / ANALYSE D'IMPACT : Fort de notre expérience d'une vingtaine d'années, de notre certification en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005) et des formations suivies auprès de la CNIL, nous réaliseront un état des lieux (audit) de votre installation en vue de son amélioration, d'une analyse d'impact ou de sa mise en conformité ;

MISE EN CONFORMITÉ CNIL/RGPD : Nous mettons à niveau une personne de votre établissement qui deviendra référent CNIL et nous l'assistons dans vos démarches de mise en conformité avec le RGPD (Règlement Européen relatif à la Protection des Données à caractère personnel).

Besoin d'un Expert ? contactez-vous

NOS FORMATIONS

: <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>
(Numéro formateur n°93 84 03041 84 (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle))



Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
(Autorisation de la DRTEF n°93 84 03041 84)
- 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

Source : *Cyberattaques, spams, malwares : les cybercriminels n'ont pas chômé au deuxième trimestre*

Une faille dangereuse découverte sur les hoverboards



Une faille
dangereuse
découverte
sur les
hoverboards

Des experts chez Alibaba Security se sont penchés sur le niveau de sécurité des hoverboards. Résultat, ils sont parvenus à mettre à jour une faille qui pourrait être dangereuse pour les utilisateurs. Les tests menés par les spécialistes ont démontré qu'il était possible de brouiller les capteurs de mouvement des hoverboards. L'utilisateur pourrait alors tomber et se blesser.

Les démonstrations, faites lors de la conférence Black Hat Security en juillet, ont révélé que la faiblesse des hoverboards n'était autre que les ondes sonores. Projetées sur les capteurs, elles peuvent perturber les mesures et données collectées par ces derniers, déséquilibrant du même coup l'hoverboard et son utilisateur...[lire la suite]

NOTRE MÉTIER :

EXPERTISES / COLLECTE & RECHERCHE DE PREUVES : Nous mettons à votre disposition notre expérience en matière d'expertise technique et judiciaire ainsi que nos meilleurs équipements en vue de collecter ou rechercher des preuves dans des téléphones, ordinateurs et autres équipements numériques;

PRÉVENTION : Nous vous apprenons à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) sous forme de conférences, d'audits ou de formations ;

SUPERVISION : En collaboration avec votre société de maintenance informatique, nous assurons le suivi de la sécurité de votre installation pour son efficacité maximale ;

AUDITS CNIL / AUDIT SÉCURITÉ / ANALYSE D'IMPACT : Fort de notre expérience d'une vingtaine d'années, de notre certification en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005) et des formations suivies auprès de la CNIL, nous réaliserons un état des lieux (audit) de votre installation en vue de son amélioration, d'une analyse d'impact ou de sa mise en conformité ;

MISE EN CONFORMITÉ CNIL/RGPD : Nous mettons à votre disposition une personne de votre établissement qui deviendra référent CNIL et nous l'assistons dans vos démarches de mise en conformité avec le RGPD (Règlement Européen relatif à la Protection des Données à caractère personnel).

Besoin d'un Expert ? contactez-vous

NOS FORMATIONS

: <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>
(Numéro formateur n°93 84 03041 84 (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle))



Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité », « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
(Autorisation de la DRTEF n°93 84 03041 84)
- 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

Source : *Les hoverboards ont un talon d'Achille, les ondes sonores*

Trouver une faille de sécurité peut rapporter jusqu'à 500 000 dollars



Trouver
une
faille de
sécurité
peut
rapporter
jusqu'à
500 000
dollars

La société Zerodium, spécialisée dans le commerce de failles zero-day, revient avec un nouvel appel d'offre : un demi million de dollars à quiconque apportera sur un plateau une vulnérabilité inconnue dans les applis de messagerie WhatsApp et Signal.

Quel est le prix de votre vie privée ? 499 999 dollars, ça vous semble correct ? Parce qu'à vrai dire, elle pourrait être bientôt être vendue pour seulement un dollar de plus. L'entreprise Zerodium, spécialisée dans l'achat et la revente de vulnérabilités zero-day, vient de proposer la rondelette somme de 500 000 dollars à celui qui sera capable mettre au point les outils nécessaires au piratage des applications de messagerie cryptée Signal et WhatsApp. Déjà, en octobre 2016, elle avait proposé 1,5 millions de dollars pour une faille dans iOS 10...[lire la suite]

NOTRE MÉTIER :

EXPERTISES / COLLECTE & RECHERCHE DE PREUVES : Nous mettons à votre disposition notre expérience en matière d'expertise technique et judiciaire ainsi que nos meilleurs équipements en vue de collecter ou rechercher des preuves dans des téléphones, ordinateurs et autres équipements numériques;

PRÉVENTION : Nous vous apprenons à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) sous forme de conférences, d'audits ou de formations ;

SUPERVISION : En collaboration avec votre société de maintenance informatique, nous assurons le suivi de la sécurité de votre installation pour son efficacité maximale ;

AUDITS CNIL / AUDIT SÉCURITÉ / ANALYSE D'IMPACT : Fort de notre expérience d'une vingtaine d'années, de notre certification en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005) et des formations suivies auprès de la CNIL, nous réaliserons un état des lieux (audit) de votre installation en vue de son amélioration, d'une analyse d'impact ou de sa mise en conformité ;

MISE EN CONFORMITÉ CNIL/RGPD : Nous mettons à niveau une personne de votre établissement qui deviendra référent CNIL et nous l'assistons dans vos démarches de mise en conformité avec le RGPD (Règlement Européen relatif à la Protection des Données à caractère personnel).

Besoin d'un Expert ? contactez-vous

NOS FORMATIONS

: <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>
(Numéro formateur n°93 84 03041 84 (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle))



Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
(Autorisation de la DRTEF n°93 84 03041 84)
- 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

Source : Une entreprise offre 500 000 dollars à celui qui

trouvera une faille de sécurité exploitable sur WhatsApp et Signal

Piratage du compte Twitter et de la page Facebook du Real Madrid



Ce samedi matin, le compte Twitter et la page Facebook du Real Madrid ont été la cible d'un hacker, qui a notamment annoncé l'arrivée de Lionel Messi chez les Merengue. Une cyber-attaque qui survient quelques jours seulement après celle subie par le FC Barcelone. Les supporters madrilènes ont dû avoir une drôle de surprise ce samedi matin en se rendant sur les réseaux sociaux. Sur Facebook comme sur Twitter, le Real a en effet été victime d'une cyber-attaque. Pendant une bonne heure, le hacker à l'origine de cette acteur a ainsi publié de fausses informations, parmi lesquelles l'arrivée de Lionel Messi sous le maillot merengue et la vente de Karim Benzema...[lire la suite]

NOTRE MÉTIER :

EXPERTISES / COLLECTE & RECHERCHE DE PREUVES : Nous mettons à votre disposition notre expérience en matière d'expertise technique et judiciaire ainsi que nos meilleurs équipements en vue de collecter ou rechercher des preuves dans des téléphones, ordinateurs et autres équipements numériques;

PRÉVENTION : Nous vous apprenons à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) sous forme de conférences, d'audits ou de formations ;

SUPERVISION : En collaboration avec votre société de maintenance informatique, nous assurons le suivi de la sécurité de votre installation pour son efficacité maximale ;

AUDITS CNIL / AUDIT SÉCURITÉ / ANALYSE D'IMPACT : Fort de notre expérience d'une vingtaine d'années, de notre certification en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005) et des formations suivies auprès de la CNIL, nous réaliseront un état des lieux (audit) de votre installation en vue de son amélioration, d'une analyse d'impact ou de sa mise en conformité ;

MISE EN CONFORMITÉ CNIL/RGPD : Nous mettons à niveau une personne de votre établissement qui deviendra référent CNIL et nous l'assistons dans vos démarches de mise en conformité avec le RGPD (Règlement Européen relatif à la Protection des Données à caractère personnel).

Besoin d'un Expert ? contactez-vous

NOS FORMATIONS

: <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>
(Numéro formateur n°93 84 03041 84 (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle))



Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
(Autorisation de la DRTEF n°93 84 03041 84)
- 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

Source : *Victimes d'un piratage, le compte Twitter et la page Facebook du Real Madrid ont annoncé la signature de Lionel*

Les failles utilisées par les hackers ont plus de 10 ans



Les
failles
utilisées
par les
hackers
ont plus
de 10 ans

Les récentes attaques de malwares et de ransomwares survenues en 2017, dont WannaCry et Petya/NotPetya ont été les plus répandues et médiatisées, ont permis aux spécialistes de la cybersécurité d'avoir une vision plus claire des failles utilisées par les hackers.

Fortinet, spécialiste de la cybersécurité, a analysé les attaques dont ont été victimes ses clients, généralement des entreprises. Dans le rapport publié en août 2017, il est mis l'accent sur la vétusté des failles utilisées par les hackers : la très grande majorité des attaques n'aurait pas pu être menée à bien si les systèmes avaient été mis à jour. Les chiffres sont éloquentes : dans 90 % des cas, les victimes ont été attaquées par le biais de failles datant de plus de 3 ans et dans 60 % des cas, ces failles étaient vieilles de 10 ans voire plus. L'attaque WannaCry a utilisé la faille EternalBlue de Windows qui faisait partie des outils de la NSA pour espionner ses cibles. Cette faille avait été rendue publique par les hackers du groupe *The Shadow Brokers*...[lire la suite]

NOTRE MÉTIER :

EXPERTISES / COLLECTE & RECHERCHE DE PREUVES : Nous mettons à votre disposition notre expérience en matière d'expertise technique et judiciaire ainsi que nos meilleurs équipements en vue de collecter ou rechercher des preuves dans des téléphones, ordinateurs et autres équipements numériques;

PRÉVENTION : Nous vous apprenons à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) sous forme de conférences, d'audits ou de formations ;

SUPERVISION : En collaboration avec votre société de maintenance informatique, nous assurons le suivi de la sécurité de votre installation pour son efficacité maximale ;

AUDITS CNIL / AUDIT SÉCURITÉ / ANALYSE D'IMPACT : Fort de notre expérience d'une vingtaine d'années, de notre certification en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005) et des formations suivies auprès de la CNIL, nous réaliserons un état des lieux (audit) de votre installation en vue de son amélioration, d'une analyse d'impact ou de sa mise en conformité ;

MISE EN CONFORMITÉ CNIL/RGPD : Nous mettons à niveau une personne de votre établissement qui deviendra référent CNIL et nous l'assistons dans vos démarches de mise en conformité avec le RGPD (Règlement Européen relatif à la Protection des Données à caractère personnel).

Besoin d'un Expert ? contactez-vous

NOS FORMATIONS

: <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>
(Numéro formateur n°93 84 03041 84 (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle))



Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
(Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



Réagissez à cet article

Source : *Les failles utilisées par les hackers ont plus de 10 ans*

Un nouveau ransomware, Defray, cible l'éducation et la santé



Les chercheurs Proofpoint ont récemment analysé un nouveau ransomware, nommé Defray. Durant le mois d'août, ils ont observé plusieurs attaques ciblées, visant notamment les secteurs de la santé, de l'éducation, de l'industrie et de l'informatique.

« Defray » a été choisi en rapport avec le nom d'hôte du serveur de commande et de contrôle (C&C) de la première attaque observée :

defrayable-listings[.]000webhostapp[.]com Par coïncidence, le terme « defray » signifie fournir de l'argent pour payer une partie d'un coût, bien que ce dont les victimes doivent s'acquitter ne soit pas tout à fait clair.

La distribution de Defray présente plusieurs caractéristiques :

- Defray est diffusé via des documents Word dans des pièces jointes d'emails
 - Les pièges sont conçus sur mesure pour attirer toutes les victimes potentielles
 - Les destinataires sont des individus ou bien des groupes d'individus, par exemple, group@ ou websupport@
 - Les pays les plus touchés sont le Royaume-Uni et les États-Unis
- [Global Security Mag Online]

NOTRE MÉTIER :

EXPERTISES / COLLECTE & RECHERCHE DE PREUVES : Nous mettons à votre disposition notre expérience en matière d'expertise technique et judiciaire ainsi que nos meilleurs équipements en vue de collecter ou rechercher des preuves dans des téléphones, ordinateurs et autres équipements numériques;

PRÉVENTION : Nous vous apprenons à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) sous forme de conférences, d'audits ou de formations ;

SUPERVISION : En collaboration avec votre société de maintenance informatique, nous assurons le suivi de la sécurité de votre installation pour son efficacité maximale ;

AUDITS CNIL / AUDIT SÉCURITÉ / ANALYSE D'IMPACT : Fort de notre expérience d'une vingtaine d'années, de notre certification en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005) et des formations suivies auprès de la CNIL, nous réaliseront un état des lieux (audit) de votre installation en vue de son amélioration, d'une analyse d'impact ou de sa mise en conformité ;

MISE EN CONFORMITÉ CNIL/RGPD : Nous mettons à niveau une personne de votre établissement qui deviendra référent CNIL et nous l'assistons dans vos démarches de mise en conformité avec le RGPD (Règlement Européen relatif à la Protection des Données à caractère personnel).

Besoin d'un Expert ? contactez-vous

NOS FORMATIONS

: <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>
(Numéro formateur n°93 84 03041 84 (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle))



Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
(Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



Réagissez à cet article

Source : Defray, le nouveau ransomware qui cible l'éducation et la santé – Global Security Mag Online

Mots de passe Wifi des espaces Lounges des principaux aéroports à travers le monde. Les conseils de Denis JACOPINI



Mots de passe Wifi des
espaces Lounges des
principaux aéroports à
travers le monde. Les
conseils de Denis
JACOPINI

Une base de donnée de nombreux codes d'accès Wifi des principaux aéroports à travers le monde accessible librement sur une carte Google Maps. Toutefois, même si le service paraît très utile, il peut aussi devenir un piège à voyageurs. Denis JACOPINI nous en dit plus

Même si pour beaucoup les vacances sont terminées, pour d'autres le réflexe à peine descendu d'un vol lors d'une escale ou arrivé à destination est de vérifier ses mails pour certains, ses j'aime, ses stats ou flash pour d'autres.

Autant anticiper en consultant cette carte et récupérer les identifiants et mots de passe des aéroports qui seront visités (avant de partir).

[Accéder à la carte avec la liste des aéroports]

Attention toutefois à prendre vos précautions lorsque vous utiliserez ces réseaux Wifi inconnus, publics ou libres ! Des pirates peuvent traîner par là et récupérer vos codes, vos informations ou pire, infecter leurs voisins numériques. Protégez bien votre ordinateur avec un système de sécurité à jour et utilisez un VPN pour accéder à des informations sensibles.

Maintenant, si c'est trop tard pour les utiliser lors des vacances de cette année pour certains, conservez précieusement ces informations pour l'année prochaine ☐

Denis JACOPINI

NOTRE MÉTIER :

EXPERTISES / COLLECTE & RECHERCHE DE PREUVES : Nous mettons à votre disposition notre expérience en matière d'expertise technique et judiciaire ainsi que nos meilleurs équipements en vue de collecter ou rechercher des preuves dans des téléphones, ordinateurs et autres équipements numériques;

PRÉVENTION : Nous vous apprenons à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) sous forme de conférences, d'audits ou de formations ;

SUPERVISION : En collaboration avec votre société de maintenance informatique, nous assurons le suivi de la sécurité de votre installation pour son efficacité maximale ;

AUDITS CNIL / AUDIT SÉCURITÉ / ANALYSE D'IMPACT : Fort de notre expérience d'une vingtaine d'années, de notre certification en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005) et des formations suivies auprès de la CNIL, nous réaliseront un état des lieux (audit) de votre installation en vue de son amélioration, d'une analyse d'impact ou de sa mise en conformité ;

MISE EN CONFORMITÉ CNIL/RGPD : Nous mettons à niveau une personne de votre établissement qui deviendra référent CNIL et nous l'assistons dans vos démarches de mise en conformité avec le RGPD (Règlement Européen relatif à la Protection des Données à caractère personnel).

Besoin d'un Expert ? contactez-vous

NOS FORMATIONS

: <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>

(Numéro formateur n°93 84 03041 84 (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle))



Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



Réagissez à cet article

Source : *Wireless Passwords From Airports And Lounges Around The World*

Attention à Faketoken, le malware Android qui vole les données bancaires en copiant des applis



Attention
à
Faketoken,
le malware
Android
qui vole
les
données
bancaires
en copiant
des applis

Une version améliorée d'un cheval de Troie bancaire vieux d'un an a été repérée par des chercheurs en sécurité en Russie.

Pour la firme de sécurité Kaspersky les malwares bancaires sont l'une des plus grandes menaces qui pèsent sur les smartphones Android. L'un d'eux, Faketoken, connu depuis un an environ, est de retour sous une nouvelle forme plus dangereuse, prévient-elle.

Au départ, ce cheval de Troie interceptait des SMS pour y récupérer des données bancaires que des utilisateurs imprudents auraient pu y indiquer. Désormais, il se greffe directement sur des applis bancaires ou sur des applis de réservations de taxis, de VTC ou d'hôtels afin de faire la même opération et écoute vos appels.

Comment parvient-il à infecter un smartphone ? Grâce à l'envoi en masse de SMS proposant de télécharger des photos. Dès lors qu'un utilisateur clique sur le lien, le malware s'installe discrètement sur l'appareil...[lire la suite]

NOTRE MÉTIER :

EXPERTISES / COLLECTE & RECHERCHE DE PREUVES : Nous mettons à votre disposition notre expérience en matière d'expertise technique et judiciaire ainsi que nos meilleurs équipements en vue de collecter ou rechercher des preuves dans des téléphones, ordinateurs et autres équipements numériques;

PRÉVENTION : Nous vous apprenons à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) sous forme de conférences, d'audits ou de formations ;

SUPERVISION : En collaboration avec votre société de maintenance informatique, nous assurons le suivi de la sécurité de votre installation pour son efficacité maximale ;

AUDITS CNIL / AUDIT SÉCURITÉ / ANALYSE D'IMPACT : Fort de notre expérience d'une vingtaine d'années, de notre certification en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005) et des formations suivies auprès de la CNIL, nous réaliserons un état des lieux (audit) de votre installation en vue de son amélioration, d'une analyse d'impact ou de sa mise en conformité ;

MISE EN CONFORMITÉ CNIL/RGPD : Nous mettons à niveau une personne de votre établissement qui deviendra référent CNIL et nous l'assistons dans vos démarches de mise en conformité avec le RGPD (Règlement Européen relatif à la Protection des Données à caractère personnel).

Besoin d'un Expert ? contactez-vous

NOS FORMATIONS

: <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>
(Numéro formateur n°93 84 03041 84 (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle))



Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
(Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



Réagissez à cet article

Source : *Faketoken, le malware qui vole les données bancaires en copiant des applis*

La stéganographie pour cacher des informations volées dans les images



En analysant de multiples campagnes de cyberespionnage et de cybercriminalité, les chercheurs de Kaspersky Lab ont identifié une nouvelle tendance inquiétante : des pirates emploient de plus en plus la stéganographie, une version numérique d'un stratagème ancien consistant à dissimuler des messages à l'intérieur d'images, afin de masquer les traces de leur activité malveillante sur un ordinateur attaqué. Un certain nombre de malwares espions ainsi que plusieurs autres destinés au vol d'informations financières ont récemment été repérés utilisant cette technique.

Dans le cadre d'une cyberattaque ciblée type, un acteur malveillant – une fois infiltré dans le réseau attaqué – établit une tête de pont puis collecte des informations de valeur afin de les transférer par la suite à un serveur de commande et de contrôle (C&C). Dans la plupart des cas, des solutions de sécurité ou des outils analytiques professionnels éprouvés sont en mesure de détecter la présence de l'intrus sur le réseau à chaque phase d'une attaque, notamment au moment de l'exfiltration des données volées. En effet, cette exfiltration laisse généralement des traces, par exemple l'enregistrement de connexions à une adresse IP inconnue ou inscrite en liste noire. Or le recours à la stéganographie rend cette détection difficile...[lire la suite]

NOTRE MÉTIER :

EXPERTISES / COLLECTE & RECHERCHE DE PREUVES : Nous mettons à votre disposition notre expérience en matière d'expertise technique et judiciaire ainsi que nos meilleurs équipements en vue de collecter ou rechercher des preuves dans des téléphones, ordinateurs et autres équipements numériques;

PRÉVENTION : Nous vous apprenons à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) sous forme de conférences, d'audits ou de formations ;

SUPERVISION : En collaboration avec votre société de maintenance informatique, nous assurons le suivi de la sécurité de votre installation pour son efficacité maximale ;

AUDITS CNIL / AUDIT SÉCURITÉ / ANALYSE D'IMPACT : Fort de notre expérience d'une vingtaine d'années, de notre certification en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005) et des formations suivies auprès de la CNIL, nous réaliserons un état des lieux (audit) de votre installation en vue de son amélioration, d'une analyse d'impact ou de sa mise en conformité ;

MISE EN CONFORMITÉ CNIL/RGPD : Nous mettons à niveau une personne de votre établissement qui deviendra référent CNIL et nous l'assistons dans vos démarches de mise en conformité avec le RGPD (Règlement Européen relatif à la Protection des Données à caractère personnel).

Besoin d'un Expert ? contactez-vous

NOS FORMATIONS

: <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>
(Numéro formateur n°93 84 03041 84 (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle))



Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

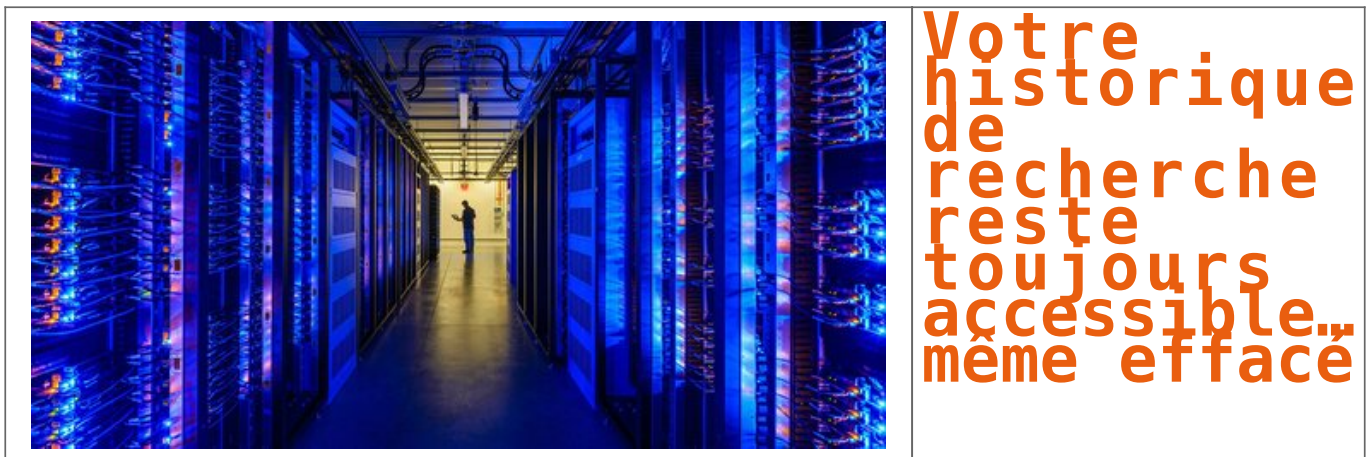
- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



Réagissez à cet article

Source : *Plusieurs groupes de pirates utilisent de plus en plus la technique de la stéganographie pour cacher des informations volées dans les images – Global Security Mag Online*

Votre historique de recherche reste toujours accessible... même effacé



Des sites pornographiques qu'on a visités aux simples liens un peu honteux en passant par les plus classiques marketplaces et réseaux sociaux, on n'aime pas forcément qu'un tiers fouille dans notre historique Internet. C'est pour ça qu'on le supprime assez régulièrement. Mais selon un chercheur en sécurité informatique, ça serait loin de suffire : on peut désanonymiser votre navigation.

Ce n'est pas la première fois qu'une telle thèse est prouvée : cette fois, Svea Deckert et Andreas Dewes en ont fait la démonstration lors de la conférence **Def Con 2017** de Las Vegas.

Les données anonymes collectées par les sites ne sont pas si anonymes que ça

Encore une fois, ce sont les sites Internet qui sont en cause et plus particulièrement les données de navigation qu'ils collectent. Ces données sont stockées pour être revendues à des tiers qui les utilisent, entre autres, pour faire de la publicité ciblée. Il n'y a rien d'illégal là-dedans, pour peu que ces données soient totalement anonymes, c'est-à-dire qu'elles ne doivent pas être reliées à l'adresse IP, unique, de l'utilisateur.

Théoriquement, l'anonymisation de ces données devrait suffire à garantir qu'il soit impossible de remonter à vous et de dire que vous avez visité telle ou telle page. Sauf que Svea Eckert et Andreas Dewes ont prouvé le contraire, en se basant sur les données collectées par 10 extensions pour navigateur Internet parmi les plus populaires du marché...[lire la suite]

NOTRE MÉTIER :

EXPERTISES / COLLECTE & RECHERCHE DE PREUVES : Nous mettons à votre disposition notre expérience en matière d'expertise technique et judiciaire ainsi que nos meilleurs équipements en vue de collecter ou rechercher des preuves dans des téléphones, ordinateurs et autres équipements numériques;

PRÉVENTION : Nous vous apprenons à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) sous forme de conférences, d'audits ou de formations ;

SUPERVISION : En collaboration avec votre société de maintenance informatique, nous assurons le suivi de la sécurité de votre installation pour son efficience maximale ;

AUDITS CNIL / AUDIT SÉCURITÉ / ANALYSE D'IMPACT : Fort de notre expérience d'une vingtaine d'années, de notre certification en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005) et des formations suivies auprès de la CNIL, nous réaliseront un état des lieux (audit) de votre installation en vue de son amélioration, d'une analyse d'impact ou de sa mise en conformité ;

MISE EN CONFORMITÉ CNIL/RGPD : Nous mettons à niveau une personne de votre établissement qui deviendra référent CNIL et nous l'assistons dans vos démarches de mise en conformité avec le RGPD (Règlement Européen relatif à la Protection des Données à caractère personnel).

Besoin d'un Expert ? contactez-vous

NOS FORMATIONS

: <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>
(Numéro formateur n°93 84 03041 84 (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle))



Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DRTEF n°93 84 03041 84)
- 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

Source : *Votre historique de recherche reste toujours accessible... même effacé*