Les États… unis contre la cybercriminalité

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.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

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 cyberdélits 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 le 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.

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 : Cybersécurité : un Français sur cinq victime de hackers en 2016

Une backdoor chinoise planquée dans des smartphones Android

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 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

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.

Le Net Expert
INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Interrogation des entreprises sur le Règlement européen sur la protection des données

Interrogation des entreprises sur le règlement européen sur la protection des données

Les entreprises veulent obtenir de la CNIL et du G29 des clarifications sur la responsabilité du délégué à la protection des données (DPO).

La Commission nationale de l'informatique et des libertés (CNIL) a rendu publique lundi la synthèse de contributions proposées lors d'une consultation sur le Règlement européen sur la protection des données (RGPD ou GDPR, en anglais). Rappelons que ce Règlement, qui entrera en vigueur en mai 2018, introduit de nouveaux droits des personnes et des obligations nouvelles pour les entreprises. Le texte renforce également les sanctions administratives à l'encontre des responsables de traitement et des sous-traitants qui ne respecteraient pas les dispositions du texte. Les entreprises et les administrations actives dans l'Union européenne sont toutes concernées, et pas seulement celles qui ont adopté le Cloud. Les professionnels ont été consultés cet été par la CNIL.

225 contributeurs, entreprises et fédérations professionnelles, ont posté plus de 540 contributions, soumises à 994 votes. Quatre premiers thèmes inscrits au plan d'action du G29, le groupe des CNIL européennes, ont été abordés. La mission de délégué à la protection des données inquiète le plus.

CIL, de futurs DPO ?

Un délégué à la protection des données (DPO) est-il responsable pénalement ? Peut-il être licencié pour faute ? Pourra-t-il exercer une autre fonction ? Les interrogations des entreprises sont nombreuses. Elles attendent des clarifications sur la responsabilité, le rôle, les moyens et les missions de ce DPO, qui n'est pas sans rappeler le CIL (correspondant informatique et libertés).

Pour répondre à ces attentes, la CNIL se dit prête à réaliser *« des actions de communication auprès des organismes ayant actuellement un CIL, et auprès des fédérations professionnelles concernées par la désignation obligatoire d'un DPO (courriers spécifiques, fiches pratiques) »*. Par ailleurs, les ateliers CIL seront enrichis (format, volume et contenus), a fait savoir le régulateur français.

Selon les prévisions de l'IAPP (International Association of Privacy Professionals), 75 000 postes de DPO seront à pourvoir dans le monde, dont au moins 28 000 en Europe et aux États-Unis. Le but : répondre présent dès le lancement du Règlement européen sur la protection des données.

Portabilité mal perçue

Le droit à la portabilité permet à une personne de récupérer des données à caractère personnel, sous une forme aisément réutilisable, et, si elle le souhaite, de les transférer à un tiers. Les entreprises y voient l'occasion de *« redonner confiance au client dans l'exploitation qu'elles font de ses données »*. Mais elles s'interrogent aussi beaucoup sur le coût et le périmètre réel de ce nouveau droit, qu'elles souhaitent *« limiter au strict minimum »*, selon la CNIL.

Le groupe technologie du G29, de son côté, planche sur un avis visant à clarifier ce périmètre, *« en fonction duquel les actions à mettre en oeuvre pourront être définies »*. À préciser, par conséquent.

Certification et labellisation

Le Règlement européen encourage aussi la mise en place de mécanismes de certification et de labels de protection des données. La délivrance de ces labels pourra être réalisée par le régulateur ou des organismes de certification accrédités. Les entreprises y sont plutôt favorables, à la condition que le cadre européen garantisse *« un niveau élevé et homogène des normes utilisées »*. Et les PME ne veulent pas de processus coûteux et complexes de certification ou labellisation. Les attentes des CIL, organismes et fédérations professionnelles sont fortes dans ce domaine. La CNIL, en plus d'actions déjà menées à leur attention, leur proposera de nouveaux supports et outils didactiques…[lire la suite]

Original de l'article mis en page : Règlement européen sur la protection des données : les entreprises s'interrogent

Des téléphones Android espions ?

Des téléphones Android espions ?

Vous être l'heureux propriétaire d'un smartphone tournant sous Android acheté pas trop cher ? Vos SMS, vos contacts, la liste de vos appels téléphoniques ou encore vos données de déplacement sont peut-être en train d'être analysés à Pékin.…[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.

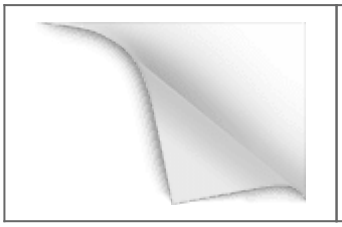
- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation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

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Intel Security promeut l'union face au cybercrime



Intel Security promeut l'union face au cybercrime

Intel Security a présenté de nombreux nouveaux produits dans toutes ses gammes. « Il y a trois fois plus d'innovations à cette conférence que dans les trois précédentes éditions réunies », constate Fabien Rech, directeur général France.…[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.

Le Net Expert
INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

BlackNurse : un déni de

service à bas volume ciblant les firewalls

BlackNurse : un déni de service à bas volume ciblant les firewalls

C’est une attaque au parfum franchement vintage mais à l’efficacité redoutable.…[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.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Contrôles biométriques en entreprise : vos obligations changent !

Contrôles biométriques en entreprise : vos obligations changent !

Le cadre légal régissant la mise en place de dispositifs biométriques en entreprise évolue. En effet, la Cnil a adopté le 30 juin 2016, suite aux exigences fixées par le règlement européen sur la protection des données personnelles (2), 2 autorisations uniques, publiées au journal officiel le 27 septembre 2016.

Ces autorisations uniques fixent un nouveau cadre légal afin d'encadrer le recours aux dispositifs biométriques et protéger au mieux les libertés individuelles des personnes concernées par de tels systèmes d'identification.
Ainsi, les entreprises ayant recours à la mise en place de dispositifs biométriques ne seront plus soumises à une autorisation préalable de la Cnil. Elles devront simplement réaliser une demande d'autorisation unique et se conformer aux obligations prévues par l'autorisation.

La Cnil distingue désormais 2 types de dispositifs :
1/ l'autorisation unique 052 (3) pour les dispositifs garantissant la maîtrise par la personne concernée sur son gabarit biométrique. Ce peut être soit :
– un système recourant au stockage des données biométriques sur un support individuel détenu par les personnes concernées ;
– si la détention d'un support dédié au seul stockage du gabarit n'est pas adaptée à l'architecture et au contexte d'exploitation du dispositif, le responsable du traitement peut, de manière alternative, assurer le verrouillage des données biométriques stockées en base, par un secret détenu uniquement par la personne concernée ;
Dans ces deux hypothèses, l'utilisation du gabarit biométrique est conditionnée à une action de la personne concernée en tant que détentrice du gabarit ou du secret permettant de le déverrouiller.

2/ l'autorisation unique 053 (4) pour les dispositifs reposant sur une conservation des gabarits en base par le responsable du traitement.
Un « gabarit » biométrique désigne les mesures qui sont mémorisées lors de l'enregistrement des caractéristiques morphologiques, biologiques ou comportementales de la personne concernée.

Ainsi, à chaque demande d'autorisation unique visant à mettre en place un dispositif biométrique dans leur entreprise, les dirigeants doivent se conformer à certaines exigences :
• justifier de la nécessité et de la pertinence d'avoir recours à un dispositif biométrique. Le recours à ce dernier ne doit pas avoir pour effet de se substituer à des dispositifs non biométriques ;
privilégier les dispositifs biométriques qui garantissent aux personnes concernées la maîtrise de leur gabarit ;
justifier et garantir la protection et la conservation des gabarits en base ;
• prendre toute mesure permettant de limiter les risques d'atteinte à la vie privée.
Si vous avez mis en place un dispositif biométrique sous couvert de l'ancien cadre légal, vous devez vérifier s'il répond à ces nouvelles exigences :
si c'est le cas : un engagement de conformité à l'une de ces nouvelles autorisations peut être réalisé ;
si ce n'est pas le cas : vous avez 2 ans pour vous mettre en conformité.

2ans pour être en conformité
Si vous ne vous êtes pas mis en conformité d'ici la fin de ce délai, sachez néanmoins que la Cnil pourra à tout moment contrôler que le dispositif de biométrie mis en place dans votre entreprise répond aux obligations imposées par les nouvelles autorisations uniques.

Références :
(1) Article 25 de la Loi n°78-17 du 6 janvier 1978 modifiée, modifié par la Loi n°2016-1321 du 7 octobre 2016 pour une République numérique
(2) Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (Texte présentant de l'intérêt pour l'EEE)
(3) Délibération n°2016-186 du 30 juin 2016 portant autorisation unique de mise en œuvre de dispositifs ayant pour finalité le contrôle d'accès par authentification biométrique aux locaux, aux appareils et aux applications informatiques sur les lieux de travail et garantissant la maîtrise par la personne concernée sur son gabarit biométrique (AU-052)
(4) Délibération n°2016-187 du 30 juin 2016 portant autorisation unique de mise en œuvre de dispositifs ayant pour finalité le contrôle d'accès par authentification biométrique aux locaux, aux appareils et aux applications informatiques sur les lieux de travail, reposant sur une conservation des gabarits en base par le responsable du traitement (AU-053)…[Article source et complet]

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 le 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.

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 : Contrôles biométriques en entreprise : vos obligations changent !

Comment pirater des codes PIN en sniffant le WiFi des smartphones ?

Comment pirater des codes PIN en sniffant le WiFi des smartphones ?

Des chercheurs peuvent récupérer des données sensibles en se basant sur les perturbations du signal WiFi lors des frappes sur l'écran.

Quand un utilisateur déplace ses doigts sur l'écran tactile de son téléphone, il perturbe le signal WiFi émis par son terminal. Ces interruptions peuvent être interceptées par un pirate, analysées et en appliquant de la rétro-ingénierie deviner quelle sont les frappes saisies sur le téléphone ou dans les champs de saisie de mot de passe.
Ce type d'attaque est nommé WindTalker (messager du vent), par des chercheurs chinois et elle n'est possible que si le pirate contrôle le point d'accès WiFi (un hotspot par exemple dans un rayon de 1,5 mètre) afin de collecter les perturbations du signal WiFi. Un contrôle impératif pour analyser le trafic et savoir quand l'utilisateur accède à des pages nécessitant une authentification.

Le CSI en ligne de mire

Si l'attaque semble issue du domaine de la science-fiction, cette menace se sert du CSI (Channel State Information), un composant du protocole WiFi chargé de fournir les informations générales sur l'état du signal WiFi. Quand l'utilisateur tape du texte sur l'écran, sa main modifie les propriétés de CSI du signal WiFi sortant et la modification peut être captée par un point d'accès malveillant.
Dans une démonstration exposée lors de la ACM Conference on Computer and Communications Security à Vienne, les chercheurs ont montré qu'en réalisant une analyse et un traitement basique du signal, un pirate peut avoir accès aux signaux CSI perturbés et deviner avec une précision moyenne de 68,3% les caractères qu'un utilisateur a tapé. La précision de WindTalker est différente selon les modèles de smartphones et elle peut être améliorée avec le niveau de données collectées…[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 le 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.

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 : WindTalker : pirater des

codes PIN en sniffant le WiFi des smartphones