Denis JACOPINI spécialiste RGPD vous donne son avis sur les applis qui pillent vos données personnelles sans vous le dire en abusant de votre consentement

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer					
	Denis JACOPINI spécialiste RGPD vous donne son avis sur les applis qui pillent vos données personnelles sans vous le dire en abusant de votre consentement				

Ces applis qui pillent vos données personnelles sans vous le dire en abusant de votre consentementExpedia, Hollister, Air Canada… sont autant d'applications disponibles sur iPhone et qui enregistreraient l'activité des utilisateurs sans leur permission. Ces données sont renvoyés aux développeurs pour « améliorer leurs services ».

Atlantico : Clics, données de saisie, changement de pages. Ces données ne seraient pas suffisamment masquées selon une enquête de TechCrunch. Elles permettraient de reproduire l'activité des utilisateurs. Concrètement quel est l'intérêt pour les entreprises outre l'optimisation des services ?

Denis Jacopini : On ne veut pas forcément imaginer qu'elles font ça pour revendre nos données puisque la plupart confirment le contraire. Par contre, une chose certaine, c'est que l'exploitation de ces données par leurs services permet d'en savoir plus sur nos comportements et là nous pouvons devenir des cibles qualifiés pour des partenaires qui ne vont pas forcément disposer de données personnelles (mails, contacts,..) mais par contre ils auront nos choix et il suffira qu'ils entrent en contact avec un partenaire intéressé par certains profils pour qu'ils puissent directement vous contacter pour le compte de ces partenaires.…[lire la suite]

Réagissez à cet article

Quelques articles sélectionnés par notre Expert qui pourraient aussi vous intéresser :

Les 10 conseils pour ne pas se faire «hacker» pendant l'été
Les meilleurs conseils pour choisir vos mots de passe
Victime d'un piratage informatique, quelles sont les bonnes pratiques ?
Victime d'usurpation d'identité sur facebook, tweeter ? Portez plainte mais d'après quel article de loi ?
Attaques informatiques : comment les repérer ?

Quel est notre métier ?

Former et accompagner les organismes à **se mettre en conformité avec la réglementation numérique (dont le RGPD)** et à **se protéger des pirates informatiques**.

Quel sont nos principales activités ?

- **RGPD**
  - FORMATION AU RGPD
  - FORMATION DE DPO
  - AUDITS RGPD
  - MISE EN CONFORMITÉ RGPD
  - ANALYSES DE RISQUES (PIA / DPIA)

- **CYBERCRIMINALITÉ**
  - FORMATIONS / SENSIBILISATION D'UTILISATEURS
  - RECHERCHE DE PREUVES

- **EXPERTISES**
  - EXPERTISES PRIVÉES
  - EXPERTISES DE VOTES ÉLECTRONIQUES
  - EXPERTISES JUDICIAIRES
  - RECHERCHE DE PREUVES

- RÉCUPÉRATION DE DONNÉES PERDUES (SMS, Photos, Contacts...)

Notre Expert, Denis JACOPINI, est Expert en Informatique assermenté, spécialisé en **Cybercriminalité**, **Recherche de preuves** et en **Protection des données personnelles**. Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), en Droit de l'Expertise Judiciaire et certifié en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005), Denis JACOPINI est aussi formateur inscrit auprès de la DDRTEFP (Numéro formateur n°93 84 03041 84).

« *Mon métier consiste à mettre à votre disposition l'expérience que j'ai acquise pendant des dizaines d'années et les connaissances que je maintiens continuellement à jour par des formations, certification et diplômes permanentes car le savoir c'est comme une mise en conformité, c'est une démarche quotidienne qui permet une amélioration sur le long terme.*
Denis JACOPINI »

Besoin d'un Expert ? contactez-nous

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en RGPD (Protection des Données à Caractère Personnel).

- Mises en conformité RGPD ;
- Accompagnement à la mise en place de DPO ;
- Formations (et sensibilisations) à la cybercriminalité (Autorisation n°93 84 03041 84) ;
- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires ;
- Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle... ;
- Expertises de systèmes de vote électronique ;

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

Contactez-nous

Source : *Ces applis qui pillent vos données personnelles sans vous le dire en abusant de votre consentement | Atlantico.fr*

Comment peut-on savoir si

vous êtes chez vous et dans quelle pièce grâce au Wifi ?

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer					
	Comment peut-on savoir si vous êtes chez vous et dans quelle pièce grâce au Wifi ?				

La présence de personnes dans un logement perturbe la propagation des ondes émises par les routeurs Wi-Fi, suffisamment en tous les cas pour savoir si quelqu'un est présent ou non.

Nous avons tous des routeurs Wi-Fi à la maison, ils sont si pratiques pour accéder à Internet. Mais les ondes radio émises par ces appareils trahissent également, de façon involontaire, notre présence dans le foyer.

Des chercheurs des universités de Santa Barbara et Chicago viennent de montrer qu'il suffit de se munir d'un smartphone et d'un plan des locaux ciblés, puis de se balader un peu autour pour savoir si une personne est présente, et parfois même dans quelle pièce. Et cela avec une précision qui dépasse les 87 %. Pour une espion ou un voleur, c'est une information plutôt intéressante….[lire la suite]

Réagissez à cet article

Quelques articles sélectionnés par notre Expert qui pourraient aussi vous intéresser :

Les 10 conseils pour ne pas se faire «hacker» pendant l'été
Les meilleurs conseils pour choisir vos mots de passe
Victime d'un piratage informatique, quelles sont les bonnes pratiques ?
Victime d'usurpation d'identité sur facebook, tweeter ? Portez plainte mais d'après quel article de loi ?
Attaques informatiques : comment les repérer ?

Quel est notre métier ?

Former et accompagner les organismes à **se mettre en conformité avec la réglementation numérique (dont le RGPD)** et à **se protéger des pirates informatiques**.

Quel sont nos principales activités ?

- **RGPD**
  - FORMATION AU RGPD
  - FORMATION DE DPO
  - AUDITS RGPD
  - MISE EN CONFORMITÉ RGPD
  - ANALYSES DE RISQUES (PIA / DPIA)

- **CYBERCRIMINALITÉ**
  - FORMATIONS / SENSIBILISATION D'UTILISATEURS
  - RECHERCHE DE PREUVES

- **EXPERTISES**

- EXPERTISES PRIVÉES
- EXPERTISES DE VOTES ÉLECTRONIQUES
- EXPERTISES JUDICIAIRES
- RECHERCHE DE PREUVES
- RÉCUPÉRATION DE DONNÉES PERDUES (SMS, Photos, Contacts...)

Notre Expert, Denis JACOPINI, est Expert en Informatique assermenté, spécialisé en **Cybercriminalité**, **Recherche de preuves** et en **Protection des données personnelles**. Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), en Droit de l'Expertise Judiciaire et certifié en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005), Denis JACOPINI est aussi formateur inscrit auprès de la DDRTEFP (Numéro formateur n°93 84 03041 84).

« *Mon métier consiste à mettre à votre disposition l'expérience que j'ai acquise pendant des dizaines d'années et les connaissances que je maintiens continuellement à jour par des formations, certification et diplômes permanentes car le savoir c'est comme une mise en conformité, c'est une démarche quotidienne qui permet une amélioration sur le long terme.*

Denis JACOPINI »

Besoin d'un Expert ? contactez-nous

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en RGPD (Protection des Données à Caractère Personnel).

- Mises en conformité RGPD ;
- Accompagnement à la mise en place de DPO ;
- Formations (et sensibilisations) à la cybercriminalité (Autorisation n°93 84 03041 84) ;
- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires ;
- Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle... ;
- Expertises de systèmes de vote électronique ;

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

Contactez-nous

Source : *Votre réseau Wi-Fi peut vous trahir et indiquer si vous êtes chez vous et dans quelle pièce*

Prédictions cybersécurité 2018

En 2018, les cybercriminels vont continuer à exploiter les faiblesses inhérentes à la nature humaine pour dérober des informations personnelles, avec des changements significatifs dans les techniques de cyberattaques. Découvrez les grandes lignes de ces tendances qui rythmeront l'année 2018 selon Proofpoint.

L'email restera le vecteur de cyberattaque le plus utilisé

Vol de cryptomonnaie : de nouvelles menaces aussi répandues que les chevaux de Troie

Le facteur humain, toujours au cœur des cyberattaques

La menace grandissante des bots sur les réseaux sociaux

[cliquez pour plus de détails]

LE NET EXPERT

• **ACCOMPAGNEMENT RGPD (ÉTAT DES LIEUX ⇒ MISE EN CONFORMITÉ)**

- **ANALYSE DE VOTRE ACTIVITÉ**
- **CARTOGRAPHIE DE VOS TRAITEMENTS DE DONNÉES**
- **IDENTIFICATION DES RISQUES**
- **ANALYSE DE RISQUE (PIA / DPIA)**
- **MISE EN CONFORMITÉ RGPD** de vos traitements
- **SUIVI** de l'évolution de vos traitements

• **FORMATIONS / SENSIBILISATION** :

- **CYBERCRIMINALITÉ**
- **PROTECTION DES DONNÉES PERSONNELLES**
- AU **RGPD**
- À LA **FONCTION DE DPO**

• **RECHERCHE DE PREUVES** (outils Gendarmerie/Police)

- ORDINATEURS (**Photos / E-mails / Fichiers**)
- TÉLÉPHONES (récupération de **Photos / SMS**)
- SYSTÈMES NUMÉRIQUES

• **EXPERTISES** & **AUDITS** (certifié ISO 27005)

- TECHNIQUES | JUDICIAIRES | ADMINISTRATIVES
- **SÉCURITÉ** INFORMATIQUE
- SYSTÈMES DE **VOTES ÉLECTRONIQUES**

Besoin d'un Expert ? contactez-nous

Notre Expert, Denis JACOPINI, est assermenté, spécialisé en **Cybercriminalité**, **Recherche de preuves** et en **Protection des données personnelles**. Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), en Droit de l'Expertise Judiciaire et certifié en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005), Denis JACOPINI est aussi formateur inscrit auprès de la DDRTEFP (Numéro formateur n°93 84 03041 84).

Réagissez à cet article

Source : *Prédictions cybersécurité 2018 – Global Security Mag Online*

Les États-Unis font voler en éclat les règles protégeant la vie privée sur Internet

Les États-Unis font voler en éclat les règles protégeant la vie privée sur Internet

De la mobilisation des lobbys à la signature du président, The Washington Post démonte le processus qui a conduit à la suppression d'une réglementation adoptée sous l'ère Obama, qui encadrait la vente de données personnelles par les fournisseurs d'accès à Internet.

Fin mars, les Américains ont eu la mauvaise surprise de voir leur Congrès voter l'abolition de nouvelles règles destinées à protéger leur vie privée sur Internet. Adoptées sous l'administration Obama, ces règles empêchaient les fournisseurs d'accès américains tels que Comcast ou AT & T de stocker et de vendre les données de leurs clients, issues de leur historique de navigation, sans leur consentement. Elles n'auront pas eu le temps d'entrer en vigueur…[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Réagissez à cet article

Source : *États-Unis. Comment les républicains ont démantelé*

des règles protégeant la vie privée sur Internet | Courrier international

---

Que sait de nous Google grâce à nos comportements sur Internet ?

	Que sait de nous Google grâce à nos comportements sur Internet ?

Mondialement connue, la firme américaine Google est utilisée par de nombreux internautes, pour son moteur de recherche, mais aussi pour ses nombreux services gratuits (Gmail, Drive, Youtube, Google Maps…). Seul petit hic ? Le revers de la médaille. Puisque Google exploite vos données sans que vous n'en ayez toujours conscience.

Tout le monde connaît Google pour son moteur de recherche ultra-performant. C'est d'ailleurs le moteur préféré des Français. Fin 2016, selon Netbooster, plus de 94 % d'entre eux l'ont utilisé pour effectuer leurs recherches en ligne. Pour apprécier la démesure de ce chiffre, il suffit de voir la part restante à ses principaux concurrents : moins de 4 % pour Bing (Microsoft) et à peine plus de 2 % pour Yahoo.

Plus de 200 services gratuits…

À travers sa maison mère « **Alphabet** », Google est l'une des premières capitalisations mondiales avec une valeur de 588 milliards de dollars, juste derrière Apple. La firme de Moutain View n'est pas la seule à analyser les données qui lui parviennent. Tous les géants du secteur (Apple, Amazon, Facebook…) le font en s'appuyant sur les traces que nous laissons chaque jour sur Internet. Ils engrangent des milliards de dollars grâce à ces informations personnelles.

Inutile donc d'être un financier avisé pour comprendre que la seule activité de moteur de recherche ne suffit pas à générer de telles entrées d'argent. Google est une pieuvre géante, dont les tentacules s'étendent dans des domaines aussi nombreux que variés. Le système d'exploitation Android, le navigateur Internet Chrome, les vidéos YouTube, la plateforme de téléchargement Google Play, la cartographie Google Maps, la suite bureautique Google Documents, le site de partage de photos Picasa…

Ce sont plus de 200 services proposés gratuitement par l'entreprise. Pour la plupart d'entre eux, la seule contrepartie demandée est l'ouverture d'un compte Gmail, le service de messagerie en ligne maison. L'adresse email et le mot de passe associé deviennent alors vos sésames pour vous identifier et entrer dans la sphère Google, depuis n'importe quel terminal à travers le monde.

… en échange de vos données personnelles

Toute cette gratuité a cependant une face cachée : l'exploitation commerciale de nos données personnelles. En effet, elles représentent une manne financière des plus importante. En acceptant les « **conditions générales d'utilisation** », que nous ne lisons quasiment jamais, nous donnons le droit à Google de tracer et d'utiliser tout ce que nous faisons sur Internet : les sites visités, les achats effectués, les lieux dans lesquels nous nous rendons, les films regardés, les livres lus, la musique écoutée…

L'ensemble de ces données est alors analysé par les puissants ordinateurs de la firme, dans le but créer une sorte de carte d'identité très précise de chaque utilisateur. Ces profils, compilant de très nombreuses données, se revendent à prix d'or aux marques désireuses de cibler au mieux leur publicité. C'est ce que l'on appelle le « **Big Data** ».

Pour profiter gratuitement des services de Google, comme ceux de nombreux autres acteurs des nouvelles technologies, nous devons donc rogner sur notre vie privée, en abandonnant la confidentialité de nos données personnelles. Il existe une formule qui résume parfaitement cette pratique : « **si c'est gratuit, c'est que le produit c'est vous !** »…[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

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

---

Réagissez à cet article

Source : *Données personnelles. Voici ce que Google sait de vous*

Voyagez aux Etats-Unis et laissez vos données être espionnées

Voyagez aux Etats-Unis et laissez vos données être espionnées

L'administration Trump envisage de demander aux voyageurs arrivant aux Etats-Unis l'accès aux données de leur smartphone et à leurs comptes Twitter, Facebook ou LinkedIn. Une sévère menace pour la cybersécurité des entreprises européennes.

Cette fois-ci, la côte d'alerte est clairement franchie. Dans ses colonnes, le *Wall Street Journal* évoque un projet de l'administration Trump qui pourrait forcer les visiteurs arrivant aux Etats-Unis à communiquer aux autorités les contacts et contenus présents sur leur téléphone mobile ainsi que les mots de passe de leurs comptes de réseaux sociaux, permettant d'accéder aux messages privés envoyés sur ces canaux. Un projet qui ne serait pas limité aux pays soumis aux règles de sécurité les plus strictes – et dont les ressortissants doivent obtenir un visa -, mais concernerait aussi les pays considérés comme des alliés des États-Unis, dont la France.
Rappelons que, pour se rendre de façon temporaire sur le sol américain, pour affaires ou en tant que touriste, les Français doivent déjà solliciter une autorisation électronique (Esta), valable 2 ans. En février, le ministre de l'Intérieur américain (Homeland Security) avait déjà évoqué, lors d'une audition devant le Sénat, le fait que les voyageurs étrangers (notamment issus des 6 pays blacklistés par un décret de l'administration Trump) venant aux États-Unis seraient tenus de fournir leurs mots de passe sur les médias sociaux aux autorités d'immigration avant de rentrer sur le territoire américain.

La peur de l'espionnage économique

Selon le *Wall Street Journal,* cette mesure serait donc étendue à d'autres pays et aussi aux contacts téléphoniques. « *S'il existe un doute sur les intentions d'une personne venant aux États-Unis, elle devrait avoir à prouver la légitimité de ses motivations, vraiment et véritablement jusqu'à ce que cela nous satisfasse* », a expliqué le conseiller principal du Homeland Security, Gene Hamilton, cité par le quotidien économique.
Si la question ne manquera pas de soulever de vifs débats sur le sol américain et entre les États-Unis et ses partenaires et si une procédure de la sorte pose également quelques questions pratiques assez épineuses, la perspective risque d'échauder de nombreuses entreprises européennes. Car, les activités des services de renseignement US associent sans vergogne antiterrorisme et espionnage économique au profit des entreprises américaines. Une porosité d'ailleurs assumée, comme l'ont montré de nombreux documents dévoilés par Edward Snowden ou *Wikileaks* et révélant les activités de la NSA en matière d'espionnage économique. Les activités de cette nature ne sont d'ailleurs pas limitées à la seule agence de Fort Meade, mais s'étendent à toute la communauté du renseignement aux Etats-Unis.
Au passage, les mesures envisagées par l'administration Trump signeraient probablement l'arrêt de mort du Privacy Shield, l'accord transatlantique sur les transferts de données qui succède au Safe Harbor. Pour mémoire, ce dernier érige comme credo le fait que les données des citoyens européens exportées aux Etats-Unis bénéficient de la même protection que celle que leur accorde le droit européen. En février, les CNIL européennes s'étaient déjà inquiétées des conséquences possibles du décret sur l'immigration du Président Trump sur cet accord…[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement..
(Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Réagissez à cet article

Source : *L’entrée aux Etats-Unis conditionnée par les données des smartphones ?*

Un logiciel malveillant russe découvert dans un ordinateur américain

Au lendemain de la passe d'armes diplomatique entre les Etats-Unis et la Russie, une entreprise américaine a fait savoir qu'un logiciel malveillant avait été découvert dans un de ses ordinateurs. Les autorités ont été alertées.
Nouvel élément dans la « guerre » que se mènent les Etats-Unis et la Russie ces derniers jours. Un programme malveillant associé à l'opération de piratage informatique russe, surnommée Grizzly Steppe par l'administration Obama, a été détecté dans un ordinateur portable lié à une compagnie d'électricité de l'Etat du Vermont. Celui-ci n'était cependant pas connecté au réseau électrique, a fait savoir l'entreprise Burlington Electric Department (BED).

« Nous avons pris aussitôt des mesures pour isoler l'ordinateur portable et avons alerté les autorités fédérales au sujet de la découverte », a dit l'entreprise BED, compagnie qui distribue l'électricité à Burlington dans le Vermont. « Notre équipe coopère avec les autorités fédérales pour remonter la piste de ce programme malveillant et empêcher toute autre tentative visant à s'introduire dans les ordinateurs du réseau électrique. Nous avons informé les autorités de l'Etat et coopérerons pleinement à l'enquête », a-t-elle ajouté.

Un seul cas connu

Le département américain de la Sécurité intérieure avait informé les compagnies d'électricité, jeudi 29 décembre, de l'existence du programme malveillant utilisé dans Grizzly Steppe. « Nous avons rapidement passé au crible l'ensemble des ordinateurs de notre système. Nous avons détecté le programme malveillant dans un seul ordinateur portable de Burlington Electric Department, non relié à la grille électrique de notre société », a indiqué la BED…[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Réagissez à cet article

Original de l'article mis en page : Cyberattaque : un logiciel malveillant russe découvert dans un ordinateur américain – LCI

Quelles tendances en 2017 pour la sécurité du Cloud ?

Quelles tendances en 2017 pour la sécurité du Cloud ?

Comme chaque année, le grand jeu des prédictions des nouvelles tendances bat son plein. J'ai donc pris le parti de vous proposer quelques réflexions portant sur le marché du Cloud et celui de la sécurité en m'appuyant sur les dernières évolutions que j'ai pu constater.

Les menaces inhérentes à l'IoT obligeront les nations à s'engager dans la lutte internationale contre le piratage

Après les incidents qui ont frappé des infrastructures critiques en France, aux Etats-Unis et en Ukraine cette année, et face aux risques de piratage des machines de vote électroniques, les administrations de nombreux pays ont décidé de prendre le problème du cyberespionnage à bras-le-corps. Si les États-Unis ont réussi, par le biais de négociations diplomatiques à huis clos, à faire baisser le nombre d'attaques informatiques de la Chine à l'encontre des entreprises du secteur privé, le piratage des objets connectés représente un enjeu d'une tout autre ampleur. Sur le plan de la défense, l'Union européenne a adopté des dispositions législatives appelant à un minimum de mesures de cybersécurité pour protéger les infrastructures névralgiques, et les États-Unis devraient lui emboîter le pas en 2017.

Des réglementations strictes influent sur la politique de cybersécurité des entreprises.

Les lois sur la protection de la vie privée des consommateurs sont censées avoir un effet dissuasif et sanctionner les négligences sécuritaires entrainant une violation de données. Or, jusqu'à présent, les organismes de réglementation semblent s'être bornés à de simples réprimandes. Sous l'impulsion de l'Europe et du nouveau règlement général sur la protection des données (GDPR), les autorités chargées de la protection des données redoublent de vigilance et revoient le montant des amendes à la hausse. L'importance des sanctions financières infligées fin 2016 pour violation de la réglementation HIPAA et des directives de l'UE relatives aux données à caractère personnel donnent le ton pour l'année à venir. Nul doute que l'entrée en vigueur du GDPR en 2018 incitera les entreprises internationales à instaurer des contrôles supplémentaires pour la protection de la confidentialité.

Les compromissions de données touchant des fournisseurs de services Cloud sensibilisent les entreprises aux risques de la « toile logistique ».Le Cloud a transformé la chaîne logistique traditionnelle en « toile logistique » où les partenaires commerciaux échangent des données via des passerelles numériques sur Internet. Une entreprise moyenne traite avec 1 555 partenaires commerciaux différents via des services Cloud, et 9,3 % des fichiers hébergés dans le Cloud et partagés avec l'extérieur contiennent des données sensibles. Dans la nouvelle économie du Cloud, les données passent entre les mains d'un nombre d'intervenants plus élevé que jamais. Une violation de données peut ainsi toucher le partenaire externe d'une entreprise dont le département informatique et le service Achats n'ont jamais entendu parler.

Restructuration des directions informatiques avec la promotion des RSSI

Avec l'avènement de la virtualisation, les technologies de l'information occupent une place tellement stratégique au sein de l'entreprise que les DSI endossent désormais le rôle de directeur de l'exploitation et de PDG. En 2017, la sécurité s'imposera en tant que moteur d'activité stratégique, aussi bien au niveau des systèmes internes que des produits. Aujourd'hui, toutes les entreprises utilisent des logiciels, ce qui fait qu'elles ont besoin de l'expertise de fournisseurs de sécurité logicielle. En 2017, la sécurité confirmera son rôle d'atout concurrentiel en aidant les RSSI à réduire les délais de commercialisation des produits, et à assurer la confidentialité des données des clients et des employés.

Microsoft réduira l'écart avec Amazon dans la guerre des offres IaaS

AWS s'est très vite imposé sur le marché de l'IaaS, mais Azure rattrape son retard. 35,8 % des nouvelles applications Cloud publiées au 4e trimestre ont été déployées dans AWS, contre 29,5 % dans Azure. Les fournisseurs spécialisés se sont taillé 14 % de parts de marché, indépendamment de marques telles que Google, Rackspace et Softlayer.

Qui protège les gardiens ? Une entreprise sera victime du premier incident de grande ampleur dans le Cloud lié au piratage d'un compte administrateur

En fin d'année, des chercheurs ont, pour la première fois, découvert la mise en vente de mots de passe d'administrateurs Office 365 globaux sur le Dark Web. Les comptes administrateur représentent un risque particulier dans le sens où ils disposent de privilèges supérieurs en matière de consultation, de modification et de suppression des données. Les entreprises rencontrent en moyenne 3,3 menaces de sécurité liées à des utilisateurs privilégiés tous les mois. Nous devons par conséquent nous attendre à voir un incident de ce type faire la une des journaux en 2017.

Les pirates délaissent les mots de passe au profit de la propriété intellectuelle

Maintenant que les entreprises ont toute confiance dans le Cloud et se servent d'applications SaaS pour les plans de produits, les prévisions de ventes, etc., les cybercriminels disposent de données de plus grande valeur à cibler. 4,4 % des documents exploités dans les applications de partage de fichiers sont de nature confidentielle et concernent des enregistrements financiers, des plans prévisionnels d'activité, du code source, des algorithmes de trading, etc. Si le piratage de bases de données comme celles de Yahoo se distinguent par leur ampleur, les secrets industriels représentent une manne d'informations plus restreinte, mais néanmoins précieuse. Pour répondre aux inquiétudes sur la confidentialité des informations hébergées dans le Cloud, des fournisseurs tels que Box établissent une classification des données permettant d'identifier les ressources qui revêtent le plus de valeur pour les entreprises…[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Réagissez à cet article

Original de l'article mis en page : Sécurité du Cloud : quelles tendances en 2017 ? — Globb Security FR

Sednit : dissection d'un groupe de cyber-espions

Sednit : dissection d'un groupe de cyber-espions

Les chercheurs ESET annoncent la publication d'un vaste document de recherche en 3 parties « En route with Sednit ». L'observation de l'utilisation simultanée d'un bootkit et d'un rootkit par les cybercriminels a permis d'analyser leurs cibles et méthodes.
Ce groupe aussi connu sous le nom d'APT28, Fancy Bear ou Sofacy, agit depuis 2004. Son principal objectif **est le vol d'informations confidentielles de cibles spécifiques :**
• Partie 1 : « En route with Sednit : Approaching the Target » se concentre sur la cible des campagnes de phishing, les méthodes d'attaque utilisées ainsi que la première phase de l'attaque utilisant le malware SEDUPLOADER, composé d'un compte à rebours et d'une charge utile associée.
• Partie 2 : « En route with Sednit : Observing the comings and goings » couvre les activités de Sednit depuis 2014 et détaille la boîte à outils d'espionnage utilisée pour la surveillance à long terme des ordinateurs compromis. Cela est rendu possible grâce à deux backdoor SEDRECO et XAGENT, ainsi qu'à l'outil réseau XTUNNEL.
• Partie 3 : « En route with Sednit : a mysterious downloader » décrit le logiciel permettant la première phase de l'attaque DOWNDHELPH qui selon nos données de télémétrie n'aurait servi que 7 fois. A noter que certains de ces déploiements ont requis des méthodes de « persistances avancées » : Windows bootkit et Windows rootkit.
« L'intérêt d'ESET pour ces activités malveillantes est née de la détection d'un nombre impressionnant de logiciels personnalisés déployés par le groupe Sednit au cours des deux dernières années », déclare Alexis Dorais-Joncas, Security Intelligence team lead chez ESET et dédié à l'exploration des activités du groupe Sednit. « L'arsenal de Sednit est en constante évolution. Le groupe déploie régulièrement des logiciels et techniques de pointe, tandis que leur malware phare a également évolué de manière significative au cours des dernières années ».
Selon les chercheurs ESET, les données collectées à partir des campagnes de phishing menées par Sednit montrent que plus de **1.000 profils d'individus hauts-placés impliqués dans la politique d'Europe de l'EST ont été attaqués.** « Contrairement aux autres groupes d'espionnage, le groupe Sednit a développé son propre « exploit kit » et utilisé un nombre étonnamment important d'exploits 0-day», conclut Alexis Dorais-Joncas.
Les activités du groupe cybercriminel de ces dernières années envers les personnalités hauts-placées, ont suscité l'intérêt de nombreux chercheurs. **Le document réalisé par les experts ESET fournit une description technique accessible et contenant les indicateurs de compromission (IOCs), à destination des chercheurs et des entreprises afin de vérifier qu'ils n'ont pas été compromis par le groupe Sednit**.
La première partie de cette recherche est disponible sur WeLiveSecurity, l'intégralité l'étant sur le Github ESET.

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

---

Réagissez à cet article

Original de l'article mis en page : Boîte de réception (2) –

Collectes massives et illégales par le Renseignement allemand

Collectes massives et illégales par le Renseignement allemand

Après avoir réalisé un contrôle sur place des services de renseignement, la Cnil allemande a dressé un bilan extrêmement critique des activités du Bundesnachrichtendienst (BND) en matière de collecte d'informations sur Internet.

Le site Netzpolitik a dévoilé le contenu d'un rapport jusque là confidentiel produit en juillet 2015 par Andrea Voßhoff, le commissaire à la protection des données en Allemagne, qui accable les services de renseignement allemands. Le rapport a été réalisé après la visite de l'homologue de la Cnil dans la station d'écoutes Bad Aibling, opérée conjointement en Bavière par l'agence allemande du renseignement, la Bundesnachrichtendienst (BND), et par la National Security Agency (NSA) américaine.
Malgré les difficultés à enquêter qu'il dénonce, Voßhoff dénombre dans son rapport 18 violations graves de la législation, et formule 12 réclamations formelles, qui obligent l'administration à répondre. Dans un pays encore meurtri par les souvenirs de la Stasi, le constat est violent.
L'institution reproche au BND d'avoir créé sept bases de données rassemblant des informations personnelles sur des suspects ou simples citoyens lambda, sans aucun mandat législatif pour ce faire, et de les avoir utilisées depuis plusieurs années au mépris total des principes de légalité. Le commissaire a exigé que ces bases de données soient détruites et rendues inutilisables.

Parmi elles figure une base assise sur le programme XKeyScore de la NSA, qui permet de réunir et fouiller l'ensemble des informations collectées sur le Web (visibles ou obtenues par interception du trafic), pour les rendre accessibles aux analystes qui veulent tout savoir d'un individu et de ses activités en ligne. Alors que XKeyScore est censé cibler des suspects, Voßhoff note que le programme collecte « un grand nombre de données personnelles de personnes irréprochables », et cite en exemple un cas qu'il a pu consulter, où « pour une personne ciblée, les données personnelles de quinze personnes irréprochables étaient collectées et stockées », sans aucun besoin pour l'enquête…[lire la suite]

Denis Jacopini anime des **conférences et des formations** 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

---

Réagissez à cet article

Original de l'article mis en page : Le Renseignement allemand pris en flagrant délit de collectes massives illégales – Politique – Numerama