Alerte : Sérieuse faille WiFi. Mettez à jour vos iPhones avec la IOS 10.3.1

Alerte : Sérieuse faille WiFi. Mettez à jour vos iPhones avec la IOS 10.3.1

La mise à jour 10.3.1 du système d'exploitation mobile iOS corrige une vulnérabilité permettant d'exécuter du code à distance sur les puces WiFi de Broadcom dans les iPhone, iPad et iPod. Le fabricant de puces a pu obtenir une grâce d'une dizaine de jours avant divulgation de l'exploit par l'équipe sécurité de Google, Project Zero.

L'iPhone 7 est concerné par la faille WiFi et éligible pour la mise à jour iOS 10.3.1. (crédit : Susie Ochs)

Si vous n'avez pas mis à jour iOS pour vos terminaux mobiles Apple depuis longtemps, voici une bonne occasion de le faire. Apple a en effet lancé la version 10.3.1 de son système d'exploitation pour iPhone, iPad et iPod pour corriger une vulnérabilité permettant à un attaquant d'exécuter du code malveillant distant sur les puces WiFi Broadcom de ces terminaux. Cette vulnérabilité touche la fonction d'authentification dans le protocole 802.11r permettant aux terminaux de se connecter de façon sécurisée entre plusieurs stations de base sans fil d'un même domaine. Les hackers peuvent exploiter cette faille pour exécuter du code au sein même du firmware de la puce WiFi s'ils se trouvent à portée du réseau sans fil des terminaux visés.
Il s'agit là d'une vulnérabilité parmi d'autres trouvées par le chercheur Gal Benjamini de l'équipe de sécurité de Google, Project Zero, dans le firmware des puces Broadcom WiFi. Certaines d'entre elles concernent également les terminaux Android et ont été patchées dans le cadre du bulletin de sécurité Android d'avril. La mise à jour iOS 10.3.1, lancée lundi, est quelque peu inhabituelle car elle vient une semaine à peine après la 10.3 qui apportait pourtant un lot de correctifs touchant différents composants. L'explication pour ce court intervalle entre ces deux mises à jour est à voir du côté du délai pratiqué par Google Project Zero pour dévoiler au public les exploits de failles…[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

---

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.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

Source : *Apple colmate une sérieuse faille WiFi dans iOS – Le Monde Informatique*

Samsung Galaxy S8 ou S8+ : Une première faille de sécurité dénichée

Samsung Galaxy S8 ou S8+ : Une première faille de sécurité dénichée

---

La semaine dernière, le géant Sud-Coréen Samsung dévoilait ses nouveaux Smartphones Galaxy S8 et S8+. Un enjeu important pour le constructeur qui souhaite retrouver une image de marque suite à ses déboires avec les batteries explosives de son Note 7. Mais alors que les nouveaux modèles S8 et S8+ ne sont pas encore commercialisés, une première faille vient d'être décelée, le système de reconnaissance faciale peut être en effet trompé par une simple photo.

Galaxy S8 : Le système de reconnaissance faciale déjoué par une simple photo

Quelques jours seulement après sa présentation officielle, le Samsung Galaxy S8 est déjà sous le feu des critiques. En effet, une vidéo mise en ligne le 29 mars par la chaîne iDeviceHelp montre un utilisateur déverrouiller un **Samsung Galaxy S8** à l'aide d'une simple photo. Le système de **reconnaissance faciale** censé être un procédé sécurisé montre donc déjà sa première faille !

Avec ses deux nouveaux modèles, le constructeur Samsung avait pourtant misé sur la sécurité avec la présence **d'un système de reconnaissance d'iris**, un lecteur d'empreintes digitales situé désormais au dos de l'appareil ainsi que la reconnaissance faciale, une manière rapide et aisée de déverrouiller le Galaxy S8 ou S8+…[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

---

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.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

Source : *Samsung Galaxy S8 ou S8+ : Une première faille de*

sécurité dénichée

Le Bourget : ces drones vont vous faciliter la vie

Le Bourget : ces drones vont vous faciliter la vie

De drôles d'engins vrombissaient ce mardi au Musée de l'Air et de l'Espace du Bourget.…[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 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

Les drones volent au secours des agriculteurs

Les drones volent au secours des agriculteurs

Et si l'avenir de l'agriculture se jouait… dans les airs ? Depuis quelques années, les exploitants agricoles ont effet la possibilité d'analyser leurs parcelles à l'aide d'un drone.…[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 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

Cybersécurité dans le monde : à quoi peut-on s’attendre ?

	**Cybersécurité dans le monde : à quoi peut-on s’attendre ?**

L'année 2016 a démontré que les mesures de sécurité traditionnelles ne suffisaient plus et que de nouvelles stratégies devaient être mises en place. 2017 va donc s'inscrire dans la continuité de ce qui a déjà été amorcé l'année passée, à savoir : toujours plus de sécurité pour toujours une protection maximisée. Les experts de NTT Security ont fait ressortir les tendances et les prévisions pour cette année qui débute.

Selon Garry Sidaway, Vice-Président Senior de la Stratégie de Sécurité

1. L'identité restera au cœur des enjeux

Au risque de nous répéter, les mots de passe fournissent aujourd'hui des garanties insuffisantes. À l'ère du digital et de la mobilité, commodité et sécurité ne font pas bon ménage. Certes, les mots de passe sont bien pratiques, mais ils sont de moins en moins perçus comme une preuve d'identité irréfutable. Devant l'utilisation croissante des smartphones et les exigences de simplicité des consommateurs et des professionnels, les solutions d'identité resteront donc au cœur des préoccupations en 2017. C'est ainsi que le mot de passe traditionnel cèdera du terrain face à la poussée du « multi-facteurs », une méthode combinant plusieurs facteurs d'authentification (localisation, possession d'un objet, d'une information, etc.). Cette association entre physique et digital, avec en toile de fond l'émergence de méthodes d'authentification avancées, favorisera le développement de nouvelles solutions de gestion des identités.

2. Le mobile sera omniprésent

Au royaume du digital, le mobile est roi. Un roi qui bouscule l'ordre établi dans de nombreux domaines, des méthodes de paiement jusqu'aux interactions sociales. Véritables hubs digitaux, nos smartphones constituent désormais non seulement une fenêtre de contrôle et d'interaction avec le monde mais aussi une interface d'identification et d'authentification. Dans un tel contexte, 2017 verra le curseur de la menace se déplacer des ordinateurs portables vers les appareils mobiles. Si, traditionnellement, les acteurs de la sécurité se sont concentrés sur les systèmes back-end et les conteneurs, ils devront revoir leur approche pour placer le mobile au cœur de leur dispositif.

3. Les entreprises surveilleront la menace interne

Le problème des menaces internes ne date pas d'hier. Côté défense, les progrès réalisés dans les domaines de l'analytique et de la détection des anomalies devraient se poursuivre en 2017. Dans un milieu de l'entreprise de plus en plus dynamique, définir les critères d'un comportement utilisateur « normal » restera un défi de taille. Toutefois, avec le développement de nouvelles techniques de machine learning, nous verrons l'analyse comportementale s'opérer directement au niveau des terminaux.

4. Fin de la détection basée sur les signatures

Antivirus nouvelle génération, solutions de sécurité des terminaux, solutions de détection et de réponse aux incidents… Peu importe leur nom, les solutions de protection des terminaux se projetteront bien au-delà de la détection basée sur des signatures statiques, à commencer par les outils d'analyses avancées que l'on retrouvera systématiquement sur ces solutions. Leur force résidera notamment dans leur capacité à exploiter la puissance du cloud pour partager l'information sur les menaces connues. La diversité et le volume sans précédent des malwares engendreront l'émergence d'une nouvelle approche. Destinée à enrayer le syndrome dit du « patient zéro », cette démarche reposera à la fois sur une collaboration internationale et l'utilisation d'une cyberveille prédictive et proactive pour libérer toute la force du collectif.

5. Le tout-en-un fera de plus en plus d'adeptes

Alors que le marché de la cybersécurité se consolide, les entreprises se tournent vers des solutions de sécurité couvrant l'intégralité des environnements TIC. Traditionnellement, la force des prestataires de sécurité managée (MSS) s'est située dans leur capacité à intégrer un maillage d'outils complexes et pointus. Aujourd'hui, la situation a changé. Tout l'enjeu consiste à intégrer le facteur sécurité à tous les échelons du cycle opérationnel de l'entreprise. Les clients chercheront donc un partenaire capable d'agir sur tous les fronts : applications métiers, infrastructure réseau, services cloud et de data center autour d'une console de gestion centralisée. En 2017, les solutions multifournisseurs apparaîtront comme datées. Les acteurs de la sécurité devront ainsi coordonner un service complet de bout en bout pour répondre aux enjeux de l'espace de travail digital.

Selon Stuart Reed, Directeur Senior Product Marketing

6. Les consommateurs exigeront plus de transparence

Une étude récente de NTT Security a mis en lumière les attentes croissantes des cyberconsommateurs en matière de transparence, tant sur le plan des pratiques que de la gestion des incidents. Ces conclusions traduisent notamment une sensibilisation accrue des consommateurs sur les questions de sécurité suite aux scandales de violations à répétition. La tendance est appelée à se poursuivre en 2017 et au-delà. Notons enfin que les entreprises dotées de politiques de sécurité et de plans d'intervention efficaces diminueront leur exposition au risque, tout en profitant d'un puissant levier de compétitivité.

7. L'innovation en moteur de consolidation

Du point de vue de l'offre comme des fournisseurs de cybersécurité, 2016 a été placée sous le signe de la consolidation. Au rang des plus grosses opérations, on citera l'acquisition de BlueCoat par Symantec, la série de rachats par Cisco et, plus proche de nous, la création de NTT Security autour de trois piliers : analytique de pointe, cyberveille avancée et conseils d'experts en sécurité. Derrière ce phénomène de consolidation, on retrouve une constante : l'innovation. Concrètement, les grandes entreprises ont racheté des spécialistes pour accéder à leurs compétences et les englober dans une offre plus aboutie. Ces grands acteurs profitent enfin d'économies d'échelle considérables – et de l'expertise et de l'efficacité qui en découlent – pour mener des programmes d'incubation qui viendront à leur tour stimuler l'innovation. Cette tendance de fond souligne bien l'importance de l'innovation pour évoluer au rythme des besoins de sécurité des clients.

8. L'identité des objets

Avec l'essor de l'IoT, la frontière entre physique et digital s'estompe peu à peu pour créer des expériences clients plus pratiques, rapides et efficaces. Seulement voilà, les cybercriminels ont eux aussi investi la sphère de l'IoT à l'affût de la moindre vulnérabilité. On a ainsi recensé des cyberattaques se servant d'objets connectés (caméras de vidéosurveillance, imprimantes…) pour lancer des attaques DDoS qui sont parvenues à paralyser des sites comme Twitter et Spotify. L'année 2017 verra sans doute une recrudescence des attaques perpétrées à l'encontre des objets connectés. D'où le besoin impérieux d'intégrer ces appareils à une politique de sécurité plus complète, notamment pour mieux contrôler l'identité et la légitimité de leurs utilisateurs.

9. L'analytique changera la donn

L'un des grands défis de la cybersécurité pourrait se résumer par cette question : comment produire une information cohérente à partir d'une avalanche de données issues de dispositifs multiples ? Si l'analyse de données a pour fonction première de « donner du sens », l'évolution des menaces doit nous inciter à revoir nos méthodes d'interprétation et de contextualisation de l'information. Dans cette optique, les outils avancés d'analyse du risque vous permettront de prendre les bonnes décisions. Au-delà des événements présents, ces outils ont pour fonction de décortiquer les données historiques pour faire ressortir des tendances, mais aussi d'utiliser l'intelligence artificielle pour identifier les schémas comportementaux annonciateurs d'une attaque. Fondées sur des technologies avancées de machine learning, des outils d'analyse automatiques et des experts en astreinte permanente, les solutions d'analytique de pointe promettent de changer la donne dans le secteur des MSS.

Selon Kai Grunwitz, Vice-Président Senior Europe Centrale

10. La cybersécurité va s'imposer comme un facteur clé de succès

Pour être reconnue comme tel par tous les acteurs concernés, la cybersécurité doit s'intégrer en amont à l'ensemble des processus métiers de l'entreprise. Dans un monde connecté où le digital gagne chaque jour en importance, les entreprises veulent pouvoir compter sur une sécurité parfaitement incorporée à leurs stratégies métiers et IT. Outre son rôle indispensable de gardienne des données sensibles, du capital intellectuel et des environnements de production, la cybersécurité sera également partie intégrante de l'innovation et de la transformation de l'entreprise.

La sécurité ne sera plus seulement le problème des DSI, mais s'invitera au cœur des processus métiers et constituera l'un des ressorts de la chaîne de valeur. Enfin, la gestion du cycle de sécurité constituera un différenciateur clé autant qu'une priorité essentielle dans le cadre d'une stratégie de sécurité orientée métiers. Elle procurera aux entreprises un avantage concurrentiel et un réel levier de valeur ajoutée.

Selon Chris Knowles, Directeur solutions

11. Le RGPD sera partout !

Si vous pensiez que le Règlement général sur la protection des données (RGPD) a été l'un des grands thèmes de 2016, attendez de voir ce que 2017 vous réserve. Alors que les fournisseurs proclameront les avantages de leurs technologies et que les équipes juridiques plancheront sur la définition d'une sécurité réellement irréprochable, les clients, eux, se lanceront dans les préparatifs.

12. Au royaume des aveugles, les borgnes sont rois… mais plus pour très longtemps !

Pour beaucoup d'entreprises, la sécurité se résume à la protection d'un périmètre au moyen de périphériques inline censés analyser l'intégralité du trafic et intervenir sur la base d'éléments visibles. Toutefois, la mobilité croissante des collaborateurs, associée à l'explosion du nombre d'applications cloud en entreprise, créent des « angles morts ». À commencer par le transit d'informations via des tunnels cryptés, le stockage et le traitement de données à l'extérieur de data centers sécurisés, ou encore les communications entre machines virtuelles qui échappent totalement à la surveillance des dispositifs de sécurité existants. En 2017, les entreprises se pencheront sur ce phénomène afin d'éliminer les angles morts et de reprendre le contrôle de leur sécurité.

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

---

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 DIRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité Contactez-nous

Réagissez à cet article

Source : *Cybersécurité dans le monde : à quoi peut-on s'attendre ?*

Le piratage informatique aussi risqué pour les animaux

Le piratage informatique aussi risqué pour les animaux

Pas évident d'y penser quand on n'est pas du milieu, mais au 21ème siècle, le braconnage se joue de plus en plus sur le terrain du numérique.

Le GPS, pour le meilleur comme pour le pire

Le balisage des animaux est une pratique qui date du début du XX^e siècle. **Après la pose de bagues sur les oiseaux au début du siècle, les scientifiques se sont tournés vers les transmetteurs radio dans les années 1950, avant de passer au système de suivi par satellite Argos dans les années 1970.** Aujourd'hui, c'est un autre système de suivi qu'utilisent les chercheurs : le GPS.

Cigogne équipée d'un GPS© Vasileios Karafillidis Shutterstock

Le GPS, tout le monde l'a dans son smartphone. Il nous facilite beaucoup la vie en nous aidant à nous retrouver dans une ville inconnue, en nous permettant d'appeler un taxi ou encore en nous rassurant lorsque nos enfants, rentrant seuls de l'école, utilisent leur smartphone pour partager avec nous leur localisation.

Mais au-delà de ces usages pratiques, s'en cache un plus obscur. Les balises GPS que les chercheurs placent sur les animaux ne sont pas des smartphones sophistiqués, il est donc assez facile de les pirater pour recevoir de manière indue ces données. Une faille que les braconniers exploitent à volonté, en mettant en danger la vie des animaux.

Lire aussi : la lutte contre le commerce en ligne de faune sauvage est engagée

Le cyber-braconnage, un problème qui ne sera pas résolu du jour au lendemain

Le phénomène est encore trop peu connu et réservé au milieu des chercheurs…[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

---

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 DIRECCTE n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

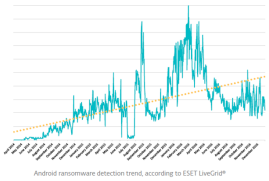
Réagissez à cet article

Source : *Le piratage informatique, un risque pour les animaux*

En 2016, les ransomwares sous Android ont augmenté de plus de 50%

En 2016, les ransomwares sous Android ont augmenté de plus de 50%

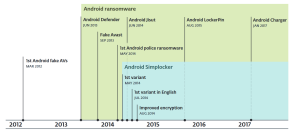
Basé sur sa technologie LiveGrid®, ESET© publie un rapport sur les menaces Android™ : sur l'ensemble des logiciels malveillants détectés en 2016, la catégorie ransomware a augmenté de plus de 50% par rapport à 2015, le plus fort taux de menaces enregistré.



Android ransomware detection trend, according to ESET LiveGrid®

« Au total, nous avons constaté **une augmentation de près de 20% des logiciels malveillants** (tous confondus) **sous Android en un an.** Sur cette plateforme, les ransomwares sont ceux qui se sont le plus développés. Selon le FBI (1), cette menace aurait rapporté jusqu'à 1 milliard de dollars aux cybercriminels l'année dernière. Avec une forte augmentation au cours du premier semestre 2016, nous pensons que cette menace ne disparaîtra pas de sitôt », déclare Juraj MALCHO, Chief Technology Officer chez ESET et qui abordera ce sujet lors du Mobile World Congress 2017.

ANDROID RANSOMWARE CHRONOLOGY



Au cours des 12 derniers mois, **les cybercriminels ont reproduit des techniques identiques à celles utilisées pour la conception de malwares infectant des ordinateurs**, afin de concevoir leurs propres logiciels malveillants sur Android : écran de verrouillage, cyrpto-ransomwares… Ainsi, ils ont réussi à développer des méthodes sophistiquées permettant de cibler uniquement les utilisateurs des différentes versions de cette plateforme.
En plus d'utiliser des techniques d'intimidation comme le « Police ransomware (2) », les cybercriminels chiffrent et cachent la charge utile malveillante sous l'application compromise, afin de rendre sa présence indétectable.
D'après les observations d'ESET, les ransomwares sous Android se concentraient sur l'Europe de l'EST puis sur les Etats-Unis en 2015, avant de migrer vers le continent asiatique en 2016. « Ces résultats montrent la vitesse de propagation de cette menace, active à l'échelle mondiale », ajoute Juraj MALCHO.

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

---

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 DIRECCTE n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

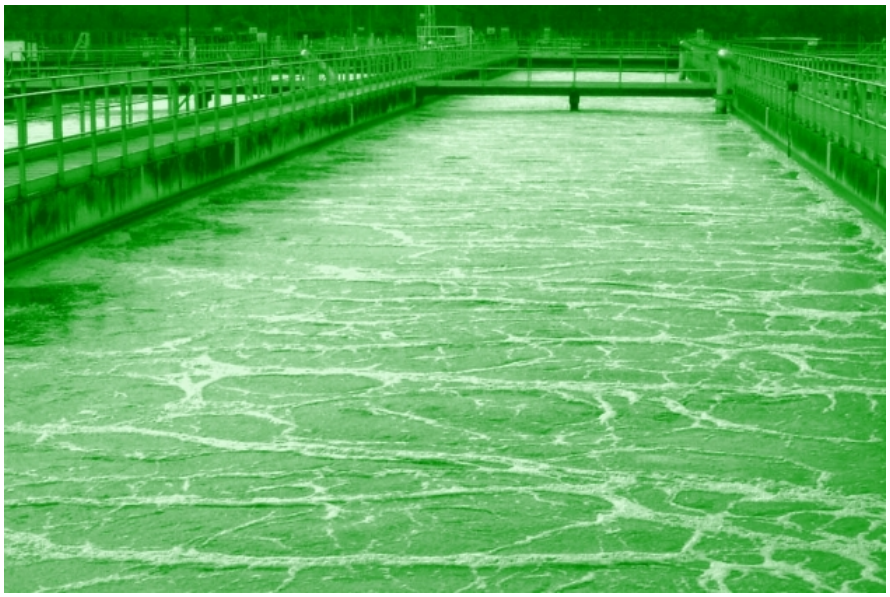
Le Net Expert INFORMATIQUE Cybersécurité & Conformité Contactez-nous

=

Réagissez à cet article

Source : *Boîte de réception (252) – denis.jacopini@gmail.com – Gmail*

Ce malware aurait la capacité d'empoisonner l'eau potable d'une ville entière



Ce malware aurait la capacité d'empoisonner l'eau potable d'une ville entière

Des chercheurs en sécurité ont créé LogicLocker, un logiciel malveillant capable de bloquer une station d'épuration d'eau dans le but d'extorquer des rançons. Ce type d'attaque serait la prochaine étape dans le domaine des ransomwares.

Les ransomwares cryptographiques, qui chiffrent les données des utilisateurs pour extorquer une rançon, vous font peur ? Alors attendez de voir les « ransomwares industriels », qui s'attaquent aux systèmes de contrôle des usines. Ils vous feront basculer en mode panique, car ils pourraient avoir des conséquences directes et néfastes sur notre environnement physique.
Pour l'instant, ce type de malware ne fait pas encore partie de l'arsenal des pirates, mais des chercheurs du Georgia Institute of Technology pensent que ce n'est qu'une question de temps, étant donné la faible sécurité des systèmes industriels. Pour montrer l'étendue de la menace, ils ont développé un prototype d'un tel ransomware et l'ont testé sur une maquette industrielle qui représente une station d'épuration d'eau d'une ville. Ils ont présenté leur travail cette semaine à l'occasion de la conférence RSA 2017, qui s'est tenue à San Francisco.

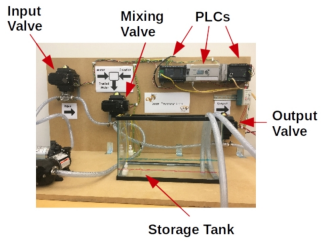


Fig. 2: Water Treatment Testbed

Baptisé LogicLocker, ce malware est capable d'infecter l'automate programmable industriel (programmable logic controller, PLC) qui régule la désinfection et le stockage de l'eau potable. L'attaque consiste à extraire le code exécutable de l'appareil et de le remplacer par un code malveillant, puis de changer le mot de passe d'accès. Ainsi, l'attaquant peut non seulement stopper le processus d'épuration, mais aussi empêcher les ingénieurs de réinstaller le code d'origine sur l'appareil. Le pirate peut alors envoyer aux responsables de la station d'épuration une demande de rançon doublée d'un ultimatum : s'ils ne payent pas au bout d'un certain temps, le code malveillant va surdoser le produit désinfectant et, du coup, rendre toute l'eau potable impropre à la consommation. Une fois la rançon payée, l'attaquant restitue le code volé.

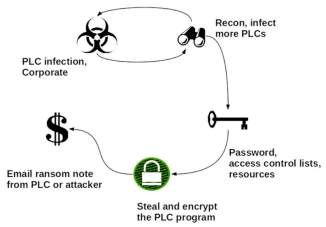


Fig. 3: General Flow of ICS Ransomware Attack

Un tel scénario est faisable dans n'importe quel domaine, à partir du moment où il y a des automates programmables connectées sur un réseau interne ou, carrément, sur Internet. Il suffit de se rendre sur le site Shodan.io pour constater qu'il existe d'ores et déjà des milliers de PLC accessibles par la Toile. Les chercheurs ont en trouvé d'emblée plus de 1400 de marque MicroLogix et 250 de marque Schneider Modicon.

Une question de profitabilité

Si les pirates n'ont pas encore exploité ce type d'attaque, ce n'est pas parce que ces automates sont bien sécurisés. Au contraire, leur manque de protection est notoire et connu depuis des années. *« La seule explication est que les cybercriminels n'ont pas encore trouvé le business model qui leur permet d'opérer de manière profitable dans ce type d'environnement »*, estiment les chercheurs dans leur étude. En effet, le ransomware industriel nécessite plus de recherche et de connaissance. Par ailleurs, son mode opératoire est très pointu et ne peut donc faire qu'un faible nombre de victimes. C'est donc exactement l'inverse des cryptoransomwares, qui sont diffusés en masse auprès d'un large parc d'utilisateurs…[lire la suite]

Source : *Ce malware pourrait empoisonner l'eau potable d'une ville entière*

Vous offrez aux hackers des données invisibles sans le

savoir

Vous offrez aux hackers des données invisibles sans le savoir

Empreintes digitales, données GPS des photos, réponses aux questions prétendues «secrètes»…: des données sensibles se cachent sur ce que vous publiez sur les réseaux sociaux, même si l'essentiel du risque se concentre sur des informations livrées plus directement encore…

Le « V » de la victoire pourrait être celui des hackers. Un chercheur japonais avertissait début janvier contre le danger contenu dans ce signe parfois associé aux selfies: en montrant vos doigts, vous courez le risque de vous faire voler vos empreintes digitales, prévient Isao Echizu.
Alors que les «données sont le pétrole du 21ème siècle », comme on l'entend à l'envi, nous avons une fâcheuse tendance à livrer les nôtres, intentionnellement, sur les réseaux sociaux, en négligeant bien souvent les règles de confidentialité ou l'utilisation commerciale qui est leur est destinée. Mais la vigilance se complique quand on n'a même pas conscience qu'une donnée en est une…

Attention aux données invisibles…

Permettez-moi d'emprunter vos empreintes

Avec la haute résolution des photos prises par les smartphones, une opération – assez complexe, toutefois, et loin d'être à la portée de tout le monde – peut permettre de récupérer les empreintes. « Or à l'inverse des mots de passe, les empreintes, une fois volées, ne pourront jamais être changées», rappelle à *20 Minutes* Gérôme Billois, expert cybersécurité au cabinet Wavestone.
Il note que si l'avertissement du professeur japonais a fait le tour du monde, « on connaissait le risque depuis 2014 »: un hacker avait montré lors d'une conférence qu'il était parvenu à cloner les empreintes digitales de la ministre allemande de la Défense. Depuis, les empreintes digitales sont de plus en plus utilisées, pour déverrouiller smartphones, objets connectés ou pour réaliser certains paiements.

Des photos très bavardes

Autre donnée invisible, la géolocalisation associée aux photos, la grande majorité étant prise aujourd'hui par des smartphones équipés d'une puce GPS (qui ne sert pas qu'à vous guider sur la route jusqu'à Palavas-Les-Flots). Aux images numériques sont associées tout un ensemble de métadonnées, qui «peuvent renseigner la date, l'heure, voire les données GPS de l'image, la marque, le numéro de série de l'appareil ainsi qu'une image en taille réduite de l'image originale», comme le précise We Fight Censorship, qui indique la marche à suivre pour nettoyer ces métadonnées.«Internet abonde de ces images floutées dont le fichier EXIF contient toujours le document avant floutage», lit-on encore.
En septembre dernier, deux étudiants de Harvard ont pu démasquer 229 dealers grâce aux coordonnées géographiques contenues dans les métadonnées associées à des photos qu'ils avaient prises et postées en ligne.

En huit tweets, tout est dit

Sur Twitter, si la géolocalisation des tweets est désactivée par défaut, beaucoup l'activent. En mai dernier, des experts du MIT et d'Oxford démontraient que huit tweets (d'utilisateurs pour lesquels la géolocalisation est activée) suffisaient à localiser quelqu'un de façon très précise. « Il est extrêmement simple pour des personnes avec très peu de connaissance technique de trouver où vous travaillez ou vivez », expliquaient-ils, à l'issue d'une expérience concluante.

Le secret imaginaire des questions secrètes

Il y a enfin ces infos que nous livrons publiquement sur les réseaux sociaux alors qu'elles contiennent parfois les réponses aux questions censées être «secrètes». «Les questions secrètes sont le talon d'Achille des réseaux sociaux, souligne Gérôme Billois. Elles vous permettent d'accéder à vos comptes en cas d'oubli de mot de passe et ce sont toujours les mêmes: Quel est le prénom de votre mère? Quel est votre plat préféré? Or toutes ces infos peuvent être retrouvées facilement sur les réseaux sociaux.»

… et surtout aux données plus évidentes, qui permettent de personnaliser le phishing

Pour les scénarios ci-dessus, qui peuvent avoir le mérite d'attirer l'attention, la probabilité d'utilisation malveillante est pourtant « faible », assure Gérôme Billois. Parallèlement, «nous passons notre temps à livrer des informations hypersensibles», et de façon bien plus directe. Or l'occupation principale des cybercriminels reste les mails de phishing, et ces données les aident à les personnaliser.
«Si le mail est pointu, que c'est votre « bonne » banque qui vous dit qu'elle a remarqué votre passage à telle heure la veille, et que toutes ces infos sont correctes parce que vous avez partagé ces données sur les réseaux sociaux, il y a toutes les chances pour que vous cliquiez sur le lien malveillant.»…[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous accompagner dans vos démarches de mise en conformité avec la réglement Européen relatif à la protection des données à caractère personnel (RGPD).
Denis JACOPINI est Expert Judiciaire en Informatique, Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), Diplômé en Droit de l'Expertise Judiciaire et Risk Manager ISO 27005, spécialisé en Cybercriminalité et en 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

---

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.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité Contactez-nous

Réagissez à cet article

Original de l’article mis en page : Sans le savoir, vous offrez aux hackers des données invisibles

---

Une puce RFID sous la peau. Des salariés volontaires l’ont essayé…

Une puce RFID sous la peau. Des salariés volontaires l’ont essayé…

Une entreprise belge a implanté une puce RFID sous la peau de huit de ses salariés volontaires. Rencontre.

Accepteriez-vous de vous faire pucer pour le boulot ?
C'est ce qu'ont consenti huit des douze salariés d'une agence digitale belge, comme avant eux une entreprise suédoise : mi-décembre, au milieu de leur petit open space blanc et rouge, un pierceur néerlandais leur a logé sous la peau, entre la base du pouce et l'index, une puce RFID (radio frequency identification).
L'une de celles que l'on implante habituellement sous le poil des animaux de compagnie ou des brebis.
Sa silhouette sombre, longue comme un grain de riz, apparaît à travers la chair quand l'un des salariés pucés serre le poing pour nous la montrer.
Comme il l'a fait devant d'autres journalistes avant nous, Tim Pauwels se plie allègrement à la démonstration : sur le trottoir de Malines, ville grise entre Bruxelles et Anvers où l'entreprise est située, il colle avec délicatesse sa main sous l'interphone. Bip!
Miracle tant attendu : la porte s'ouvre. Nous entrons.

« Adoptons la technologie »

L'idée de se faire implanter une puce pour ouvrir la porte de leur boîte leur est venue un vendredi. A l'instar des si cool entreprises de la Silicon Valley, les salariés de Newfusion ont chaque semaine « deux heures de libre » dédiées à la cogitation de projets.
Parce que certains oubliaient régulièrement leur clé, ils ont lancé un vendredi le projet de les remplacer par un système électronique de badges. « Plus facile, plus digital », précise dans un anglais fluide Vincent Nys, 27 ans, qui a lancé NewFusion il y a quatre ans.
« On a passé deux jours dessus, on l'a mis en place mais quelques jours plus tard, ils oubliaient leur carte. Alors on a réfléchi : « quelle est la prochaine étape ? » Nous voulions faire quelque chose d'innovant et ouvrir une discussion. »

Une puce RFID et l'un des kits commandés par Newfusion (Emilie Brouze)
En parfaite adéquation avec son époque, Vincent Nys adore l'innovation (il répète le mot à l'envi). Les milliers de personnes dans le monde qui possèdent une puce électronique se divisent à son sens en deux catégories. Ceux qui le font pour se différencier – « être unique, spécial » – et les consommateurs précoces, « comme nous ». Ceux qui n'ont pas peur de se dire :

« Adoptons la technologie et allons plus loin. »
Son associé complète :
« Ceux qui avancent sont ceux qui ouvrent les portes aux autres… Il faut innover pour pouvoir faire des progrès. »
Innovons donc en ouvrant des portes.

« Est-ce qu'on le sent ? »

Avant de commander les puces à une entreprise américaine qui les commercialise en kits stérilisés, il y a tout de même eu discussion au sein de Newfusion. « On a eu un débat, mais pas celui qu'il y a dans les médias », rétorque Vincent Nys :
« Est-ce que c'est sûr ? Est-ce qu'il y a des implications médicales ? Est-ce qu'on pourra passer un scanner ? Est-ce qu'on le sent ? Est-ce que ça a un impact sur notre vie ? »
Seulement quatre salariés ont refusé de se faire pucer. « Je ne perds pas mon badge, je n'ai pas vu l'intérêt d'une puce », répond Sam Van Campenhout, développeur.
« Je crois que je n'aimerais pas avoir quelque chose sous ma peau. C'est bizarre », ajoute Sil Colson, jeune designer multimédia.

Sil Colson fait partie des salariés ayant refusé de s'implanter une puce RFID (Emilie Brouze)

Ce qui pourrait la faire changer d'avis ? Que la puce contienne son passeport et qu'il suffise de présenter sa main au moment des contrôles, sans risquer d'oublier ou d'égarer le document en vacances. Ou que la puce contienne les infos essentielles de son carnet médical, immédiatement accessible en cas d'urgence. Pour ouvrir la porte d'entrée, Sil préfère conserver son badge.
Un autre développeur raconte que lui a tout de suite été enthousiaste à l'idée (sa copine un peu moins) : « J'adore la technologie. »
En quelques heures, il a bidouillé un programme que le patron lui demande de nous montrer. Alors Dries Van Craen presse sa main droite contre un boîtier relié à son ordinateur. Bip! (La sonorité est la même qu'à la caisse d'un supermarché.)
S'affiche sur l'écran, sur un fond automnal, un message de bienvenue personnalisé. Sur la colonne de droite sont empilés ses morceaux de musique préférés, au-dessus des temps de transport pour rentrer chez lui, actualisés en temps réel.
Le patron s'enthousiasme :
« Voilà ce que tu peux faire sans argent et en une demi-journée. Avec des années et une vision, on pourra faire plein de choses. »
Le jeune patron technophile a installé chez lui un système lui permettant d'ouvrir la porte de son domicile d'un geste de la main.
Prochaine étape : bricoler un moyen de régler son éclairage intérieur grâce à la même puce (un jeu de lumières pour ses soirées en solitaire, un autre quand il est avec sa compagne).

« Disrupter » le marché

Quand on lui fait remarquer l'utilité à ce stade toute relative de ces puces sous-cutanées, Vincent Nys assume. Parce qu'il ne s'agit pas que de se débarrasser des badges d'entrée : c'est une piste de développement pour Newfusion.
« Dans nos têtes, on ne s'est même pas demandé ce qu'on pouvait faire avec [les puces RFID]. On s'est dit « Allons-y, faisons-le ». On ne s'est pas trop préoccupé de questions éthiques, morales et des possibles applications.
On pense qu'il faut être les premiers à le faire. On commence par « disrupter » le marché, puis on créé des applications. «
Sur la RTBF, qui a diffusé l'un des premiers reportages sur l'opération de puçage, Alexis Deswaef, président de la ligue des Droits de l'Homme en Belgique, soulevait une question éthique : « Dans le futur, braderons-nous un peu plus nos droits à la vie privée pour plus de sécurité ou de confort ? »
En dépit des critiques, Vincent Nys, comme son associé, sont ravis des retombées médiatiques, eux qui espéraient intéresser seulement quelques blogs techs avec leur communiqué de presse : on parle d'eux dans le monde entier. Quelle bonne pub ! Des banques, une société de transports publics ou encore une municipalité ont d'ores et déjà pris contact avec eux.

« Big Brother »

A côté de ces potentiels nouveaux clients, Newfusion a aussi reçu une cinquantaine de messages désagréables. « Des gens qui faisaient référence aux années Hitler – parce qu'on marquait les gens -, des personnes qui nous traitaient d'antéchrist ou nous parlent de Big Brother… » Beaucoup d'après lui n'ont pas bien compris la technologie.
Vincent Nys fait défiler certains commentaires Facebook sur son téléphone : « Ce n'est pas éthique », « 0% liberté », « il est temps que je lise de nouveau « 1984 » »… Il remarque :
« Ils sont tous fixés sur ce livre. »

Vincent Nys, fondateur et directeur de Newfusion, le 9 février 2017 à Malines (Emilie Brouze)
Au début, le patron répondait poliment et pédagogiquement à ceux qui ne sont manifestement pas mûrs pour "aller plus loin" : non, non, non, il ne s'agit pas de traquer les gens. La puce RFID qu'il a lui aussi sous la peau fonctionne sans batterie et ne peut pas transmettre à un tiers la localisation du porteur.
Elle contient un numéro unique ainsi qu'un espace mémoire lui permettant par exemple d'enregistrer sa carte de visite pour la donner à un client en posant sa main sur son smartphone.
Alors oui, le patron peut savoir exactement quand un des employés pucés entre ou sort du bâtiment, « comme avec les badges ou la caméra fixée à l'extérieur », semble-t-il relativiser. « Mais ce n'est pas le but et ce n'est pas notre culture. Les employés ont des horaires de travail souples. »…[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous accompagner dans vos démarches de mise en conformité avec la réglement Européen relatif à la protection des données à caractère personnel (RGPD).
Denis JACOPINI est Expert Judiciaire en Informatique, Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), Diplômé en Droit de l'Expertise Judiciaire et Risk Manager ISO 27005, spécialisé en Cybercriminalité et en 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

---

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 DIRECCTE n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité Contactez-nous

Réagissez à cet article

Original de l’article mis en page : Travailleurs belges pucés : « On ne s’est pas trop préoccupé de questions éthiques » – L’Obs