4.5 MILLION PEOPLE FORCED TO CANCEL CREDIT & DEBIT CARDS IN THE LAST YEAR DUE TO ONLINE FRAUD

One in ten people have been the victim of a cyber-attack on their credit or debit card in the last year, according to new research from comparethemarket.com. In 62% of cases, money was successfully removed from the account with an average of £475 stolen. At a national level this equates to 4.…[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

Cyberattaques. TPE et PME, cibles faciles

Cyberattaques. TPE et PME, cibles faciles

Les attaques informatiques se multiplient. En particulier dans le monde professionnel, où les petites entreprises sont des cibles de choix pour les pirates. Le géant américain Yahoo! vient de l'avouer, 500 millions de comptes de ses utilisateurs ont été piratés à la fin de 2014.…[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

Yahoo!, victime de la « cyberguerre froide » ?

Le piratage massif des comptes de Yahoo!, qui s'estime attaqué

par un Etat, pourrait être un nouvel exemple d'une « cyberguerre froide » menée par des pays comme la Russie ou la Chine, mais rien ne sera jamais prouvé, selon des experts.…[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.

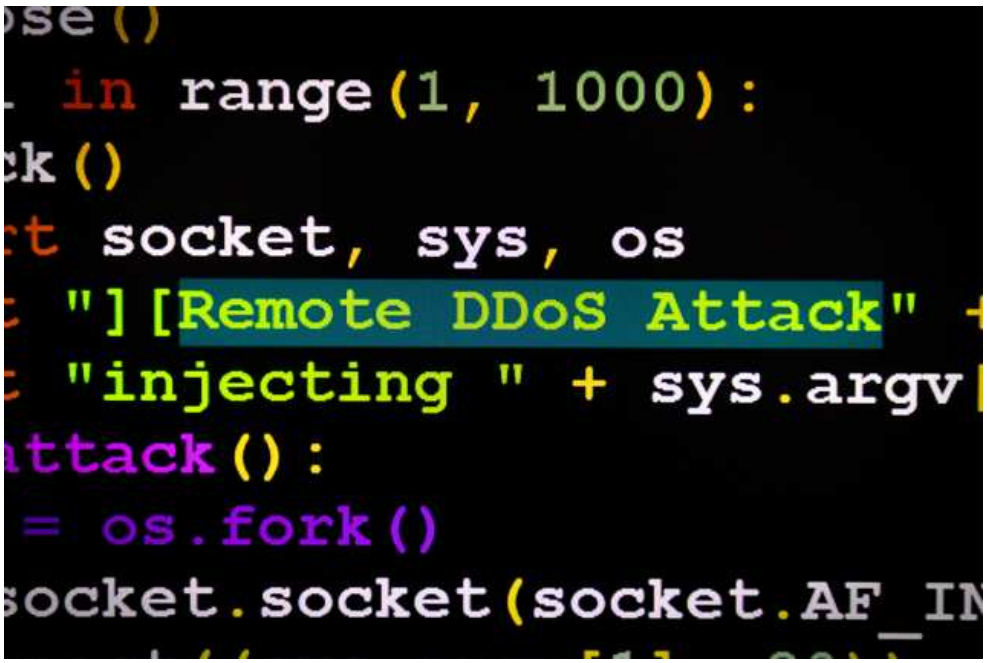
- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation 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

OVH attaqué par des réseaux d’objets connectés



OVH attaqué par des réseaux d’objets connectés

C’est un record dont il se serait sans doute passé. La semaine dernière, le fondateur d’OVH Octave Klaba expliquait sur son compte Twitter que l’hébergeur roubaisien était victime d’une série d’attaques en déni de service (DDoS) d’une ampleur inédite.

Ces attaques, qui consistent à submerger un service Web de demandes pour le mettre hors service, sont monnaie courante sur la Toile. Dans une étude portant sur la période avril 2015-mai 2016 , la société Imperva notait une multiplication par deux du nombre d’attaques DDoS par rapport à l’année précédente (à 445 attaques par semaine chez ses clients).
Mais c’est surtout la puissance de feu déployée récemment qui surprend. Mesurée en Gigabits par seconde (Gbps) quand elle se concentre sur la couche réseau, l’attaque la plus forte enregistrée par Imperva atteignait 470 Gbps mi-2016. Depuis, ce record ne cesse de tomber.
Cet été, les organisateurs des Jeux olympiques de Rio remportaient la médaille d’or de l’attaque DDoS avec des pics à 540 Gbps. La semaine dernière, c’était au tour du blog du spécialiste de la sécurité informatique Brian Krebs de subir « la plus grande attaque DDoS qu’Internet ait jamais vu », à 665 Gbps. Presque simultanément, OVH lui ravissait la couronne, encaissant des pics à plus de 1.000 Gbps.

Des botnets extrêmement efficaces

Pour mener des raids aussi violents, les cybercriminels s’appuient désormais non plus seulement sur des ordinateurs corrompus pour relayer leurs attaques (un « botnet », dans le jargon), mais sur des millions d’objets connectés – caméras IP, enregistreurs vidéo, routeurs…
Selon Octave Klaba, le botnet qui s’est attaqué à OVH comprenait ainsi pas moins de 145.607 caméras et enregistreurs numériques . Si les premiers botnets d’objets connectés (téléviseurs, réfrigérateurs…) ont été détectés dès 2014 , ils sont devenus extrêmement efficaces…[lire la suite]

Réagissez à cet article

Original de l’article mis en page : OVH : ces cyberattaques dopées par des réseaux d’objets connectés, High tech

---

Attaque informatique par Clé

USB piégée, plus fréquente qu’il n’y parraît

	**Attaque informatique par Clé USB piégée, plus fréquente qu’il n’y parraît**

Attaque informatique via votre boîte aux lettres ! La police Australienne alerte les citoyens de Melbourne après la découverte de clés USB piégées distribuées dans des boites aux lettres.

Voilà une attaque informatique, couplée à du social engineering, qui laisse songeur. La police fédérale de l'État de Victoria [Australie] a mis en garde les habitants de la banlieue de Pakenham (région de Melbourne) de ne surtout pas utiliser la clé USB qui a pu leur être proposée. Une clé USB diffusée dans un courrier, placé directement dans leur boite aux lettres. L'avertissement que j'ai repéré dans le site officiel de la Police locale indique que « ***Les lecteurs USB sont considérés comme extrêmement dangereux et le public est invité à ne pas les brancher sur leurs ordinateurs ou d'autres appareils informatiques.***«
Il a été constaté que la clé USB mystérieuse lançait des processus dans les ordinateurs comme l'installation d'outils dédiés à des abonnements malveillants. Même si les clés USB ont été détectées dans un seul quartier, la police de Victoria a néanmoins jugé bon d'émettre une alerte à l'échelle de l'État…[lire la suite]

Denis Jacopini anime des **conférences et des formations** et est régulièrement invité à des **tables rondes en France et à l'étranger** 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

---

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 : ZATAZ Attaque informatique : Clé USB piégée dans votre boîte aux lettres – ZATAZ

Enfin une idée pour suivre en temps réel la localisation des avions

Enfin une idée pour suivre en temps réel la localisation des avions

Une constellation de satellites pour pister les avions où qu'ils soient. Tel est le projet de deux sociétés américaines qui vont placer des récepteurs dans des satellites qui seront mis en orbite très prochainement.

C'est une question qui taraude systématiquement l'industrie aéronautique à chaque fois qu'un avion disparaît mystérieusement sans laisser la moindre trace : comment aurait-on pu améliorer le suivi de l'appareil ? À cette question, les progrès techniques ont déjà fourni au fil du temps des réponses qui ont fortement amélioré la qualité du contrôle du trafic aérien.
Mais ce n'est évidemment pas suffisant. Il y a à peine plus de deux ans, le vol MH370 de la Malaysia Airlines sortait de son plan de vol initial – l'avion, un Boeing 777, devait relier Kuala Lumpur à Pékin – pour s'abîmer quelque part dans l'océan Indien. La carcasse principale n'a jamais été retrouvée. Seuls quelques débris charriés au gré des courants ont fini par échouer sur les côtes.

DES SATELLITES EN ORBITE BASSE À LA RESCOUSSE

C'est pour éviter la répétition de ce scénario que deux sociétés américaines œuvrent sur un dispositif consistant à placer des récepteurs ADS-B (automatic dependent surveillance-broadcast) dans des satellites situés en orbite terrestre basse, à une altitude d'environ 780 km. Les deux entreprises, FlightAware et Aireon, anticipent une mise en service aux alentours de 2018.
« *Cela n'aura pas d'importance que le vol se trouve au-dessus de l'océan, d'un désert ou du Pôle Nord, nous saurons où est l'avion* », commente, très confiant, Daniel Baker, le patron de FlightAware à Reuters. Selon les instigateurs du projet, il sera possible d'avoir un suivi des avions en quasi-temps réel, de manière à éviter que ne subsistent de trop longues plages de temps entre deux contacts automatiques de l'avion.

IRIDIUM NEXT

Ce sont des satellites de la future constellation Iridium NEXT qui seront utilisés pour accueillir les récepteurs ADS-B. Ces satellites, qui doivent être au nombre de 70 (66 actifs et 4 de réserve), doivent être mis en orbite par SpaceX au cours de sept missions distinctes devant décoller de la base de l'Air Force Vandenberg en Californie.
C'est la fusée Falcon 9 qui sera utilisée. Au départ, il était prévu que les vols démarrent à la fin 2016. Toutefois, les premiers décollages risquent d'être reportés à cause de l'explosion d'un lanceur au début du mois de septembre. Le groupe a toutefois une piste sur l'origine de la catastrophe et se dit persuadé de pouvoir reprendre ses missions dès novembre… pile pour les vols des satellites Iridium NEXT.
Le cas du vol MH370 n'a pas uniquement nourri la réflexion de FlightAware et Aireon. Du côté du conseil de l'organisation de l'aviation civile internationale (OACI), une série de modifications a été proposée ce printemps pour pister plus efficacement un aéronef en détresse dans des zones isolées. Il est en particulier question de pouvoir obtenir la localisation de l'avion toutes les minutes…[lire la suite]

Réagissez à cet article

Original de l’article mis en page : Des satellites pour suivre en permanence la localisation des avions – Tech – Numerama

---

Alerte, découverte d’un virus qui se propage principalement via les Réseaux Sociaux

Alerte, découverte d’un virus qui se propage principalement via les Réseaux Sociaux

---

Afin de voler leurs données, le malware utilise une campagne de diffusion massive ciblée en renvoyant les victimes vers un site gouvernemental libyen compromis et contenant le malware

Malgré le manque de sophistication du malware et un mécanisme de propagation rudimentaire, les auteurs de cette menace ont démontré qu'ils étaient capables de compromettre des sites gouvernementaux avec succès.
Au cours de leurs recherches, les **experts ESET** ont découvert que les attaquants compromettent des profils de réseaux sociaux (Facebook, Twitter…) et postent des liens amenant au téléchargement de logiciels malveillants. Le post est rédigé en arabe et explique : « le premier ministre a été capturé à deux reprises, dont cette fois-ci dans une bibliothèque ».

Ce message texte relativement court est suivi d'un lien vers le site gouvernemental compromis.

Figure 1 : Post sur Facebook renvoyant vers un lien comportant le malware

En plus de la diffusion massive de cette campagne, les cybercriminels mènent des attaques ciblées par l'envoi d'e-mail contenant une pièce jointe malveillante de type spearphishing. Pour convaincre les victimes d'exécuter le code malveillant, des astuces d'ingénierie sociale sont mises en œuvre, comme l'utilisation d'icônes MS Word et PDF à la place de celles des exécutables et de techniques de double extension dans les noms de fichier, comme .pdf.exe. Dans certains cas, le malware peut afficher un document leurre.
Les experts ESET ont identifié le malware comme appartenant à la famille des Chevaux de Troie qui tentent de recueillir diverses informations par le vol de données classiques. Il peut être déployé sous plusieurs configurations. **La version complète du logiciel malveillant peut enregistrer les frappes de clavier, collecter des fichiers de profil des navigateurs Mozilla Firefox et Google Chrome, enregistrer des sons à partir du microphone, réaliser des captures d'écran depuis la webcam, et recueillir des informations sur la version du système d'exploitation et du logiciel antivirus installé.** Dans certains cas, le logiciel malveillant peut télécharger et exécuter des outils tiers de récupération de mots de passe enregistrés à partir d'applications installées.
« Nous avons analysé un échantillon de ce malware qui est actif depuis au moins 2012 dans des régions spécifiques du globe. Par le passé, les auteurs de cette cybermenace utilisaient ce malware pour une diffusion massive. Il convient de noter qu'il est encore utilisé dans des attaques de spearphishing », explique Anton Cherepanov, malware researcher chez ESET.
Pour plus de détails sur ce malware, cliquez ici.
Source : ESET

Réagissez à cet article

Original de l’article mis en page : Boîte de réception (10) – denis.jacopini@gmail.com – Gmail

---

Un utilisateur de Yahoo! poursuit le groupe pour « négligence »

Un utilisateur de Yahoo! poursuit le groupe pour « négligence »

Le plaignant regrette que les mesures de sécurité du groupe n'aient pas été renforcées. Il s'autoproclame représentant des utilisateurs lésés par le vol de données.

Après l'annonce, jeudi 22 septembre, du piratage d'au moins 500 millions de comptes d'utilisateurs de Yahoo!, le groupe est désormais poursuivi pour « *négligence grave* » à la suite de la plainte d'un utilisateur. Le groupe de Sunnyvale (Californie) fait face à un certain nombre de questions relatives à sa gestion de l'incident.
La plainte a été déposée vendredi auprès du tribunal fédéral de San Jose (Californie), par Ronald Schwartz, un résident de New York qui entend représenter tous les utilisateurs américains de Yahoo! affectés par le vol de leurs informations personnelles.
L'opérateur de services Internet a annoncé, la veille, que les données volées pourraient inclure des noms, des adresses emails, des numéros de téléphone, des dates de naissance et des mots de passe cryptés. Il a exclu à ce stade le vol de données bancaires dans ce qu'il présente comme une attaque menée par un « *agent piloté par un Etat* », sans apporter de preuve de cette hypothèse. L'action en justice vise le statut de recours collectif (« *class action* ») et entend réclamer des dommages et intérêts.
Selon le plaignant, le piratage aurait pu être évité si le groupe avait renforcé ses mesures de sécurité après plusieurs précédentes tentatives d'effraction. Il déplore également la lenteur de Yahoo!, qui aurait, selon lui, mis trois fois plus de temps que ses concurrents pour faire état du piratage…[lire la suite]

Denis Jacopini anime des **conférences et des formations** et est régulièrement invité à des **tables rondes en France et à l'étranger** 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

---

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

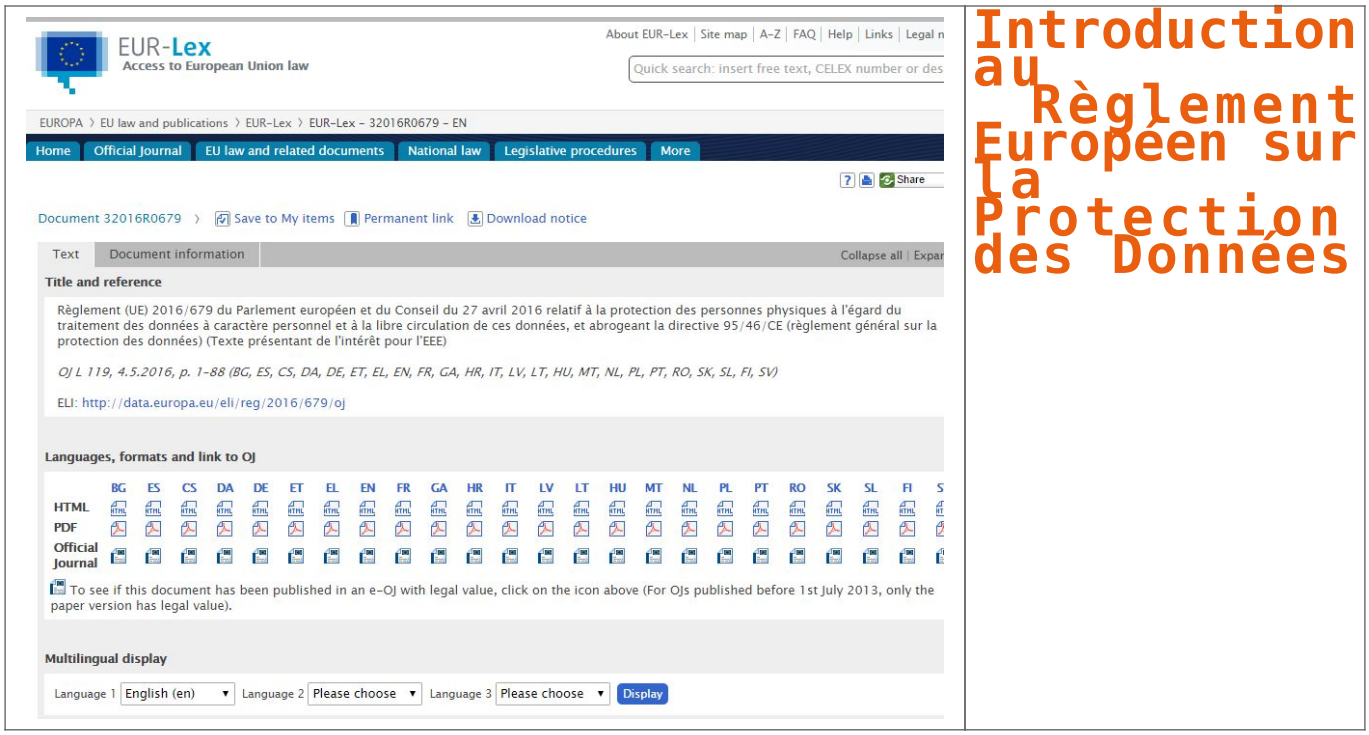
Contactez-nous

Réagissez à cet article

Original de l'article mis en page : Piratage massif : Yahoo!

poursuivi pour « négligence » par un utilisateur

Introduction au Règlement Européen sur la Protection des Données



Introduction au Règlement Européen sur la Protection des Données

Le Règlement Général de l'Union Européenne sur la Protection des Données (RGPD) impose aux entreprises d'effectuer un suivi de toutes les occurrences des données à caractère personnel des clients au sein de leur organisation, d'obtenir le consentement des clients concernant l'utilisation de leurs informations personnelles (y compris le « droit à l'oubli ») et de documenter l'efficacité de cette gouvernance des données pour les auditeurs.

Deux tiers (68 %) des entreprises, selon Compuware, risquent de ne pas être en conformité avec le RGPD, en raison d'une augmentation de la collecte des données, de la complexité informatique grandissante, de la multiplicité des applications, de l'externalisation et de la mobilité. Ce risque tient aussi aux politiques laxistes concernant le masquage des données et l'obtention d'une autorisation explicite des clients en matière de données. Les entreprises européennes comme américaines doivent, par conséquent, adopter une série de bonnes pratiques, notamment un masquage plus rigoureux des données de test et de meilleurs pratiques concernant le consentement des clients, afin d'éviter des sanctions financières et une altération possible de leur image de marque résultant d'une non-conformité.
Le RGPD de l'Union européenne a été adopté en avril 2016, afin d'unifier des obligations auparavant réparties à travers différentes juridictions européennes concernant l'utilisation, la gestion et la suppression des informations personnellement identifiables (IPI) des clients par les entreprises. Toutes les entreprises dans l'UE, aux États-Unis et ailleurs, qui collectent des IPI relatives à des citoyens de l'UE, ont jusqu'en mai 2018 pour se conformer à ces dispositions. Tout non-respect du RGPD expose les entreprises à des amendes pouvant atteindre 20 millions € ou 4 % du chiffre d'affaires mondial….[lire la suite]

Denis Jacopini anime des **conférences et des formations** et est régulièrement invité à des **tables rondes en France et à l'étranger** 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

---

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

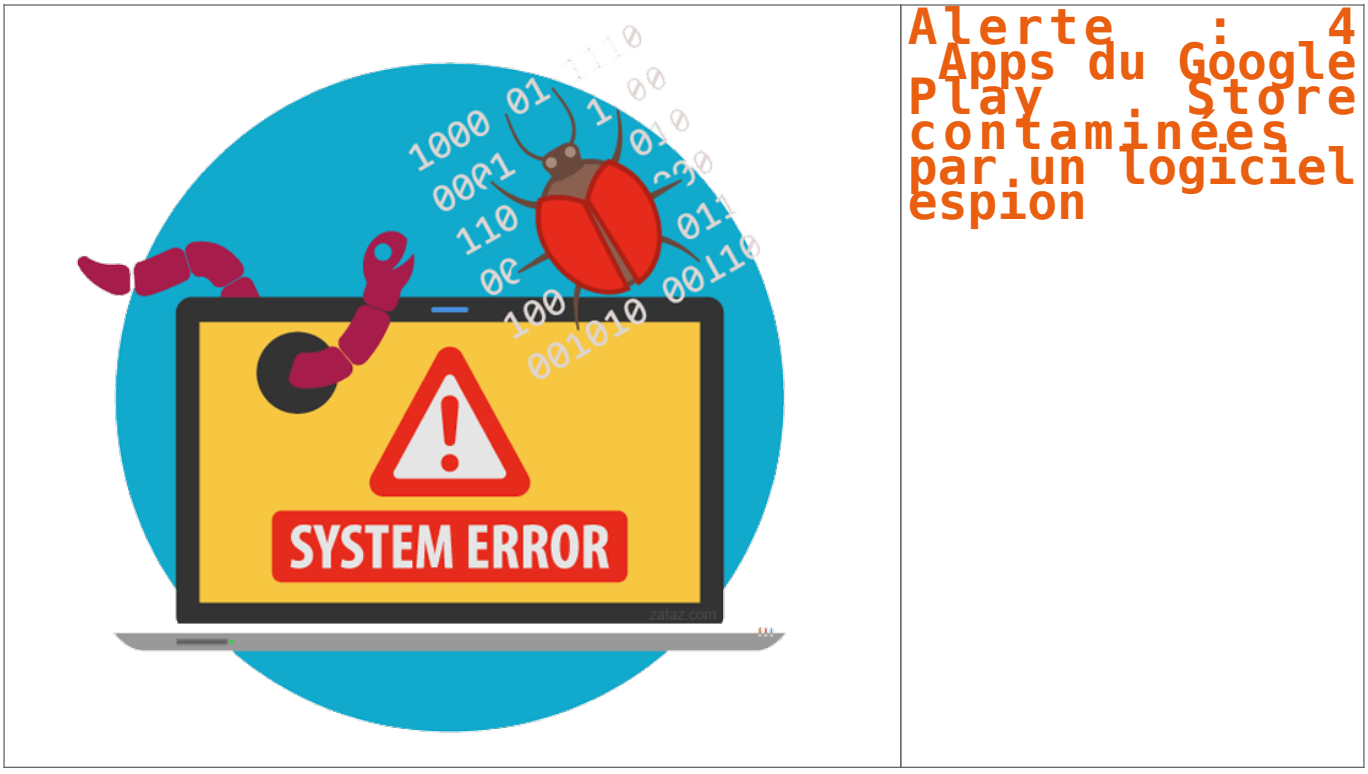
Contactez-nous

Réagissez à cet article

Original de l’article mis en page : Retour sur le RGPD, le Règlement Général de l’Union Européenne sur la Protection des Données – Data Security BreachData Security Breach

---

Alerte : 4 Apps du Google Play Store contaminées par un logiciel espion



Alerte : 4 Apps du Google Play Store contaminées par un logiciel espion

---

Quelques semaines seulement après avoir alerté Apple sur le logiciel espion PEGASUS qui avait trouvé une faille TRIDENT pour s'infiltrer sur IOS, l'équipe de veille et de recherche de Lookout Mobile Security, annonce avoir découvert un logiciel espion qui a attaqué plusieurs Apps sur Google Play Store.

Le spyware appelé OVERSEER, a été identifié sur quatre applications, dont une, Embassy, qui permettait aux voyageurs de rechercher des Ambassades à l'étranger. Ce malware a aussi été injecté sous forme de Trojan dans des applications de diffusion actualités Russes et Européennes. Google a promptement retiré les quatre applications infectées après avoir été prévenu par Lookout.
OVERSEER est un spyware qui cible par exemple grâce à Embassy, les grands voyageurs avec la fonction principale d'effectuer des recherches d'adresses d'Ambassades à travers le monde. Les personnes en voyages d'affaires, qui voyagent régulièrement, peuvent être particulièrement vulnérables à une telle attaque en installant sur leur téléphone l'application…[lire la suite]

Denis Jacopini anime des **conférences et des formations** et est régulièrement invité à des **tables rondes en France et à l'étranger** 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

---

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 : Un nouveau logiciel espion OVERSEER s'attaque aux Apps du Google Play Store – Data Security BreachData Security Breach