

WhatsApp et Telegram corrigent des vulnérabilités importantes



WhatsApp et Telegram ont corrigé des failles dans leurs applications après que des chercheurs en sécurité ont révélé qu'il était possible de prendre le contrôle des comptes d'utilisateurs.

WhatsApp et Telegram sont deux applications de messagerie instantanée qui ont plus d'un milliard d'utilisateurs cumulés. Elles offrent des communications chiffrées, un envoi de messages rapide et un tas d'autres fonctionnalités. Mais de nouvelles recherches révèlent qu'une image injectée par un logiciel malveillant aurait suffi à voler les comptes Web WhatsApp ou Telegram d'une personne. Il faudrait seulement quelques secondes pour que l'attaquant obtienne un contrôle total sur les comptes, y compris l'accès aux images, aux vidéos, aux fichiers audio et aux contacts. Et le cryptage serait effectivement une aide avec ce genre de hack.

La vulnérabilité était présente sur les versions desktop des applications, ainsi si vous n'utilisez pas WhatsApp ou Telegram sur votre ordinateur, alors vous étiez déjà à l'abri.

Les chercheurs en sécurité ont découvert que le code malveillant pouvait être caché à l'intérieur d'une image. Lorsqu'il est cliqué, le fichier image exécute le code et l'attaquant obtient un accès complet aux données de stockage WhatsApp et/ou Telegram. Le pirate pourrait ensuite envoyer le fichier à tous les contacts de la victime, en diffusant le malware à d'autres cibles.

Découverte par Check Point, la vulnérabilité a été communiquée à WhatsApp et Telegram le 8 mars, et les deux entreprises ont déjà déployé des correctifs pour leurs clients desktop...[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.



[Contactez-nous](#)

Réagissez à cet article

Source : WhatsApp et Telegram corrigent des vulnérabilités importantes – Gridam

Formations en cybersécurité en France

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer					
 LE NET EXPERT AUDITS & EXPERTISES	 LE NET EXPERT EXPERTISES DE SYSTEMES DE VOTES ELECTRONIQUES	 LE NET EXPERT RGPD CYBER MISES EN CONFORMITE	 SPY DETECTION Services de détection de logiciels espions	 LE NET EXPERT FORMATIONS	 LE NET EXPERT ARNAQUES & PIRATAGES
 vous informe		Formations en cybersécurité en France			

A titre indicatif, voici la liste des formations en cybersécurité délivrant un titre reconnu par l'Etat (ministère en charge de l'enseignement supérieur ou CNCF) de niveau équivalent à Bac3 (licence professionnelle) jusqu'à Bac+5 (master, ingénieur).

Cette liste de formations a vocation à informer les étudiants sur l'ensemble des formations accessibles. Ne figurent dans cette liste ni la formation continue, ni les titres non reconnus officiellement par l'Etat (DU, masters spécialisés, MSc2, etc.). Les éléments figurant ci-dessous sont issus d'une recherche de données multiples et éparpillées dans l'ensemble des établissements d'enseignement supérieur en France. Cette liste n'est plus maintenue et sera supprimée en juillet 2017.

Ne savoir plus sur Serhmedu, le label de formations initiales en cybersécurité de l'enseignement supérieur

3		
FORMATIONS RECOGNÉES DE NIVEAU LICENCE		
NON ÉTABLISSEMENT	NOM FORMATION	SITE INTERNET
Cnam Bretagne	Licence Pro « Analyse en Sécurité des Systèmes Télécoms Réseau et Informatiques » MSTIS	http://comsecuredéfense.fr/formation-securite-telecoms-reseau/
Université d'Als-Mersenne	Licence Pro « Administration et sécurité des réseaux d'entreprises »	http://sat.univ-als.fr/diplomes/licence-professionnelle-reseau-telecommunications-specialite-administration-securite
Université d'Artois	Licence Pro « Systèmes informatiques et logiciel - Sécurité informatique »	http://formation.univ-artois.fr/dm312/etw_cdegetfrwainak_cdePR_M2_M20203_PM_3LSI20203_M2_rndrctvoir_fiche_program_langfr_FR_englet-description
Université de Cergy-Pontoise 1	Licence Pro « Administration et Sécurité des Réseaux »	http://labweb.u-cergy.fr/virtual/formation/formation0824
Université de Grenoble Joseph Fourier	Licence Pro « Réseau Sans Fil et Sécurité »	https://utis1-ufj-grenoble.fr/formation-et-mettre/licence-professionnelle/reseaux-et-telecommunications
Université de Grenoble Pierre Mendès France	Licence Pro « Administration et Sécurité des Réseaux »	http://www.univ-valence.fr/licence-professionnelle-seu/
Université de Haute-Normandie	Licence Pro « Administration et Sécurité des Réseaux »	http://www.univ-lorraine.fr/licence-professionnelle-reseau-telecommunications
Université de la Réunion	Licence Pro « Réseau Sans Fil et Sécurité »	http://www.univ-lorraine.fr/licence-professionnelle-reseau-telecommunications
Université de la Rochelle	Licence Pro « Administration et Sécurité des Réseaux »	http://www.univ-lorraine.fr/licence-professionnelle-reseau-telecommunications
Université de Valenciennes et du Hainaut-Cambresis	Licence Pro « Collaborateur de Défense et Aide à l'Intrusion des Systèmes Informatiques (CDAISI) »	http://formation.univ-valenciennes.fr/cdegetfrwainak_cdePR_M2_M20203_PM_3LSI20203_M2_rndrctvoir_fiche_program_langfr_FR_englet-description
Université de Montpellier 2	Licence Pro « Administration et sécurité des réseaux »	http://www.univ-lorraine.fr/licence-professionnelle-reseau-telecommunications
Université de Lorraine	Licence Pro « Réseau Sans Fil et Sécurité »	http://utisb.univ-lorraine.fr/cdegetfrwainak_cdePR_M2_M20203_PM_3LSI20203_M2_rndrctvoir_fiche_program_langfr_FR_englet-description
Université de Metz	Licence Pro « Administration et sécurité des réseaux »	http://www.univ-lorraine.fr/licence-professionnelle-reseau-telecommunications
Université Paris Est Créteil Val de Marne	Licence Pro « Réseau informatique, mobilité, sécurité (RIMS) »	http://www.univ-lorraine.fr/licence-professionnelle-reseau-telecommunications
Université Paris 13	Licence Pro « Administration et Sécurité en Réseaux »	http://www.univ-lorraine.fr/licence-professionnelle-reseau-telecommunications
Université de Paris Sud	Licence Pro « Sécurité des Réseaux et Systèmes Informatiques »	http://www.univ-lorraine.fr/licence-professionnelle-reseau-telecommunications
Université de Rennes 1	Licence Pro « Administration et Sécurité des Réseaux »	http://www.univ-lorraine.fr/licence-professionnelle-reseau-telecommunications
Université de Rouen	Licence Pro « Administration Sécurité des Réseaux »	http://www.univ-lorraine.fr/licence-professionnelle-reseau-telecommunications
Université de Toulouse 2	Licence Pro « Réseau Sans Fil et Sécurité »	http://www.univ-lorraine.fr/licence-professionnelle-reseau-telecommunications
Université de Toulon	Licence Pro « Sécurité des Réseaux et Systèmes Informatiques »	http://www.univ-lorraine.fr/licence-professionnelle-reseau-telecommunications
Université de Trier	Licence Pro « Sécurité des Réseaux et Systèmes Informatiques »	http://www.univ-lorraine.fr/licence-professionnelle-reseau-telecommunications
Université de Versailles Saint-Quentin	Licence Pro « Administration et Sécurité des Réseaux »	http://www.univ-lorraine.fr/licence-professionnelle-reseau-telecommunications
Université de Pau et des Pays de l'Adour	Licence Pro « Administration et Sécurité des Réseaux »	http://www.univ-lorraine.fr/licence-professionnelle-reseau-telecommunications
Université de Bordeaux 1	Licence Pro « Administration et Sécurité des Réseaux »	http://www.univ-lorraine.fr/licence-professionnelle-reseau-telecommunications
Université des Antilles et de la Guyane	Licence Pro « Administration et Sécurité des Réseaux »	http://www.univ-lorraine.fr/licence-professionnelle-reseau-telecommunications

FORMATIONS RECOGNÉES DE NIVEAU MASTER	NOM FORMATION	SITE INTERNET
NON ÉTABLISSEMENT	NOM FORMATION	SITE INTERNET
Université de Bourgogne	Master « Réseaux et sécurité des systèmes informatiques »	http://www.univ-bourgogne.fr/formation/formation-programme/master-gra-rech-informatique-specialite-reseaux-et-securite-des-systemes-informatiques-200756.kjsp
Université de Bordeaux 1	Master « Cryptologie et sécurité informatique »	http://www.math.u-bordeaux.fr/guery/theses/2012/
Université de Bretagne Sud (UBS)	Ingénieur « Management et Ingénierie de sécurité des systèmes - cybersécurité »	http://www.univ-brest.fr/formation/formation-programme/master-gra-rech-informatique-specialite-reseaux-et-securite-des-systemes-informatiques-200756.kjsp
Université Grenoble Alpes et Grenoble INP/Ensimag	Master « Cryptologie, sécurité et usage de l'information »	http://www.univ-brest.fr/formation/formation-programme/master-gra-rech-informatique-specialite-reseaux-et-securite-des-systemes-informatiques-200756.kjsp
Université Grenoble Alpes	Master « Sécurité, audit, informatique légale - SAFI »	http://www.univ-brest.fr/formation/formation-programme/master-gra-rech-informatique-specialite-reseaux-et-securite-des-systemes-informatiques-200756.kjsp
Université Grenoble Alpes et Grenoble INP/Ensimag	Master « Cybersécurité »	http://www.univ-brest.fr/formation/formation-programme/master-gra-rech-informatique-specialite-reseaux-et-securite-des-systemes-informatiques-200756.kjsp
Université de Lorraine (Mines Nancy, Telecom Nancy, ENSI)	Master « Security et Computer Systems »	http://www.univ-brest.fr/formation/formation-programme/master-gra-rech-informatique-specialite-reseaux-et-securite-des-systemes-informatiques-200756.kjsp
Université de Lorraine	Master « Services, sécurité des systèmes et des réseaux »	http://www.univ-brest.fr/formation/formation-programme/master-gra-rech-informatique-specialite-reseaux-et-securite-des-systemes-informatiques-200756.kjsp
Université de Lorraine	Master « Sécurité des systèmes d'information et de communication - SSC »	http://www.univ-brest.fr/formation/formation-programme/master-gra-rech-informatique-specialite-reseaux-et-securite-des-systemes-informatiques-200756.kjsp
Université de Lyon 1	Master SAFIR, parcours « Sécurité des systèmes informatiques en finance et en assurance »	http://www.univ-brest.fr/formation/formation-programme/master-gra-rech-informatique-specialite-reseaux-et-securite-des-systemes-informatiques-200756.kjsp
Université de Lyon 2	Master « Organisation et protection des systèmes et des réseaux - OPSIS »	http://www.univ-brest.fr/formation/formation-programme/master-gra-rech-informatique-specialite-reseaux-et-securite-des-systemes-informatiques-200756.kjsp
Université de Nice Sophia Antipolis	Ingénieur « Cryptographie, Sécurité, et Vie Privée dans les Applications et Réseaux »	http://www.univ-brest.fr/formation/formation-programme/master-gra-rech-informatique-specialite-reseaux-et-securite-des-systemes-informatiques-200756.kjsp
Université de Paris 8 - en partenariat avec Paris Diderot (Paris 7)	Master « Mathématiques fondamentales et protection de l'information »	http://www.univ-brest.fr/formation/formation-programme/master-gra-rech-informatique-specialite-reseaux-et-securite-des-systemes-informatiques-200756.kjsp
Université de Paris-Diderot (Paris 7) - en partenariat avec Paris 8	Master « Mathématiques, Informatique et applications à la Cryptologie - MIC »	http://www.univ-brest.fr/formation/formation-programme/master-gra-rech-informatique-specialite-reseaux-et-securite-des-systemes-informatiques-200756.kjsp
Université de Paris-Est Créteil (Paris 12)	Master « Sécurité des systèmes informatiques »	http://www.univ-brest.fr/formation/formation-programme/master-gra-rech-informatique-specialite-reseaux-et-securite-des-systemes-informatiques-200756.kjsp
Université de Poitiers	Licence Pro « Management des risques informatiques et industriels »	http://www.univ-brest.fr/formation/formation-programme/master-gra-rech-informatique-specialite-reseaux-et-securite-des-systemes-informatiques-200756.kjsp
Université de Reims Champagne-Ardenne	Master spécialité informatique, parcours « Administration et sécurité des réseaux »	http://www.univ-brest.fr/formation/formation-programme/master-gra-rech-informatique-specialite-reseaux-et-securite-des-systemes-informatiques-200756.kjsp
Université de Rennes 1	Master « Sécurité des Systèmes d'Information - SSIC »	http://www.univ-brest.fr/formation/formation-programme/master-gra-rech-informatique-specialite-reseaux-et-securite-des-systemes-informatiques-200756.kjsp
Université de Rennes 1, Université de Bretagne Sud, Université de Bretagne Occidentale, ENS Rennes, ENSI, ENSI Bretagne, ENSI Rennes, CentraleSupélec, Telecom Bretagne	Master « Sécurité des contenus et des infrastructures informatiques »	http://www.univ-brest.fr/formation/formation-programme/master-gra-rech-informatique-specialite-reseaux-et-securite-des-systemes-informatiques-200756.kjsp
Université de Rouen	Master « Sécurité des Systèmes Informatiques (SSI) »	http://www.univ-brest.fr/formation/formation-programme/master-gra-rech-informatique-specialite-reseaux-et-securite-des-systemes-informatiques-200756.kjsp
Université de Valenciennes	Master « Informatique, Réseaux et Sécurité - IRS »	http://www.univ-brest.fr/formation/formation-programme/master-gra-rech-informatique-specialite-reseaux-et-securite-des-systemes-informatiques-200756.kjsp
Université de Versailles-Saint-Quentin	Master « Sécurité des contenus, des réseaux, des télécommunications et des systèmes - SAFICS »	http://www.univ-brest.fr/formation/formation-programme/master-gra-rech-informatique-specialite-reseaux-et-securite-des-systemes-informatiques-200756.kjsp
Université d'Orléans	Master « Informatique Numérique, Intelligence et Sécurité »	http://www.univ-brest.fr/formation/formation-programme/master-gra-rech-informatique-specialite-reseaux-et-securite-des-systemes-informatiques-200756.kjsp
Université du Havre	Master « Systèmes informatiques, Réseaux et Sécurité - MITS »	http://www.univ-brest.fr/formation/formation-programme/master-gra-rech-informatique-specialite-reseaux-et-securite-des-systemes-informatiques-200756.kjsp
Université Pierre et Marie Curie (Paris 6) - avec l'APSI	Master « Informatique, spécialité IPSI, Filière sécurité informatique - PSI »	http://www.univ-brest.fr/formation/formation-programme/master-gra-rech-informatique-specialite-reseaux-et-securite-des-systemes-informatiques-200756.kjsp
Université Technologique de Troyes	Master « Sécurité des systèmes d'information »	http://www.univ-brest.fr/formation/formation-programme/master-gra-rech-informatique-specialite-reseaux-et-securite-des-systemes-informatiques-200756.kjsp
Université de Valenciennes et du Hainaut-Cambresis	Master « Cyber-défense et sécurité de l'information - CSI »	http://www.univ-brest.fr/formation/formation-programme/master-gra-rech-informatique-specialite-reseaux-et-securite-des-systemes-informatiques-200756.kjsp
ENSICM	Ingénieur « Multimédia et sécurité des systèmes »	http://www.univ-brest.fr/formation/formation-programme/master-gra-rech-informatique-specialite-reseaux-et-securite-des-systemes-informatiques-200756.kjsp
EPITA	Ingénieur « Systèmes, réseaux et sécurité - SRS »	http://www.univ-brest.fr/formation/formation-programme/master-gra-rech-informatique-specialite-reseaux-et-securite-des-systemes-informatiques-200756.kjsp
EPIS	Programme Ingénieur Informatique - option Sécurité Informatique	http://www.univ-brest.fr/formation/formation-programme/master-gra-rech-informatique-specialite-reseaux-et-securite-des-systemes-informatiques-200756.kjsp
ESAP	Ingénieur « Informatique et réseaux, spécialité cybersécurité »	http://www.univ-brest.fr/formation/formation-programme/master-gra-rech-informatique-specialite-reseaux-et-securite-des-systemes-informatiques-200756.kjsp
ESIC	Master « Sécurité informatique »	http://www.univ-brest.fr/formation/formation-programme/master-gra-rech-informatique-specialite-reseaux-et-securite-des-systemes-informatiques-200756.kjsp
ESIS	Ingénieur parcours « Fondamental et Sécurité (SIC) »	http://www.univ-brest.fr/formation/formation-programme/master-gra-rech-informatique-specialite-reseaux-et-securite-des-systemes-informatiques-200756.kjsp
ESISLIC	Ingénieur « Architecture et sécurité des réseaux - ASR »	http://www.univ-brest.fr/formation/formation-programme/master-gra-rech-informatique-specialite-reseaux-et-securite-des-systemes-informatiques-200756.kjsp
ETNA-Alternance	Ingénieur « Architecture système réseaux et sécurité »	http://www.univ-brest.fr/formation/formation-programme/master-gra-rech-informatique-specialite-reseaux-et-securite-des-systemes-informatiques-200756.kjsp
EURECOM	Ingénieur de spécialisation en « sécurité des systèmes informatiques et des communications »	http://www.univ-brest.fr/formation/formation-programme/master-gra-rech-informatique-specialite-reseaux-et-securite-des-systemes-informatiques-200756.kjsp
IL3 Laval	Manager en ingénierie informatique (M2) option « Management de la sécurité des systèmes d'information (SSI) »	http://www.univ-brest.fr/formation/formation-programme/master-gra-rech-informatique-specialite-reseaux-et-securite-des-systemes-informatiques-200756.kjsp
INSA Centre Val de Loire	Ingénieur « Sécurité et technologies informatiques »	http://www.univ-brest.fr/formation/formation-programme/master-gra-rech-informatique-specialite-reseaux-et-securite-des-systemes-informatiques-200756.kjsp
INSA-CN	Master « Ingénierie informatique & Management - Sécurité informatique »	http://www.univ-brest.fr/formation/formation-programme/master-gra-rech-informatique-specialite-reseaux-et-securite-des-systemes-informatiques-200756.kjsp
ISIR-Université Blaise Pascal	Ingénieur « Réseaux et Sécurité Informatique »	http://www.univ-brest.fr/formation/formation-programme/master-gra-rech-informatique-specialite-reseaux-et-securite-des-systemes-informatiques-200756.kjsp
Supélec (Rennes)	Ingénieur « Systèmes d'information sécurisés »	http://www.univ-brest.fr/formation/formation-programme/master-gra-rech-informatique-specialite-reseaux-et-securite-des-systemes-informatiques-200756.kjsp
Telecom Lille	Ingénieur « Sécurité des réseaux et des systèmes »	http://www.univ-brest.fr/formation/formation-programme/master-gra-rech-informatique-specialite-reseaux-et-securite-des-systemes-informatiques-200756.kjsp
Telecom SudParis	Ingénieur « Sécurité des systèmes et des réseaux »	http://www.univ-brest.fr/formation/formation-programme/master-gra-rech-informatique-specialite-reseaux-et-securite-des-systemes-informatiques-200756.kjsp
Toulouse Ingénierie	Licence Pro « Sécurité et TLS-SEC »	http://www.univ-brest.fr/formation/formation-programme/master-gra-rech-informatique-specialite-reseaux-et-securite-des-systemes-informatiques-200756.kjsp

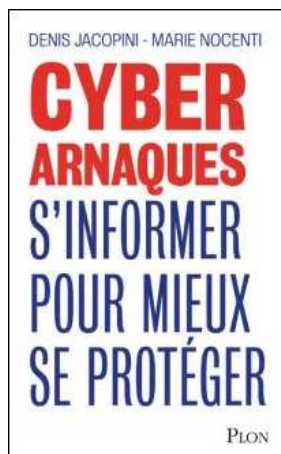
A voir aussi

• Formations Labellisées Serhmedu
• Profils métiers de la cybersécurité
[liste à suivre]

[block id="24761" title="Pied de page HAUT"]

CYBERARNAQUES - S'informer pour mieux se protéger (Le Livre)

Denis JACOPINI Marie Nocenti (Plon) ISBN : 2259264220



Denis Jacopini, expert judiciaire en informatique diplômé et spécialisé en cybercriminalité, raconte, décrypte et donne des parades contre toutes les cyberarnaqes dont chacun peut être victime.

Il est témoin depuis plus de 20 ans d'attaques de sites Internet, de piratages d'ordinateurs, de dépouillements de comptes bancaires et d'autres arnaques toujours plus sournoisement élaborées.

Parce qu'il s'est rendu compte qu'à sa modeste échelle il ne pourrait sensibiliser tout le monde au travers des formations et des conférences qu'il anime en France et à l'étranger, il a imaginé cet ouvrage afin d'alerter tous ceux qui se posent la question : Et si ça m'arrivait un jour ?

Plutôt que de présenter une longue liste d'arnaqes Internet recensées depuis plusieurs années, Denis Jacopini, avec la collaboration de Marie Nocenti, auteur du roman Le sourire d'un ange, a souhaité vous faire partager la vie de victimes d'arnaqes Internet en se basant sur des faits réels, présentés sous forme de nouvelles suivies de recommandations pour s'en prémunir. Et si un jour vous rencontrez des circonstances similaires, vous aurez le réflexe de vous méfier sans risquer de vivre la fin tragique de ces histoires et d'en subir les conséquences parfois dramatiques.

Pour éviter de faire entrer le loup dans votre bergerie, il est essentiel de le connaître pour le reconnaître !

Commandez sur Fnac.fr

<https://www.youtube.com/watch?v=lDw3kI7ra2s>

06/04/2018 A l'occasion de la sortie de son livre "CYBERARNAQUES : S'informer pour mieux se protéger", Denis JACOPINI répond aux questions de Valérie BENHAÏM et ses 4 invités : 7 Millions de victimes de la Cybercriminalité en 2010 (Symantec) 13,8 Millions de victimes de la Cybercriminalité en 2016 (Symantec) 19,3 Millions de victimes de la Cybercriminalité en 2017 (Symantec) Plus ça va moins ça va ? Peut-on acheter sur Internet sans risque ? Si le site Internet est à l'étranger, il ne faut pas y aller ? Comment éviter de se faire arnaquer ? Comment on fait pour renifler une arnaque sur Internet ? Comment avoir un coup d'avance sur les pirates informatiques ? Quelle est l'arnaque qui revient le plus souvent ? Denis JACOPINI vous répond sur C8 avec Valérie BENHAÏM et ses invités.

Commandez sur Fnac.fr

https://youtu.be/usg12zkRD9I?list=UUoHqj_HKcbzRuvIPdu3FktA

12/04/2018 Denis JACOPINI est invité sur Europe 1 à l'occasion de la sortie du livre "CYBERARNAQUES S'informer pour mieux se protéger"

Comment se protéger des arnaques Internet

Commandez sur amazon.fr



Je me présente : Denis JACOPINI. Je suis l'auteur de ce livre coécrit avec Marie Nocenti, romancière.

Pour ma part, je suis Expert de justice en informatique spécialisé en cybercriminalité depuis 1996 et en protection des Données à Caractère Personnel.

J'anime des formations et des conférences sur le RGPD et la Cybercriminalité pour aider les organismes à se protéger des pirates informatiques et à se mettre en conformité avec la réglementation autour du numérique (dont le RGPD : Règlement Général sur la Protection des Données).

Commandez sur [Fnac.fr](https://www.fnac.fr)

Source : *Formation et cybersécurité en France* | Agence nationale de la sécurité des systèmes d'information

Le cyber-espionnage, en tête

des menaces en 2017 ?

Denis JACOPINI



vous informe

Le cyber-
espionnage, en
tête des menaces
en 2017 ?

Selon Trend Micro, l'augmentation des ransomware et des attaques menées par des Etats constituent un risque croissant pour les infrastructures critiques.

La dernière étude menée par Trend Micro, soutient que 20 % des entreprises mondiales classent le cyber-espionnage comme la plus forte menace pour leur activité, 26 % luttant pour suivre et anticiper l'évolution rapide des différentes menaces. Aux Etats-Unis, 20 % ont déjà subi une attaque de ce type en 2016.

L'étude révèle que le cyber-espionnage arrive en tête des préoccupations de sécurité pour 2017, suivi par les attaques ciblées (17 %) et le phishing (16 %). Les entreprises situées en Italie (36 %), en France (24 %), en Allemagne (20 %) et aux Pays-Bas (17 %) sont celles qui craignent le plus le cyber-espionnage, ce qui s'explique notamment par la tenue d'élections dans chacun de ces pays cette année. Huit pays sur dix ont mentionné le caractère de plus en plus imprévisible des cybercriminels (36 %) comme étant le plus grand frein à la protection contre les cyber-menaces. Ils sont également 29 % à faire état de lacunes concernant la compréhension des dernières menaces, et 26 % à s'efforcer de suivre l'évolution rapide des menaces et la sophistication croissante des activités cybercriminelles. Selon l'étude, près des deux tiers (64 %) des entreprises avaient subi une cyber-attaque majeure « connue » au cours des 12 derniers mois. En moyenne, elles en avaient même connu quatre. Les menaces de type ransomware étaient de loin les plus courantes, 69 % des personnes interrogées indiquant avoir été attaquées au moins une fois au cours de la période. En réalité, seul un quart (27 %) des entreprises interrogées n'avait pas été ciblé par un ransomware.

Autre fait notable : à peine 10 % des entreprises pensent que les attaques de type ransomware constitueront une menace en 2017, alors que l'année 2016 a été marquée par une augmentation de 748 % de ces attaques, avec 1 milliard de dollars de pertes pour les entreprises à travers le monde. On estime que le nombre de ransomware va augmenter d'encore 25 % en 2017, s'attaquant à divers appareils tels que les téléphones portables, les objets connectés (IoT) et les dispositifs d'IoT industriel (IIoT)...[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.



[Contactez-nous](#)

Réagissez à cet article

Source : *Le cyber-espionnage, en tête des menaces en 2017* |

Alerte : Comptes Twitter piratés. Comment les pirates ont fait et comment vous en protéger ?



De nombreux comptes, dont celui du ministère français de l'Economie, ont été piratés, mercredi matin, par un message évoquant le référendum constitutionnel du 16 avril en Turquie.

« #Allemagne nazie #Pays-Bas nazis. Voici une petite claque ottomane pour vous. » Mercredi 15 mars au matin, de nombreux comptes Twitter de personnalités et d'institutions ont publié un message, débutant par une croix nazie, évoquant le référendum constitutionnel du 16 avril en Turquie.

Parmi les victimes de ce piratage massif et hautement politique se trouvent :

- Le Ministère français de l'Economie,
- Le journal économique Forbes,
- Le Monde,
- Le site d'Alain Juppé,,
- le magazine « Envoyé spécial »,
- L'Académie de Rennes,
- Reuters au Japon,,
- le compte de l'émission « Envoyé Spécial »,,
- Nike en Espagne,,
- Unicef USA,,
- la Philharmonie de Berlin,
- Comptes d'université américaine...



Le compte Twitter officiel de Bercy a été piraté mercredi 15 mars. (CAPTURE D'ÉCRAN)

Comment les pirates ont procédé

Pour réussir cette opération, le ou les pirates n'ont, a priori, pas eu recours à un système de détournement de mots de passe des comptes Twitter concernés. La faille provient, en fait, d'une « application tierce » : Twitter Counter, un outil payant et indépendant du réseau social. En échange d'une autorisation d'accès au compte, cette application propose aux entreprises et institutions des statistiques avancées, comme un suivi détaillé du nombre d'abonnés.

L'application Twitter Counter a confirmé, mercredi matin, le piratage de son service, et a annoncé le lancement d'une enquête interne. Dans un message posté sur le réseau social, l'entreprise rappelle qu'elle ne conserve pas les mots de passe de ses clients et assure qu'elle a désormais bloqué l'option qui lui permettait de poster des messages sur le compte de ses clients.

Cette méthode de piratage ne concerne malheureusement pas seulement les comptes Twitter d'importance. Si vous êtes un adepte du réseau social, vous avez sans doute déjà été tenté d'installer une application tierce vous permettant, par exemple, d'identifier les utilisateurs qui ont cessé de suivre votre compte. Celles-ci, comme Twitter Counter, ont de grandes chances de pouvoir publier des tweets en votre nom.

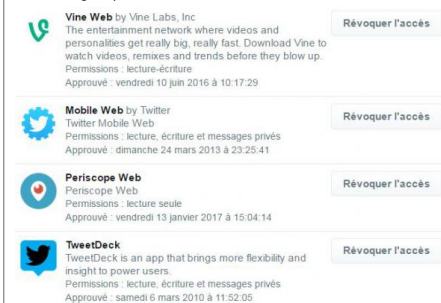
Comment savoir si votre compte est vulnérable

Pour vérifier l'identité des programmes tiers ayant accès à votre compte, rendez-vous dans la catégorie « Applications » des paramètres de Twitter. Vous trouverez une liste de tous les programmes tiers que vous avez installés, ainsi que les différents niveaux d'autorisations d'accès de ces applications à votre compte.

Si vous voyez l'application « Twitter Counter » dans cette liste, cliquez sur le bouton « Révoquer l'accès » en face d'elle.

Si certaines vous semblent farfelues ou peu sûres, vous pouvez également les signaler auprès de Twitter en cliquant sur « Signaler l'application » après avoir révoqué leur accès à votre compte.

Dans l'exemple ci-dessous, l'application Periscope est ainsi autorisée à lire uniquement des tweets, Vine à lire et à publier, et Tweetdeck à lire, publier, et accéder aux messages privés.



Notre avis

Je pense qu'il est anormal qu'une application tierce à Twitter comme « Twitter Counter » ait des droit d'écriture directement sur les comptes Twitter de ses abonnés ?

Pour ceux qui ne le savent pas, Twitter Counter permet d'analyser l'évolution de votre compte Twitter en « nombre de tweets, d'abonnés, de retweets et de mentions ». Pourquoi une telle application à imposé à ses utilisateurs de pouvoir écrire sur leur compte ? Un simple droit en lecture est suffisant pour connaître le nombre d'abonnés, de tweets, retweets...

Partez à la chasse aux applications intrusives en vous rendant dans :

Twitter > Paramètres et fonctionnalités > Applications

et n'hésitez pas à « Révoquer l'accès » pour chacune des applications suspectes.

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 téléphoniques, disques dur, e-mails, contenus, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Président de la DITEP - PPSM 000146)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



[Contactez-nous](#)

Réagissez à cet article

Source : *Twitter : comment Bercy et d'autres comptes officiels ont été piratés (et comment vous en protéger)*

Arnaques entre cybercriminels !



Les chercheurs de Kaspersky Lab ont découvert PetrWrap, une nouvelle famille de malware exploitant le module d'origine du ransomware Petya et distribuée via une plate-forme RaaS (Ransomware as a Service) pour mener des attaques ciblées contre des entreprises. Les créateurs de PetrWrap ont produit un module spécial qui modifie le ransomware Petya existant « à la volée », laissant les auteurs de ce dernier impuissants face à l'utilisation non autorisée de leur propre malware. Ce pourrait être le signe d'une intensification de la concurrence sur le marché souterrain du ransomware.

En mai 2016, Kaspersky Lab avait découvert le ransomware Petya, qui non seulement chiffre les données stockées sur un ordinateur mais écrase aussi le secteur d'amorce (MBR) du disque dur, ce qui empêche le démarrage du système d'exploitation sur les machines infectées. Ce malware est un modèle de RaaS (Ransomware as a Service), c'est-à-dire que ses créateurs proposent leur produit malveillant « à la demande », afin de le propager via de multiples distributeurs en s'octroyant un pourcentage des profits au passage. Pour s'assurer de recevoir leur part du butin, les auteurs de Petya ont inséré certains « mécanismes de protection » dans leur malware de façon à prévenir un usage non autorisé de ses échantillons. Les auteurs du cheval de Troie PetrWrap, dont les activités ont été détectées pour la première fois au début de 2017, sont parvenus à contourner ces mécanismes et ont trouvé un moyen d'exploiter Petya sans verser de redevance à ses auteurs.

Le mode de diffusion de PetrWrap reste à éclaircir. Après infection, PetrWrap lance Petya afin de chiffrer les données de sa victime, puis exige une rançon. Ses auteurs emploient leurs propres clés de chiffrement privées et publiques en lieu et place de celles fournies avec les versions « standard » de Petya. Cela leur permet d'exploiter le ransomware sans avoir besoin de la clé privée d'origine pour décrypter la machine de la victime, dans le cas où cette dernière paie la rançon...[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 DRETF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



[Contactez-nous](#)

Réagissez à cet article

Source : PetrWrap : des cybercriminels volent le code de ransomware d'autres criminels Le nouveau ransomware mène des attaques ciblées contre des entreprises – Global Security Mag Online

Google, ou la révolution transhumaniste via le Big Data



A l'occasion de la sortie du livre de Christine Kerdellant Dans la Google du loup, Éric Delbecque décrypte le projet de « fusion » entre le vivant et le digital porté par le géant de l'informatique américain.

Christine Kerdellant a relevé un beau défi *Dans la Google du loup* (Plon)! Elle met le doigt là où Google pose véritablement problème, à savoir sur la révolution anthropologique du transhumanisme... Pour ce qui concerne sa participation à la société de surveillance globale que fabriquent un certain nombre d'acteurs publics et privés, l'affaire est entendue depuis des années... Sous l'administration Obama, les dirigeants de Google se rendirent à la Maison-Blanche 230 fois! Ils confirmèrent en 2013 que les agences gouvernementales de l'Oncle Sam les sollicitaient annuellement – dans le cadre du Patriot Act – pour surveiller 1000 à 2000 comptes. En janvier 2015, la firme vedette du Web a reconnu avoir fourni au Ministère de la Justice américain l'intégralité des comptes Google de trois membres de WikiLeaks.

Nous assistons à l'émergence d'une société de surveillance de masse dont l'État n'est pas le centre mais l'un des maillons.

Il paraît dès lors compliqué de penser qu'une idéologie sécuritaire explique à elle seule l'extension de l'ombre de Big Brother sur le monde. Les géants du numérique du secteur privé (les GAFA: Google, Amazon, Facebook, Apple) participent largement à la manœuvre, plus ou moins volontairement (pas pour des raisons politiques, mais économiques). Nous assistons à l'émergence d'une société de surveillance de masse dont l'État n'est pas le centre mais l'un des maillons. Sa stratégie en matière de renseignement doit se lire comme un fragment d'un système cybernétique (au sens de science du contrôle) beaucoup plus vaste, où le capitalisme financier californien et numérique occupe une place décisive. Séparer ce dernier du complexe militaro-sécuritaro-industriel de l'Oncle Sam devient de plus en plus difficile, voire hasardeux.

L'intérêt plus décisif du livre de Christine Kerdellant est ailleurs. Il explore de manière très accessible et percutante le cœur du projet Google, ou plutôt sa signification philosophique profonde. Derrière les joyeux Geeks de la Silicon Valley s'exprime la volonté de réifier l'humanité, de l'enchaîner à une raison calculante. Cette dernière va nous émanciper nous répète-t-on, nous libérer – via le Big Data – des limites de notre condition, nous délivrer de la mort et transformer notre existence en un jardin de fleurs. Mais lorsqu'on choisit d'examiner de plus près les conséquences des propositions de Google, on découvre une perspective d'avenir moins réjouissante...[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.



[Contactez-nous](#)

Réagissez à cet article

Source : Google, ou la révolution transhumaniste via le Big

Développement de l'outil PIA (Privacy Impact Assessment, étude d'impact sur la vie privée) de la CNIL



Date remise des offres: Mercredi, 29 mars, 2017...[Lire la suite]

Denis JACOPINI anime des **conférences, des formations** sur la mise en conformité CNIL, des formations sur la protection des données Personnelles et est régulièrement invité à des **tables rondes en France et à l'étranger** pour sensibiliser les décideurs et les utilisateurs aux **obligations et moyens de se mettre en conformité avec le RGPD, futur règlement européen relatif 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).

Plus d'informations sur notre page formations.



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.



[Contactez-nous](#)

Réagissez à cet article

RGPD : Ce qui va changer pour les professionnels de santé

 Denis JACOPINI FR ? vous informe	RGPD : Ce qui va changer pour les professionnels de santé
---	---

Fin des déclarations Cnil, demandes de consentement et sanctions renforcées, une nouvelle réglementation européenne* va venir chambouler la gestion des données personnelles en magasin. En tant que commerçants et professionnels de santé, vous collectez et transmettez des données relatives à vos clients. Le GDPR (General Data Protection Régulation) devra donc s'appliquer à votre point de vente. Zoom sur ce qui change dès le 25 mai 2018.

Registre des traitements et désignation d'un délégué à la protection des données

Quotidiennement vous gérez, stockez et envoyez les données de santé de vos clients que ce soit pour la pratique du tiers payant ou effectuer une commande auprès de vos fournisseurs. Identité, numéro de Sécurité sociale, facturation, prescription... vous êtes amenés à traiter des données personnelles, qui doivent actuellement faire l'objet d'une déclaration auprès de la Cnil (Commission nationale de l'informatique et des libertés). Mais bientôt, vous n'aurez plus besoin de cette formalité préalable.

En effet, le règlement européen sur la protection des données personnelles repose sur une logique de conformité, dont les acteurs seront désormais responsables. En d'autres termes, le poids de la procédure administrative va être transféré de la Cnil. **Dès le 25 mai 2018, vous devrez être en possession et tenir un « registre des traitements mis en œuvre ».** Ce dernier devra notamment spécifier :

- les catégories de données traitées ;
- la finalité ;
- les différents destinataires ;
- la durée de conservation.

« Ce registre informatisé permettra au professionnel de se ménager des preuves vis-à-vis de la Cnil. Il prouve son adhésion à un code de conduite, explique Maître Cécile Vernudachi, avocate au Barreau de Paris. Les grandes enseignes pourront également désigner un délégué à la protection des données, qui deviendra le point de contact avec la Cnil et un véritable « chef d'orchestre » de la conformité en matière de protection des données au sein de son organisme. Dans les plus petites structures, ce ne sera pas une obligation », précise-t-elle.

Consentement renforcé et transparence

Le règlement européen impose également la mise à disposition d'une information claire, intelligible et aisément accessible à vos clients. Il définit en ce sens l'expression du consentement : **« les utilisateurs doivent être informés de l'usage de leurs données et doivent en principe donner leur accord pour le traitement de leurs données, ou pouvoir s'y opposer.** La charge de la preuve du consentement incombe au responsable de traitement. La matérialisation de ce consentement doit être non ambiguë », précise le document.

En d'autres termes, avant chaque devis ou chaque vente, vous êtes tenus d'obtenir le consentement de votre porteur pour pouvoir traiter et transmettre ses données personnelles. « Concernant la correction, seul le patient peut donner son accord pour la transmission de cette donnée, souligne Maître Vernudachi. **Son consentement doit obligatoirement être écrit.** Dans le cadre de l'exécution d'un contrat, il n'y a alors plus de restriction. Toutefois, il est interdit d'utiliser cette information pour la vendre à un tiers ou à des fins marketings et commerciales ».

Spécificité pour les moins de 16 ans :

Pour la première fois, la législation européenne comporte des dispositions spécifiques pour les moins de 16 ans. L'information sur les traitements de données les concernant doit être rédigée en des termes clairs et simples, que l'enfant peut aisément comprendre. Le consentement doit être recueilli auprès du titulaire de l'autorité parentale. Devenu adulte, le consentement donné sur un traitement doit pouvoir être retiré et les données effacées.

Des sanctions encadrées et graduées

Les responsables de traitement, autrement dit les dirigeants ou chef d'entreprise, les plateformes de services et les complémentaires santé, peuvent enfin faire l'objet de **sanctions administratives importantes en cas de non-conformité au nouveau règlement.** Les autorités de protection peuvent notamment :

- prononcer un avertissement ;
- mettre en demeure l'entreprise ;
- limiter temporairement ou définitivement un traitement ;
- suspendre les flux de données ;
- ordonner de satisfaire aux demandes d'exercice des droits des personnes ;
- ordonner la rectification, la limitation ou l'effacement des données.

S'agissant des amendes dans le cas d'une entreprise, elles peuvent s'élever de 2% à 4% du chiffre d'affaires annuel mondial, en fonction de la catégorie de l'infraction.

Notons que selon l'étude « Crossing the Line » du cabinet KPMG**, les Français sont 2ème sur le podium des consommateurs les plus vigilants quant au traitement de leurs données personnelles. Aussi, le règlement européen sera en vigueur dès le 25 mai 2018. Il vous faut donc être vigilant et vous y préparer dès maintenant !

***Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016**

****étude publiée en novembre 2016**

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



[Contactez-nous](#)



Réagissez à cet article

Source : *Ce qui va changer dans les magasins pour le traitement des données personnelles* | Acuité

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.



[Contactez-nous](#)

Réagissez à cet article

Les messages de WhatsApp peuvent être facilement lus par la CIA



L'organisation WikiLeaks a reçu une importante base de données révélant les techniques de cyber-surveillance et de piratage de la CIA. Selon ces informations l'agence de renseignement américaine peut facilement accéder aux messageries, y compris WhatsApp et Telegram.

La Central Intelligence Agency (agence centrale de renseignement, CIA) est capable de contourner le cryptage de certaines applications populaires de messagerie, y compris WhatsApp et Telegram, selon les documents publiés par WikiLeaks aujourd'hui.

« Ces techniques permettent à la CIA de contourner le cryptage de WhatsApp, de Signal, de Telegram, de Wiebo, de Confide et de Cloackman en piratant les téléphones « intelligents » sur lesquels ces applications sont installées et de collecter les enregistrements audio et les messages avant que le cryptage ne soit activé », informe le document publié par WikiLeaks.



© FLICKR/ VIN CROSBIE

Espionnage en plein ciel: Air France dans le viseur des services secrets US et UK

Cette fuite a semé le trouble parmi les utilisateurs de WhatsApp, dont beaucoup ont réagi avec virulence aux nouvelles selon lesquelles l'application aurait commencé à partager des données avec Facebook l'année dernière.

La révélation de WikiLeaks suggère que les espions du gouvernement américain ont eu accès aux messages des utilisateurs malgré la mise en place d'un cryptage de bout en bout, qui est pourtant conçu pour protéger la confidentialité des utilisateurs.

Cependant, il se pourrait que la CIA n'ait pas piraté les applications elles-mêmes, mais craqué les outils de cryptage en attaquant les smartphones des utilisateurs.



© AFP 2017 SAUL LOEB

Wikileaks publie plus de 8.700 documents concernant les capacités de cyber-espionnage de la CIA

Le site de Julian Assange, WikiLeaks, a annoncé le 7 mars la publication d'une nouvelle série de fuites sur la CIA sous le code « Vault 7 » qui sera, d'après le communiqué de l'organisation, la plus importante publication de documents confidentiels sur l'agence.

La première partie des fuites, intitulée « Year Zero », comprend 8 761 documents et fichiers qui ont été collectés sur un réseau isolé de haute sécurité du Centre Cyber Intelligence (département de la CIA) à Langley, dans l'État de Virginie.

Les fuites de « Year Zero » révèlent les capacités de piratage de la CIA contre un large éventail de produits américains et européens, notamment Windows, iPhone, Android et même les téléviseurs Samsung, qui ont été transformés en microphones cachés par le programme Weeping Angel...[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.



Contactez-nous

Réagissez à cet article

Source : *Les messages de WhatsApp peuvent être facilement lus par la CIA*