Les Français plus vulnérables aux virus propagés par clé USB

Les Français plus vulnérables aux virus propagés par clé USB

Les logiciels malveillants s'adaptent et les menaces en matière de cybersécurité varient d'un pays à l'autre, révèle une étude menée par la société de sécurité informatique Avira.

Vols de mots de passe, chevaux de Troie, ver, applications indésirables… En matière de cybersécurité, chaque pays «cultive» son défaut et son logiciel malveillant : tel est le principal enseignement d'une étude publiée lundi par la société de sécurité informatique Avira.
Le talon d'Achille de la France – l'un des cinq pays étudiés avec les Etats-Unis, le Royaume-Uni, l'Allemagne et l'Italie – se trouverait… dans la clé USB. Infestée de «vers».
Avira a en effet remarqué que le logiciel malveillant le plus fréquent en France était un ver, ou *worm* en anglais, de son nom technique Verecno.Gen. Son mode de contamination favori ? L'utilisation de clés USB. Celui-ci «n'est pas sans risque, rappelle la société dans son étude. Le ver Verecno est ainsi capable de se propager automatiquement dès que la clé USB est insérée dans l'appareil. Savez-vous d'où vient la clé USB qui vous est tendue ?» Avira délivre un conseil particulier aux Français : «Ne sur-socialisez pas».

A chaque pays son point faible

Les utilisateurs des Etats-Unis sont davantage vulnérables aux chevaux de Troie modifiant le comportement des systèmes d'exploitation Windows de leurs ordinateurs, les Allemands aux kits d'exploitation prospérant sur les défauts de mise à jour, les Italiens aux vols de mots de passe via les emails et les Britanniques au téléchargement d'applications indésirables.

leparisien.fr

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 : *Cybersécurité : les Français plus vulnérables aux virus propagés par clé USB – Le Parisien*

Le ministère de la Défense confirme l'augmentation des tentatives de piratage informatique

Le ministère de la Défense confirme l'augmentation des tentatives de piratage informatique

---

L'armée sud-coréenne a récemment été la cible de tentatives accrues de piratage informatique sur fond de relations tendues avec la Chine et de comportement belliqueux de la Corée du Nord, a fait savoir ce mardi le porte-parole du ministère de la Défense Moon Sang-gyun.
«Récemment, les tentatives d'intrusion dans (notre) système informatique se sont quelque peu accrues», a déclaré le porte-parole lors d'un point de presse, tout en notant qu'il n'y a eu aucun dégât subi. Il n'a toutefois pas précisé l'origine des cybermenaces évoquées.
Plus tôt dans la journée, un quotidien sud-coréen a rapporté que le nombre de cyberattaques contre l'armée sud-coréenne a fortement augmenté depuis que celle-ci a acquis le mois dernier un terrain de golf du groupe Lotte, dans le sud-est du pays, pour le déploiement du système de défense antimissile à haute altitude THAAD (Terminal High Altitude Area Defense) des Etats-Unis. La Chine est fortement opposée au plan des deux pays alliés de renforcer leur capacité à intercepter les missiles nord-coréens.
Le nombre de tentatives de piratage informatique contre le réseau informatique de l'armée a été de 44 entre les 9 et 15 mars, selon le rapport. Moon n'a pas confirmé ce chiffre.
Il a écarté les inquiétudes sur l'éventuelle vulnérabilité de l'intranet de l'armée, en soulignant qu'il est complètement «séparé» du serveur Internet.
L'intranet de l'armée a subi pour la première fois une cyberattaque en septembre dernier dont le Nord serait également à l'origine.
lsr@yna.co.kr

Réagissez à cet article

Source : *Le ministère de la Défense confirme l'augmentation*

des tentatives de piratage informatique | Agence de presse Yonhap

---

Les Banques organisent la riposte au cybercrime sur smartphone

	**Les Banques organisent la riposte au cybercrime sur smartphone**

Les banques songent à intégrer des logiciels dans leurs applications pour sécuriser les smartphones de leurs clients.

La pédagogie est la clef pour décourager les clients qui seraient tentés de télécharger des applications sur des « Stores Android » non officiels, de s'aventurer à débloquer leur smartphone ou encore de se connecter sur leur application bancaire depuis le réseau wi-fi d'un café, non sécurisé. *« La carte bancaire a beau être sécurisée, si le client divulgue son code, nos efforts de sécurisation sont vains. Il en va de même pour les usages sur le mobile , il y a des principes élémentaires de sécurité à respecter »,* souligne Marc Zanoni, directeur sécurité des systèmes d'information du groupe BPCE.

Convaincre les clients

Comme pour la banque en ligne, les établissements veulent donc convaincre leurs clients de la nécessité de sécuriser leur smartphone. Certains les encouragent à télécharger des antivirus qui détectent les logiciels malveillants présents dans le téléphone et d'autres, comme Société Générale, promeuvent l'enregistrement du téléphone de leurs clients pour que la banque puisse vérifier, à chaque transaction, qu'il s'agit bien d'une demande officielle et non d'un pirate qui aurait capté des codes d'accès.
Ces outils restent optionnels car *« toute la difficulté est de garantir la sécurité sans dégrader l'expérience client. Nous ne voulons pas imposer de nouvelles pratiques brutalement »,* explique un autre responsable Sécurité d'une grande banque française. Ce qui veut dire que *« les banques vont devoir agir à la place de leurs clients car ils n'auront pas la maturité nécessaire sur ces questions »,* estime Clément Saad, fondateur de Pradeo, une jeune pousse spécialisée dans la cybersécurité…[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

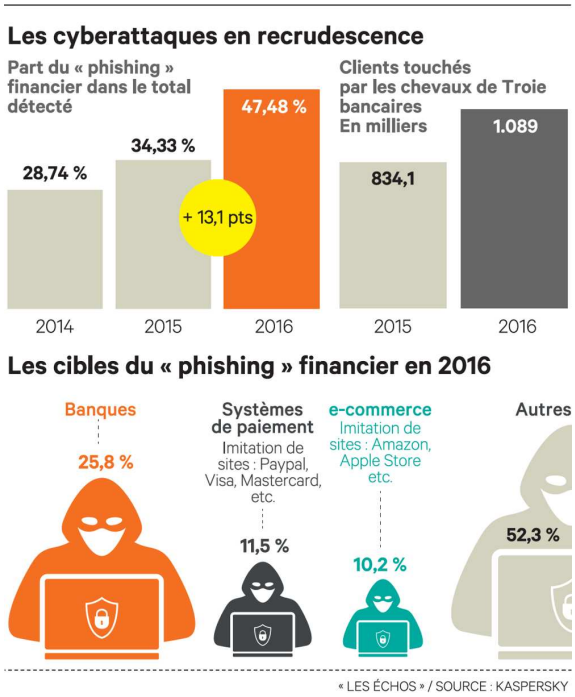
Source : *La riposte au cybercrime sur smartphone s'organise, Banque – Assurances*

Les pirates informatiques menacent les clients des banques

	Les pirates informatiques menacent les clients des banques

---

Les opérations de « phishing » ciblant les clients des banques augmentent. La montée en puissance de la banque mobile ouvre un nouveau terrain de jeu pour les cybercriminels.



En 2016, les cyberpirates ont marqué les esprits en parvenant, à plusieurs reprises, à déjouer les systèmes de sécurité des banques membres du réseau interbancaire SWIFT. Ces vastes opérations aux perspectives de gains étourdissantes n'ont pour autant pas remplacé les cyberattaques traditionnelles qui visent directement les clients des banques.

« Les plus petits groupes de cybercriminels ciblent toujours plus massivement les clients particuliers, petites ou moyennes entreprises avec des logiciels malveillants disponibles sur la Toile : après deux ans de baisse du nombre de clients attaqués, nous avons détecté une hausse significative du nombre de victimes parmi nos clients en 2016 », explique le spécialiste de la sécurité informatique Kaspersky dans son rapport annuel sur les services financiers.

Le « hameçonnage » progresse

Dans le détail, les opérations de « phishing » , c'est-à-dire l'envoi de courriels frauduleux à des clients pour obtenir leurs données de carte bancaire ou d'accès à leur compte en ligne, continuent de se développer. En 2016, la part des « phishings » financiers dans le total des e-mails frauduleux détectés par Kaspersky a progressé de plus de 13%. Les banques restent les principales victimes de ces méthodes qui dirigent les clients peu vigilants vers des sites mimant ceux des établissements.

En 2016, les banques ont été visées par près de 26% des e-mails financiers frauduleux, contre 10% à 11% pour les systèmes de paiements alternatifs et les e-commerçants. Chez Société Générale, l'équipe chargée de fermer les faux sites du groupe qui voient le jour sur la Toile en recense ainsi « *des centaines chaque mois et les chiffres augmentent* », indique un proche du groupe.

Chevaux de Troie

Autre menace qui se renforce pour les consommateurs : les chevaux de Troie bancaires qui se glissent dans les systèmes d'exploitation des clients et captent les données qui ouvrent l'accès aux espaces bancaires en ligne. En 2016, Kaspersky observe une hausse de 30,5 % de ces attaques dans le monde. « *Plus d'un million de clients ont été touchés, un chiffre qui croît avec le développement de la banque en ligne et de la banque mobile* », explique David Emm, Principal Security Researcher chez Kaspersky Lab…[lire la suite]

Sharon Wajsbrot, Les Echos

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 : *Cybersécurité : menace accrue pour les clients des banques, Banque – Assurances*

WhatsApp et Telegram corrigent des vulnérabilités importantes

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.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

Source : *WhatsApp et Telegram corrigent des vulnérabilités importantes – Gridam*

Formations en cybersécurité en France

À titre indicatif, voici la liste des formations en cybersécurité délivrant un titre reconnu par l'État (ministère en charge de l'enseignement supérieur ou CNCP) de niveau équivalent à Bac+3 (licence professionnelle) jusqu'à Bac+5 (master, ingénieur).

Cette liste de formations a vocation à informer les étudiants sur l'ensemble des programmes accessibles. Ne figurent dans cette liste ni la formation continue, ni les titres non reconnus officiellement par l'État (DU, masters spécialisés, BADGE, etc.).
Les éléments fournis ci-dessous sont issus d'une récolte de données multiples et éparses dans l'ensemble des établissements d'enseignement supérieur en France. Cette liste n'est plus maintenue et sera supprimée en juillet 2027.

En savoir plus sur SecNumedu, le label de formations initiales en cybersécurité de l'enseignement supérieur

FORMATIONS RECENSÉES DE NIVEAU LICENCE

NOM ETABLISSEMENT	NOM FORMATION	SITE INTERNET
Cnam Bretagne	Licence Pro « Analyste en Sécurité des Systèmes Télécoms Réseaux et Informatiques » ASSTRI	http://cnamsecuritedefense.fr/formation-securite-telecoms-reseaux/
Université d'Aix-Marseille	Licence Pro « Administration et sécurité des réseaux d'entreprises »	http://iut.univ-amu.fr/diplomes/licence-professionnelle-reseaux-telecommunications-specialite-administration-securite
Université d'Artois	Licence Pro « Systèmes informatiques et logiciel – Sécurité informatique »	http://formations.univ-artois.fr/cdm33rc2/ws7_cmd=getFormation&_oid=FR_RNE_0623957F_FR_L3LSEIN291&_redirect=voir_fiche_programS_lang=fr-FR&_onglet=Description
Université de Clermont-Ferrrand 1	Licence Pro « Administration et Sécurité des Réseaux »	http://iutweb.u-clermont1.fr/xfTest?xml/formation?idFormation=16824
Université de Grenoble Joseph Fourier	Licence Pro « Réseaux Sans Fil et Sécurité »	https://iut1.ujf-grenoble.fr/formation-et-metier/licence-professionnelle/reseaux-et-telecommunications
Université de Grenoble Pierre Mendès France	Licence Pro « Administration et Sécurité des réseaux »	http://www.iut-valence.fr/licence-professionnelle-asur
Université de Haute-Alsace	Licence Pro « Administration et Sécurité des réseaux »	http://www.iutcolmar.uha.fr/fr/LP-RT-ASUR-260.html
Université de la Réunion	Licence Pro « Réseaux Sans Fil et Sécurité »	http://www.iut-lareunion.fr/licences/reseaux-a-telecommunications
Université de la Rochelle	Licence Pro « Administration et sécurité des réseaux »	http://www.iut-larochelle.fr/licences-professionnelles/lp-administration-et-securite-des-reseaux
Université de Valenciennes et du Hainaut Cambrésis	Licence Pro « Collaborateur de Défense et Anti Intrusion des Systèmes Informatiques (CDAISI) »	http://formations.univ-valenciennes.fr/cdm/program/FR_RNE_0593279U_FR_SOF-5899
Université de Montpellier 2	Licence Pro « Administration et sécurité des réseaux »	http://www.iutbeziers.univ-montp2.fr/licence-pro-reseaux-et-telecoms.html
Université de Lorraine	Licence Pro « Réseaux Sans Fil et Sécurité »	http://iutnb.univ-lorraine.fr/index.php?op=lbaccplus3/lp_rt_reseaux.htm
Université de Nantes	Licence Pro « Administration et sécurité des réseaux »	http://www.iutlaroche.univ-nantes.fr/70407600/0/fiche___formation/&RH=IUTRY_FR1
Université Paris Est Créteil Val de Marne	Licence Pro « Réseaux informatiques, mobilité, sécurité (R3MS) »	http://www.u-pec.fr/pratiques/universite/formation/licence-professionnelle-reseaux-informatiques-mobilite-securite-rims-641083.kjsp
Université Paris 13	Licence Pro « Administration et Sécurité en Réseaux »	http://www.iutv.univ-paris13.fr/formations/licences-pro/reseaux-et-telecommunications.html
Université de Paris Sud	Licence Pro « Sécurité des Réseaux et Systèmes informatiques »	http://www.iut-orsay.u-psud.fr/fr/formations/licences_professionnelles/info_lp_srsi.html
Université de Rennes 1	Licence Pro « Administration et Sécurité des Réseaux »	http://sfc.univ-rennes1.fr/informatique/lp_administration-securite-reseaux.html#.U-R2OVRX6lB
Université de Rouen	Licence Pro « Administration Sécurité des Réseaux »	http://iutrouen.univ-rouen.fr/licence-professionnelle-administration-et-securite-des-reseaux-279942.kjsp
Université de Toulouse 2	Licence Pro « Réseaux Sans Fil et Sécurité »	http://www.univ-tlse2.fr/accueil/formation-insertion/decouvrir-nos-formations/licence-professionnelle-reseaux-sans-fil-et-securite-885.kjsp
Université de Tours	Licence Pro « Qualité – Sécurité des Systèmes d'Information »	http://iut-blois.univ-tours.fr/formations/qualite-securite-des-systemes-d-information-92850.kjsp
Université de Versailles Saint-Quentin	Licence Pro « Administration et Sécurité des Réseaux »	http://www.uvsq.fr/licence-professionnelle-metiers-des-reseaux-informatiques-et-telecommunications-parcours-administration-et-securite-des-reseaux-341092.kjsp?RH=1271771445917
Université de Pau et des Pays de l'Adour	Licence Pro « Administration et Sécurité des Réseaux »	http://iutpa.univ-pau.fr/live/RT/LP/LP+ASUR
Université de Bordeaux 1	Licence Pro « Administration et Sécurité des Réseaux »	http://www.univ-bordeaux.fr/formations/programme.jsp?f=0&t=3000&p=2213
Université des Antilles et de la Guyane	Licence Pro « Administration et Sécurité des Réseaux »	http://sut.univ-ag.fr/formations/licences-professionnelles/lp-asur/

FORMATIONS RECENSÉES DE NIVEAU MASTER

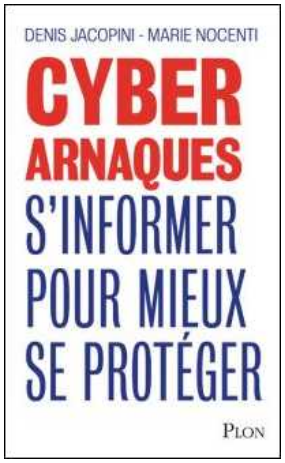
NOM ETABLISSEMENT	NOM FORMATION	SITE INTERNET
Université de Basse Normandie	Master « Réseaux et sécurité des systèmes informatiques »	http://www.unicaen.fr/formations/formations-proposees/master-pro-rech-informatique-specialite-reseaux-et-securite-des-systemes-informatiques-388756.kjsp
Université de Bordeaux 1	Master « Cryptologie et sécurité informatique »	http://www.math.u-bordeaux1.fr/~gzemor/dossier_CSI/
Université de Bretagne Sud (ENSIBS)	Ingénieur « Management et Ingénierie de sécurité des systèmes – cyberdéfense »	http://www-ensibs.univ-ubs.fr/devenir-ingenieur-en-cyberdefense-debouches-356662.kjsp?RH=1351525595668&RF=1351525595668
Université Grenoble Alpes et Grenoble-INP/Ensimag	Master « Cryptologie, sécurité et codage de l'information »	http://www-fourier.ujf-grenoble.fr/enseignement/spip.php?rubrique19
Université Grenoble Alpes	Master « Sécurité, audit, informatique légale – SAFE »	http://www.ujf-grenoble.fr/formation/diplomes/masters/domaine-sciences-technologies-sante/master-mention-mathematiques-informatique-specialite-securite-audit-informatique-legale-safe-p-838102.htm
Université Grenoble Alpes et Grenoble-INP/Ensimag	Master « Cybersecurité »	http://cybersecurity.imag.fr/
Université de Limoges	Master « Sécurité de l'Information et Cryptologie – CRYPTIS »	http://www.cryptis.fr/
Université de Lorraine (Mines Nancy, Telecom Nancy, ENSEM)	Master « Security of Computer Systems »	http://www.mines-nancy.univ-lorraine.fr/content/master-science-msc-security-computer-systems
Université de Lorraine	Master « Services, sécurité des systèmes et des réseaux »	http://msm.univ-lorraine.fr/content/master-informatique-ssr
Université de Lorraine	Master « Sécurité des systèmes d'information et de communication – SSIC »	https://formations.univ-lorraine.fr/fr-FR/fiche/presentation/UL-PROG2654/UL-PROG3211
Université de Lyon 1	Master SAFIR, parcours « Sécurité des systèmes informatiques en finance et en assurance – S2IFA »	http://isfa.univ-lyon1.fr/parcours_S2IFA
Université de Lyon 2	Master « Organisation et protection des systèmes et des réseaux – OPSIE »	http://www.univ-lyon2.fr/master-informatique-specialite-informatique-decisionnelle-et-statistique-opsie-264018.kjsp
Université de Nice Sophia Antipolis	Ingénieur « CryptograAphie, Sécurité, et vie Privée dans les Applications et Réseaux »	http://www.polytechnice.fr/informatique/page251.html
Université de Paris 8, en partenariat avec Paris Diderot (Paris 7)	Master « Mathématiques fondamentales et protection de l'information »	https://www.univ-paris8.fr/Master-Mathematiques-pour-la-protection-de-l-information
Université de Paris-Diderot (Paris 7) — en partenariat avec Paris 8	Master « Mathématiques, Informatique et applications à la Cryptologie – MIC »	http://www.math.univ-paris-diderot.fr/formations/masters/mic/index
Université de Paris-Est Créteil (Paris 12)	Master « Sécurité des systèmes informatiques »	http://www.lacl.fr/ens/master.html
Université de Poitiers	Master « Management des risques informationnels et industriels »	http://irisaf.univ-poitiers.fr/formation/master-management-des-risques-des-systemes-d-information/master-professionnel-et-recherche-sciences-technologies-sante-mention-gestion-des-risques-specialite-management-des-risques-des-systemes-d-information-11079.kjsp
Université de Reims Champagne-Ardenne	Master spécialité informatique, parcours « Administration et sécurité des réseaux »	http://www.master-informatique.net
Université de Rennes 1	Master « Sécurité des Systèmes d'Information – ISTIC »	http://etudes.univ-rennes1.fr/masterInformatique/themes/SecondeAnnee/Specialites/SSI
Université de Rennes 1, Université de Bretagne Sud, Université de Bretagne Occidentale, ENS Rennes, ENIB, ENSTA Bretagne, INSA Rennes, CentraleSupélec, Télécom Bretagne	Master « Sécurité des contenus et des infrastructures informatiques »	http://master.irisa.fr/index.php/fr/parcoursprog-fr/parcours-rennes-3-fr
Université de Rouen	Master « Sécurité des Systèmes Informatiques (SSI) »	https://dpt-info-sciences.univ-rouen.fr/index.php/accueil-mssi
Université de Valenciennes	Master « Informatique, réseaux et sécurité – IRS »	http://formations.univ-valenciennes.fr/cdm/program/FR_RNE_0593279U_FR_SOF-7415
Université de Versailles-Saint-Quentin	Master « Sécurité des contenus, des réseaux, des télécommunications et des systèmes – SeCReTS »	http://www.master-secrets.uvsq.fr/
Université d'Orléans	Master « Informatique Nomade, intelligence et sécurité »	http://formation.univ-orleans.fr/fr/formation/offre-de-formation/master-lmd-XR/sciences-technologies-sante-STS/master-informatique-specialite-informatique-nomade-intelligence-et-securite-finalite-professionnelle-et-recherche-program-sciesf2-502-2.html
Université du Havre	Master « Systèmes informatiques, Réseaux et Sécurité – MATIS »	http://matis.univ-lehavre.fr/
Université Pierre et Marie Curie (Paris 6) — avec l'AFTI	Master « Informatique, spécialité SFPN, filière sécurité informatique — MSI »	http://www-master.ufr-info-p6.jussieu.fr/lmd/specialite/sfpn/
Université Technologique de Troyes	Master « Sécurité des systèmes d'information »	http://www.utt.fr/fr/formation/master-en-sciences—technologies—sante/specialite-ssi.html
Université de Valenciennes et du Hainaut-Cambrésis	Master « Cyber-défense et sécurité de l'information – CDSI »	http://formations.univ-valenciennes.fr/cdm/program/FR_RNE_0593279U_FR_SOF-15674
ENSICAEN	Ingénieur « Monétique et sécurité des systèmes »	https://www.ensicaen.fr/formations/masteres-specialises-cpa/masteres-monetique-et-transactions-securisees/
EPITA	Ingénieur « Systèmes, réseaux et sécurité – SRS »	http://srs.epita.fr/
EPSI	Programme Ingénierie informatique – option Sécurité Informatique	http://www.epsi.fr/Programmes/Programme-Ingenierie/Ingenierie-5eme-annee
ESAIP	Ingénieur « Informatique et réseaux, spécialité cybersécurité »	http://www.esaip.org/formations/ingenieur-informatique
ESGI	Mastère « Sécurité informatique »	http://www.esgi.fr/master-informatique/master-securite-informatique.html
ESIEA	Ingénieur parcours « Fondamentals of Security (SEC) »	http://www.esiea.fr/formation-ingenieurs/majeures-ecole-ingenieurs/
ESIGELEC	Ingénieur « Architecture et sécurité des réseaux – ASR »	http://www.esigelec.fr/fr/dominantes
ETNA-Alternance	Ingénieur « Architecte système réseaux et sécurité »	http://www.etna-alternance.net/formation-2e-annee.aspx
EURECOM	Ingénieur de spécialisation en « sécurité des systèmes informatiques et des communications »	http://www.eurecom.fr/fr/les-formations/ingenieur-de-specialisation/securite-des-systemes-informatiques-et-des-communications
IIA Laval	Manager en ingénierie informatique (M2I) option « Management de la sécurité des systèmes d'information (MSSI) »	http://iia-laval.fr/ecole-superieure-en-informatique/l3m1m2-diplome-m2i/bac5-diplome-m2i/
INSA Centre Val de Loire	Ingénieur « Sécurité et technologies informatiques »	http://www.insa-centrevaldeloire.fr/formation/securite-et-technologies-informatique
IONIS-STM	Master « Ingénierie informatique & Management : Sécurité informatique »	http://ionis-stm.com/master-securite-informatique.aspx
ISIMA-Université Blaise Pascal	Ingénieur « Réseaux et Sécurité Informatique »	http://www.isima.fr/f5-reseaux-et-securite/
Supélec (Rennes)	Ingénieur « Systèmes d'information sécurisés »	http://www.rennes.supelec.fr/ren/fi/sis/
Télécom Lille	Ingénieur « Sécurité des réseaux et des systèmes »	http://www.telecom-lille.fr/specialisations-sciences-et-technologies
Télécom SudParis	Ingénieur « Sécurité des systèmes et des réseaux »	http://www.telecom-sudparis.eu/p_fr_formations-post-grade_MS_1178.html?idm=65
Toulouse Ingénierie	Ingénieur « TLS-SEC »	http://tls-sec.github.io/tls-sec/

À voir aussi

- Formations labellisées SecNumedu
- Profils métiers de la cybersécurité
(Lien ne mène)

[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 cyberarnaques 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'arnaques 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'arnaques 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 Milions de victimes de la Cybercirminalité 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

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

Le cyber-espionnage, en tête

des menaces en 2017 ?

	**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.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité 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 ?

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…

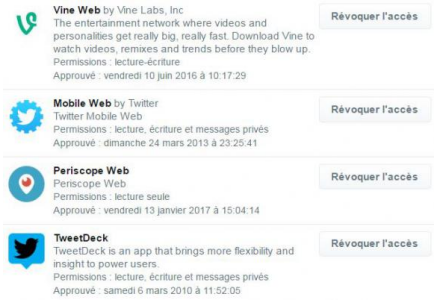
Le compte Twitter officiel de Bercy a été piraté mercredi 15 mars. (CAPTURE D'ÉCRAN)

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

Arnaques entre cybercriminels !

	**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]

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*

Les messages de WhatsApp peuvent être facilement lus par la CIA

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]

Réagissez à cet article

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