

Journée de la Biométrie – 2ème édition le 7 juillet 2017 à l'ENSICAEN



JOURNÉE DE LA BIOMÉTRIE
SAVE THE DATE

Démonstrations Conférences

Le 7 juillet 2017 9h30-17h

ENSI Caen, 6 boulevard Maréchal Juin 14000 Caen

Public académique industriel

GREYC

INRA

CNRS

Journée de la Biométrie – 2ème édition le 7 juillet 2017 à l'ENSICAEN

Suite au succès de The Biometrics Day In Normandy de novembre 2014, le Laboratoire GREYC en partenariat avec l'ENSICAEN, le Pôle TES, l'AD Normandie, Orange et Normandie Université organise la seconde édition le 7 juillet prochain.

La journée dédiée aux acteurs de la Biométrie, enseignants-chercheurs et partenaires industriels, sera ponctuée de conférences, de démonstrations et de temps d'échanges. L'occasion de faire connaître les activités de recherche dans ce domaine, mettre à l'honneur les innovations et la vision de demain de la Biométrie.

L'inscription est gratuite mais obligatoire : inscription

Journée de la Biométrie – vendredi 7 juillet 2017, de 9h30 à 17h

ENSICAEN – 6 Boulevard Maréchal Juin – Caen

Téléchargez l'affiche

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 : *Journée de la Biométrie – AD Normandie*

EternalRocks, le successeur de WannaCry encore plus inquiétant ?

 <p>Denis JACOPINI</p> <p>VOUS INFORME</p> <p>LCI</p>	<p>EternalRocks, le successeur de WannaCry encore plus inquiétant ?</p>
--	---

Après l'attaque du ransomware WannaCry, les chercheurs ont identifié le ver de réseau EternalRocks. Celui-ci utilise jusqu'à 7 outils de hacking ayant été volés à la NSA puis exposés par le groupe Shadow Brokers.

Selon Malwarebytes, WannaCry a recherché les ports SMB vulnérables avant d'utiliser EternalBlue pour rentrer sur le réseau et le backdoor DoublePulsar pour installer le ransomware. EternalRocks utilise aussi ces deux outils. (crédit : D.R.)

Une semaine après l'attaque perpétrée par le ransomware WannaCry au niveau mondial, un autre logiciel d'exploitation de failles fait parler de lui. Selon des chercheurs en sécurité, il y a au moins une personne qui utilise 7 des outils d'attaque volés à la NSA dans un ver de réseau dénommé EternalRocks par ceux qui l'ont identifié. Les chercheurs ont constaté que ce ver ciblait la même vulnérabilité du protocole SMB de Windows, en s'avérant plus menaçant et plus difficile à contrer. Comme WannaCry, EternalRocks utilise EternalBlue, l'un des outils de la NSA.

Malwarebytes pense que WannaCry n'a pas été diffusé par une campagne de spams malveillant mais par une opération de scanning qui a d'abord recherché les ports SMB accessibles publiquement et vulnérables avant d'utiliser EternalBlue pour rentrer sur le réseau et d'utiliser la porte dérobée DoublePulsar pour installer le ransomware...[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)

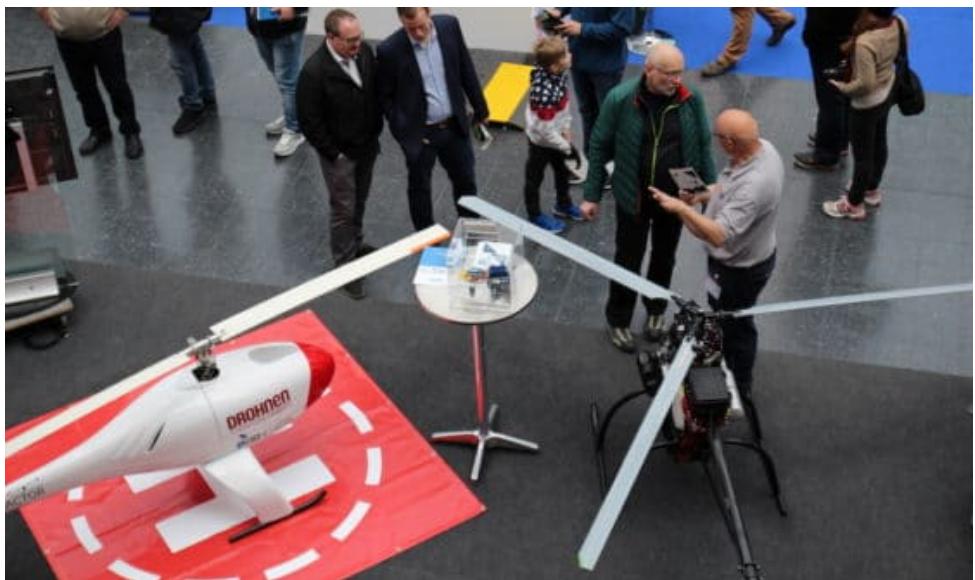
Plus d'informations sur : <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>



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.

Les drones civils aussi devront répondre au concept de « Privacy by Design »



Les drones civils aussi devront répondre au concept de « Privacy by Design »

D'ici un an, les opérateurs de drones comme les fabricants, auront l'obligation de mettre en œuvre des « mesures techniques et opérationnelles appropriées » afin protéger les droits des personnes et des données. Laurent Archambault, avocat à la Cour, explique ici comment les acteurs de la filière drone, en Europe à partir du 25 mai 2018, devront non seulement acheter ou concevoir des drones qui prennent en compte cette question, planifier leurs missions dans cet état d'esprit, mais aussi adopter une organisation qui permette une protection maximisée des tiers et de leurs données.

Les drones sont par essence des appareils permettant des prises de vue ou la captation de données, discrètement. La grande majorité de ces aéronefs est de petite taille. Ils peuvent voler près du sol, longer des édifices ou encore suivre une personne de jour comme de nuit. Comme souligné par Edouard Geffray, Secrétaire général de la CNIL, la problématique du drone pour la vie privée et la protection des données réside d'ailleurs, non pas tant dans l'emport de capteurs, mais bien dans la mobilité et la discréetion du drone.

A cet égard, le concept de « *Privacy by Design* » pourrait constituer un moyen de limiter, voire de supprimer tant les atteintes à la vie privée que la captation de données personnelles par drone (ces dernières pouvant être grossièrement définies, comme des «*données non anonymes* »). Insistons sur le fait qu'à l'ère du numérique, ces deux domaines sont poreux entre eux..[lire la suite]

A Lire aussi :

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

DIRECTIVE (UE) 2016/680 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016

Le RGPD, règlement européen de protection des données. Comment devenir DPO ?

Comprendre le Règlement Européen sur les données personnelles en 6 dessins

Notre sélection d'articles sur le RGPD (Règlement Européen sur la Protection des données Personnelles) et les DPO (Délégués à la Protection des Données)

Notre métier : Vous accompagner dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

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

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



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.

Source : *Le concept de « Privacy by Design » à la rescousse des drones civils européens* – Aerobuzz

Google veut jouer à Madame Irma et anticiper les problèmes de santé avec l'Intelligence Artificielle



Google veut jouer à Madame Irma et anticiper les problèmes de santé avec l'Intelligence Artificielle

Prévenir plutôt que guérir : si la grande majorité des médecines traditionnelles de par le monde appliquent déjà ce principe depuis des milliers d'années, il semblerait que la technologie puisse intégrer, elle aussi, ce principe de prévention. Et c'est bien l'intention de Google avec ce nouveau développement de son pôle de recherche scientifique, Google Brain. Cela donnerait un coup de pouce géant à certains domaines de la médecine moderne, notamment en termes de prévision et prévention des maladies cardio-vasculaires, de plus en plus nombreuses, chez les hommes comme chez les femmes.

Google s'est associé avec les universités américaines de Chicago et de San Francisco, afin de concevoir une technologie qui, grâce à l'intelligence artificielle et aux données récupérées par les hôpitaux parmi les milliers de dossiers médicaux des patients, permettrait de pouvoir prédire des risques médicaux, une projection de l'état de santé post-hospitalisation, ou les arrêts cardiaques, entre autres espérances...[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 : *Intelligence artificielle : Google veut jouer à Madame Irma et anticiper les problèmes de santé*

Uber fait les prix à la tête du client aidé par une Intelligence Artificielle



Uber fait les prix à la tête du client aidé par une Intelligence Artificielle

Uber a reconnu avoir recours à l'intelligence artificielle pour facturer ses clients en fonction de ce qu'ils sont susceptibles d'être prêts à payer.

Comme indiqué par Bloomberg, le service de transport explique que le nouveau système est basé sur l'IA et des algorithmes qui estiment les prix de courses que les groupes de clients seront prêts à payer en fonction de la destination, de l'heure et de l'emplacement.

Dans le passé, votre tarif serait défini en fonction du kilométrage, du temps et de la demande géographique. Cependant, le nouveau système de « tarification basée sur l'itinéraire » utilise des techniques d'apprentissage automatique pour modifier les prix par rapport à un certain nombre de facteurs sociologiques.

Un prix à la tête (et aux données) du client

Déployé actuellement dans 14 villes, le nouveau système prend en compte la richesse estimée. Par exemple, si un passager fait un trajet d'une région riche à l'autre, on peut lui demander de payer plus cher que quelqu'un qui se dirige vers une zone moins aisée, quelle que soit la distance, le kilométrage ou le temps nécessaire pour voyager.

En outre, comme l'a noté Bloomberg, malgré les hausses possibles de ces prix sur mesure, cela ne signifie pas que les conducteurs recevront une part de ces factures gonflées.

La question découle de ce que Uber appelle des « prix initiaux » qui garantissent aux clients un tarif fixe avant leur réservation. Les passagers savent combien ils sont censés payer, mais les conducteurs ont fait savoir qu'ils ne constataient pas de compensation supplémentaire du fait de la hausse des prix produite par le système d'IA.

Dans un communiqué, un porte-parole d'Uber a déclaré que les trajets sont facturés différemment « en fonction de notre compréhension des choix des passagers afin que nous puissions servir plus de personnes dans plus d'endroits aux tarifs qu'ils peuvent se permettre »...[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 : Uber utilise l'IA pour vous faire payer plus un trajet : une dérive ? – ZDNet

WannaCry : seulement trois antivirus protègent de l'exploit EternalBlue



WannaCry :
seulement
trois
antivirus
protègent
de
l'exploit
EternalBlue

Prompts à clamer qu'ils bloquent WannaCry, les éditeurs d'antivirus oublient de mentionner qu'ils ne détectent pas, à trois exceptions près, l'exploit EternalBlue. Or, c'est celui-ci qui risque d'être réutilisé par de nouvelles menaces.

Depuis la crise WannaCry, qui s'est déclenchée le 12 mai 2017 et s'est traduite par l'infection de centaines de milliers de systèmes, les éditeurs d'antivirus n'hésitent pas à clamer que leurs outils arrêtent tous la menace. Un test monté par MRG Effitas, une entreprise anglaise spécialisée dans la recherche en sécurité informatique (MRG signifiant Malware Research Group), montre que la réalité est un peu plus contrastée.



En testant la capacité des logiciels de protection grand public (avec leurs paramétrages par défaut) à détecter l'exploit EternalBlue, mis à profit par WannaCry pour se diffuser, MRG Effitas établit que seuls trois produits stoppent le code de la NSA récupéré par les auteurs du ransomware : Eset Smart Security, F-Secure Safe et Kaspersky Internet Security. « *Deux de ces produits utilisent le filtrage réseau pour détecter cet exploit et le bloquer avant son exécution au niveau du noyau* », écrit MRG Effitas, qui précise que ce mode de détection pourrait être contourné en masquant la signature de l'exploit.

...[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.

Source : *WannaCry : seulement trois antivirus protègent de l'exploit EternalBlue*

Cyberattaque : va-t-on un jour prendre votre télévision connectée en otage ?



Cyberattaque : va-t-on un jour prendre votre télévision connectée en otage ?

Pour exiger une rançon, des hackers pourraient pirater vos cafetières, télévisions, GPS connectés. Mais est-ce vraiment crédible ?

Les récentes attaques massives de « ransomwares », ces logiciels malveillants exigeant une rançon pour débloquer les ordinateurs qu'ils ont infectés, font craindre pour l'avenir des objets connectés, **des jouets aux téléviseurs en passant par le réfrigérateur ou la cafetière**, qui se multiplient dans nos foyers.

« Concernant l'attaque du week-end passé, il n'y a pas de risque pour les objets connectés. Elle touchait en particulier des systèmes avec Windows (...), et il n'y a pas d'objets connectés grand public aujourd'hui qui embarquent Windows pour fonctionner », assure Gérôme Billois, consultant chez Wavestone. « En revanche, il y a déjà eu des attaques massives sur des objets connectés », rappelle-t-il.

Le malware (logiciel malveillant) Mirai a ainsi récemment infecté par centaines de milliers des objets connectés mal sécurisés, non pas pour les bloquer, mais **pour les transformer en zombies et créer des relais pour de futures cyberattaques**.

Transformer vos objets en mouchards

Mardi à La Haye, le jeune prodige Reuben Paul, 11 ans, a épaté une galerie d'experts en cybersécurité en piratant le bluetooth de leurs appareils électroniques pour prendre le contrôle d'un ours en peluche.

Les objets connectés sont donc des cibles tout à fait crédibles, qui peuvent aussi bien **siphonner des données que se transformer en mouchards**. Selon des documents révélés en mars par WikiLeaks, les services de renseignement américains sont capables de « hacker » des smartphones, des ordinateurs et des télévisions intelligentes, notamment pour prendre **le contrôle de leurs micros et écouter ce qu'il se passe**.

« Tous les autres objets connectés sont piratables, ça a été démontré, que ce soit la cafetière, le réfrigérateur, le thermostat, la serrure électronique, le système d'éclairage... » Loïc Guézo stratégiste 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 DRETEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Source : *Cyberattaque : va-t-on un jour prendre votre télévision connectée en otage ?* – Sud Ouest.fr

Une intelligence artificielle pourrait comprendre la langue des dauphins d'ici 2021



Une intelligence artificielle pourrait comprendre la langue des dauphins d'ici 2021

La startup suédoise Gavagai AB développe une intelligence artificielle capable de comprendre une multitude de langues. Elle vient de lancer un projet d'une durée de quatre ans pour adapter son outil à la compréhension du langage des dauphins....[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 cette page.



Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

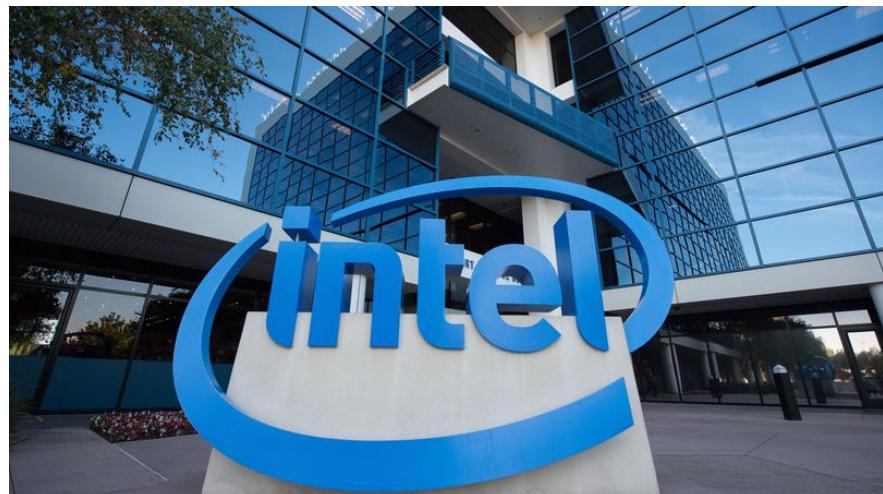
- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



[Contactez-nous](#)

Réagissez à cet article

Faille de sécurité dans les processeurs Intel pour les ordinateurs professionnels



Faille de sécurité dans les processeurs Intel pour les ordinateurs professionnels

Une faille de sécurité majeure a été repérée sur les processeurs d'Intel. Elle permettrait la prise de contrôle de serveurs et d'ordinateurs d'entreprise.

Depuis 2008, les puces d'Intel comportaient une faille de sécurité. Le géant américain de l'électronique a publié lundi une annonce et une mise à jour afin de corriger le problème. Cette erreur de conception touche une grande partie des processeurs de la marque allant du Nehalem (2008) à Kaby Lake (2017), intégrés sur les PC professionnels. Les entreprises dotées de ces ordinateurs doivent, par contre, mettre à jour rapidement leur système.

La faille est située au niveau du programme «Active Management Technology». Il permet aux administrateurs accrédités d'accéder et de gérer des flottes d'ordinateurs à distance, ce qui explique pourquoi la faille touche les gammes professionnelles. Selon le site SemiAccurate, des hackers pourraient prendre le contrôle de l'intérieur et agir comme bon leur semble. Les informations présentes sur certains serveurs et les PC sont donc exposés à ces attaques. Les propriétaires d'ordinateurs équipés de puces Intel et issus de la grande consommation n'ont rien à craindre, selon Intel...[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 : *Intel révèle une faille de sécurité dans ses processeurs*

Pour AV-Test, 29 suites de sécurité sur 32 ne sont pas correctement protégées



Pour AV-Test, 29 de 32 suites de sécurité sur 32 ne sont pas correctement protégées

AV-Test publie l'analyse de 32 suites de sécurité visant à mesurer leur capacité à s'autoprotéger. Seuls trois éditeurs, dont ESET, ont réussi le test.

De la même façon que les utilisateurs protègent leurs appareils, les logiciels doivent disposer de mesures de sécurité pour s'autoprotéger en cas d'attaque. Plusieurs techniques existent comme l'ASLR et la DEP.

« Pour offrir une protection exceptionnelle en matière de cybersécurité, les éditeurs doivent fournir une protection reposant sur un noyau parfaitement protégé », déclare Andreas Marx, PDG d'AV-TEST GmbH. Lors de la publication du premier test d'autoprotection en 2014, **2 produits seulement (dont ESET) utilisaient en continu la technique de l'ASLR et de la DEP**. Une prise de conscience s'est alors emparée des autres éditeurs, mais cela ne suffit pas.

Autre mesure de sécurité, l'utilisation de signatures et de certificats de fichiers. Ceci est important, car elle permet de vérifier l'authenticité et l'intégrité des fichiers. AV-Test analyse donc dans son test un certificat et sa validité concernant les fichiers PE en mode utilisateur pour 32 et 64 bits. Là encore, **certains éditeurs de sécurité ont jusqu'à 40 fichiers non sécurisés sur leur produit**, soit 16% de la totalité des fichiers.

« Certains fabricants n'ont toujours pas compris qu'une suite de sécurité doit être cohérente dans son ensemble : elle doit offrir la meilleure protection à l'utilisateur tout en étant parfaitement sûre elle-même, à commencer par le téléchargement de la version d'essai sur un serveur protégé », ajoute Andreas Marx.

AV-Test étudie également le protocole de transfert utilisé. En théorie, les logiciels de sécurité doivent passer par le protocole HTTPS. Il garantit la sécurité de leur site Internet. Sans cette protection, des attaques peuvent avoir lieu à l'insu de l'utilisateur. Bien qu'il n'y ait pas de téléchargements directs pour les solutions réservées aux entreprises, de nombreux éditeurs proposent une version d'essai gratuite aux particuliers. AV-Test dresse alors un constat effrayant : **sur les 19 fabricants, 13 d'entre eux ne disposent pas d'un protocole HTTP sécurisé**. Seuls 6 éditeurs, dont ESET, ont recours au protocole HTTPS.

Si vous souhaitez accéder à l'analyse complète du rapport AV-Test, cliquez ici. Pour toutes questions relatives aux règles de sécurisation, nous nous tenons à votre disposition.

[Article original]

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

Source : *Boîte de réception (302) – denis.jacopini@gmail.com – Gmail*