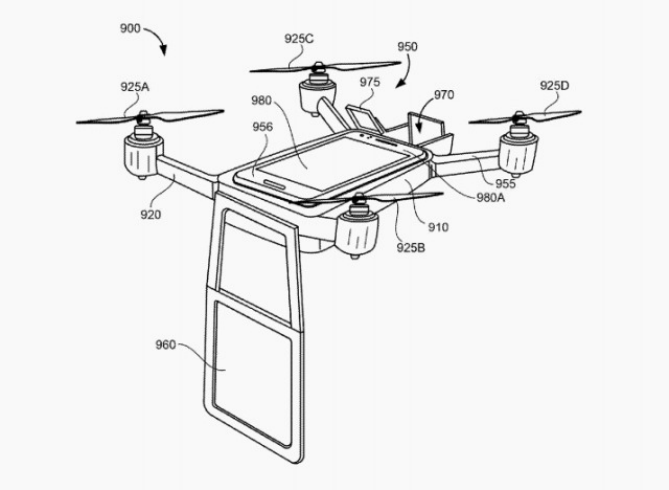
Google imagine un drone de télé-présence

Google imagine un drone de télé-présence

Il y a quelques mois, Google a obtenu un brevet concernant un concept de drone capable de servir de support pour de la télé-présence.

Google a un intérêt marqué pour les drones. En la matière, son projet le plus avancé s'appelle Wing et consiste à mettre au point un système de livraison de colis par les airs. Dévoilé en 2013, il doit faire ses débuts commerciaux l'année prochaine. D'ici là, grâce au feu vert de l'administration de l'aviation civile, Google va pouvoir effectuer des tests sur le territoire américain.

La firme de Mountain View a d'autres idées dans son sac. Il reste néanmoins à leur donner corps. C'est le cas par exemple de ce brevet repéré par Quartz qui décrit le principe d'un drone de type quadricoptère qui embarque plusieurs terminaux et équipements de façon à pouvoir afficher sur un écran l'image d'un interlocuteur situé à un autre endroit. En gros, c'est de la télé-présence déployée sur un drone.



On identifie sans peine l'écran et la tablette sur le drone…[lire la suite]

Notre métier : Sensibiliser les décideurs et les utilisateurs aux risques liés à la **Cybercriminalité** et 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).

Denis JACOPINI anime dans toute le France et à l'étranger des conférences, des tables rondes et des formations pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles (Mise en Place d'un Correspondant Informatique et Libertés (CIL) dans votre établissement.

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

---

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

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

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Original de l'article mis en page : Google imagine un drone de télé-présence — Tech — Numerama

Drone piégé utilisé par l’EI contre deux militaires français

Drone piégé utilisé par l’EI contre deux militaires français

Selon des informations du Monde, deux militaires français qui étaient en opération auprès des Kurdes en Irak ont été rapatriés en France après avoir été grièvement blessé par un drone piégé de l'État islamique.

C'est un mode d'action que les forces de l'ordre redoutent sur le territoire national, et qui semble désormais déployé sur le terrain de l'adversaire. Le Monde affirme ce mardi que deux militaires français ont été gravement blessés par un drone qui avait été piégé par des militants de l'État islamique, en Irak. L'un des deux serait entre la vie et la mort.
« Les deux commandos ont été touchés par un drone volant piégé, envoyé par un groupe lié à l'EI, dans des circonstances qui restent à préciser. Les militaires auraient intercepté le drone, avant que celui-ci explose à terre. Ce mode d'action contre des forces françaises est en tout état de cause inédit », rapporte le quotidien, qui précise que ses informations sont confirmées par d'autres médias.
Ce piège aurait été tendu aux commandos parachutistes qui intervenaient auprès des forces kurdes à Erbil, dans le nord de l'Irak, entre Mossoul et Kirkouk. La ville est la capitale de la région autonome du Kurdistan.

Le Monde indique que le ministère de la Défense ne souhaite pas confirmer cette attaque d'un nouveau genre et le rapatriement des deux soldats à l'hôpital militaire de Percy-Clamart, non seulement par souci de protéger les familles, mais aussi peut-être en raison des « moyens employés pour cette attaque » (on peut ajouter que de manière plus générale s'agissant des propagandes de guerre, les armées n'aiment jamais communiquer sur leurs propres pertes, préférant mettre en avant leurs réussites pour conserver le moral des troupes et le soutien des populations).

LA CRAINTE D'UN ATTENTAT PAR DRONE
La crainte est sans doute que le mode opératoire, relativement peu coûteux et surtout peu risqué pour les attaquants, ne donne des idées sur le front irakien ou syrien, mais aussi en occident. L'hypothèse qu'une petite bombe puisse être transportée par un drone sans savoir d'où il a décollé et d'où il est contrôlé est soulevée depuis longtemps par les experts de la sécurité aérienne. Elle avait notamment été évoquée en France lors du survol des centrales nucléaires par des drones.
Depuis, le législateur s'est emparé du sujet en élaborant une proposition de régulation des drones en cours d'examen, qui prévoit notamment l'obligation d'identifier les drones à distance ou de brider leur utilisation dans certaines zones réglementées. Mais par définition les lois n'ont aucune influence contre ceux qui veulent les violer, et il paraît bien difficile d'empêcher totalement le transport de bombes par drone, sauf à utiliser des moyens technologiques encore balbutiants et impossibles à déployer sur tout le territoire comme des brouilleurs, des lasers, des perturbateurs de signaux GPS, des filets, ou même des aigles.

UNE RÉPONSE ARTISANALE À L'UTILISATION DE « ROBOTS TUEURS » ?
Le fait que les troupes de l'EI utilisent des bombes montées sur des drones n'est aussi, hélas, qu'une réponse attendue à l'utilisation croissante des drones et autres engins militaires conduits à distance par les troupes alliées. En août dernier, l'armée irakienne était fière de présenter un fusil mitrailleur monté sur un véhicule conduit à 1 km de distance, qui permettait d'aller tuer sans risquer de se faire tuer, ce qui est aussi l'objectif des avions de combat semi-autonomes, des navires de guerre ou des nouveaux chars d'assaut. L'utilisation de drones piégés n'est à cet égard qu'une réponse artisanale de même nature.
Il faut ajouter qu'en droit international, l'utilisation de telles armes n'est pas interdite dès lors qu'elles visent à tuer des militaires combattants, et non des civils. La question de la régulation des « robots tueurs » a déjà fait l'objet de débats dans la communauté internationale, dans le cadre de révisions des conventions de Genève, mais les perspectives d'un accord sont excessivement lointaines. La seule piste évoquée, encore très incertaine, est l'obligation qui pourrait être faite qu'un humain reste en permanence aux commandes des engins robotisés, pour ne pas parvenir à des guerres menées par IA interposées.
[Article source]

Original de l'article mis en page : L'État islamique aurait piégé un drone et blessé grièvement deux militaires français — Politique — Numerama

---

52 % des DSI Français acceptent moins de sécurité pour plus de mobilité

52 % des DSI Français acceptent moins de sécurité pour plus de mobilité

C'est une nouvelle à la fois peu surprenante et inquiétante : plus de la moitié des responsables informatiques en France cèdent du terrain sur le plan sécuritaire pour avantager la mobilité et le Bring Your Own Device.

« **Rendre les salariés et les opérations plus agiles** »
On ne cesse de le répéter depuis des années : le BYOD est loin d'être toujours un choix, il n'est pas rare qu'il s'impose de lui-même. Rejeter cette situation, c'est risquer une utilisation sous-marine, multipliant ainsi les risques. L'accepter, c'est limiter les risques en question en encadrant le BYOD.
Dans une étude menée par le cabinet Vanson Bourne pour le compte de VMware (plus de détails en fin d'article), nous apprenons que 52 % des responsables informatiques français font face à une telle pression vis-à-vis de la mobilité d'entreprise « qu'ils sont prêts à prendre des risques inconsidérés vis-à-vis de la sécurité des données de leur organisation ».
Ces risques sont en grande partie pris pour contenter les cadres dirigeants qui souhaitent absolument accéder aux données pro via leurs propres terminaux, « même si cela va à l'encontre des stratégies de leur entreprise » et que cela multiplie les risques de cyberattaques.
Mais les gains en valent la chandelle puisque les DSI cèdent. 51 % d'entre eux estiment ainsi que les bénéfices sont supérieurs aux risques. « Transformation numérique et mobilité sont indissociables. Les organisations doivent sans cesse chercher à développer leurs activités et à innover. Elles prennent donc des risques à court terme sur le plan de la sécurité afin de rendre les salariés et les opérations plus agiles » explique notamment Sylvain Cazard, directeur général de VMware France.
Pour s'adapter au marché et aux désirs de certains salariés, les DSI n'hésitent donc pas à prendre plus de risques. Il faut dire que près d'un quart des responsables informatiques estiment que le manque de mobilité des salariés réduit leur productivité. Un argument qui fait mouche et pousse logiquement les DSI à lâcher du lest côté sécurité.

Des salariés mal formés, des patrons sous-informés
Bien évidemment, les responsables n'ont pas à laisser la porte ouverte au premier pirate informatique venu. Une plus forte pédagogie auprès des salariés devient ainsi indispensable si l'entreprise ne souhaite pas voir toutes ses données partir dans la nature. Ce point est d'autant plus majeur sachant que l'étude indique que 60% des salariés mobiles précisent ne pas connaître la politique de sécurité de leur entreprise… Une statistique douloureuse et effrayante qu'il convient de ne pas minimiser.
Plus grave encore pour les dirigeants d'entreprises, une ancienne enquête de Vanson Bourne montrait que 25 % des DSI français ont confié ne pas informer leur patron en cas de cyberattaque. Ceci alors même que 29 % des DSI et 21 % des employés estiment que leurs patrons sont responsables en cas de fuite de données. Une incohérence qui en dit long sur la complexité de la problématique…[lire la suite]

Notre métier : Sensibiliser les décideurs et les utilisateurs aux risques liés à la **Cybercriminalité** et 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).
Denis JACOPINI anime dans toute le France et à l'étranger des conférences, des tables rondes et des formations pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles (Mise en Place d'un Correspondant Informatique et Libertés (CIL) dans votre établissement.
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

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

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

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Original de l’article mis en page : BYOD : 52 % des DSI Français acceptent moins de sécurité pour plus de mobilité

Quelles failles pour les voitures connectées ?

Quelles failles pour les voitures connectées

L'édition du salon de l'auto interpelle le grand public sur les nouveaux pirates de la route. Voitures connectées : les cybercriminels dans l'angle mort ?

Nul doute, la voiture connectée est encore l'une des stars du salon de l'auto cette année. Comme tout ce qui attrait à internet et aux objets connectés, il est légitime de se poser quelques questions notamment sur la sécurité liée au partage des données ainsi qu'à cette forme de déplacement autonome. Un véhicule connecté est en effet doté d'un accès à Internet ainsi que, plus généralement, d'un réseau local sans fil. L'accès Web offre divers services supplémentaires tels que la notification automatique des embouteillages, la réservation de parking, la surveillance du style de conduite (pouvant par ailleurs avoir une incidence sur le montant des primes d'assurance automobiles) etc.
De multiples raisons peuvent motiver les cybercriminels à tenter de pirater des voitures connectées :
L'appât du gain : ll s'agit de bloquer l'accès au véhicule jusqu'à ce la victime paie une rançon.
L'espionnage : l'activation du micro ou de la caméra équipant le véhicule peut donner accès à des informations exclusives et des données sensibles.
La violence physique : les attaques peuvent avoir pour but de blesser le conducteur, ses passagers, ou encore d'endommager d'autres véhicules sur la route.
C'est en analysant ses raisons que la société russe développe une approche de la sécurité interne des véhicules connectés. Elle reposent sur deux principes : D'abord l'isolement veille à ce que deux entités indépendantes (applications, pilotes, machines virtuelles) ne puissent interférer l'une avec l'autre en aucune façon. Ensuite, le contrôle des communications signifie que deux entités indépendantes ayant à communiquer dans le système doivent le faire conformément à des règles de sécurité. L'utilisation de techniques de cryptographie et d'authentification pour l'envoi et la réception des données fait également partie intégrante de la protection du système.
Pour respecter notre travail, merci de ne reprendre que l'intro. Pour lire la suite de cet article original direction ->
http://www.datasecuritybreach.fr/voitures-connectees-cybercriminels-langle-mort/#ixzz4MV1xJas6

…[lire la suite]

Notre métier : Sensibiliser les décideurs et les utilisateurs aux risques liés à la **Cybercriminalité** et 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).
Denis JACOPINI anime dans toute le France et à l'étranger des conférences, des tables rondes et des formations pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles (Mise en Place d'un Correspondant Informatique et Libertés (CIL) dans votre établissement.
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

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

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

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

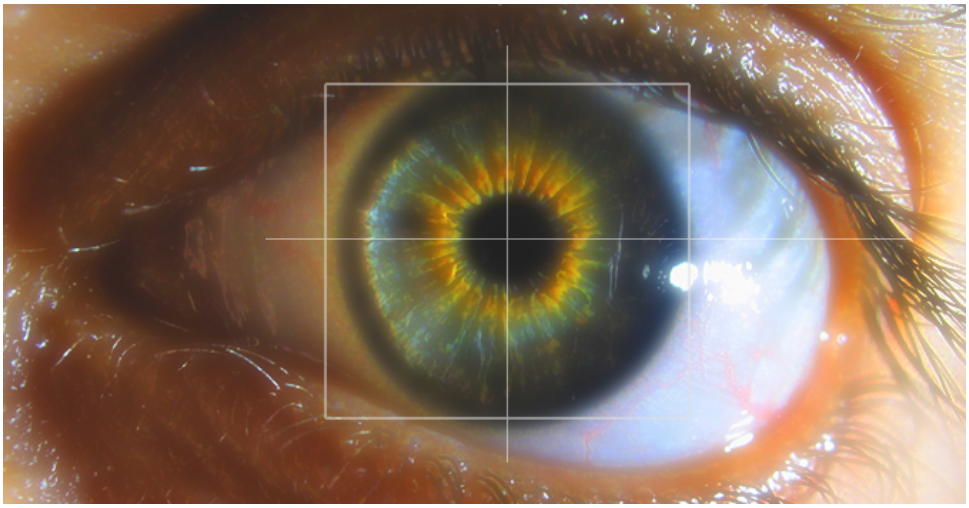
Contactez-nous

Réagissez à cet article

Original de l’article mis en page : Voitures connectées : les cybercriminels dans l’angle mort ? – Data Security Breach

---

MasterCard déploie le paiement par selfie



MasterCard déploie le paiement par selfie

Après une phase de test dans quelques pays, le paiement par selfie imaginé par MasterCard se déploie en Europe.

C'est une procédure que vous connaissez forcément si vous avez déjà eu l'occasion d'effectuer un achat en ligne. Au moment du paiement, la boutique vous demande de renseigner les informations de votre carte bancaire (son numéro, sa date d'expiration et son cryptogramme visuel).
Une fois ces informations envoyées, votre banque est censée vous envoyer un SMS de confirmation contenant un code qu'il faut inscrire sur le site du marchand afin de valider définitivement la transaction. Cette mesure est nécessaire en cas de vol de la carte, afin de neutraliser toute tentative d'utilisation frauduleuse.
Avec l'envoi d'un code par texto (ou par mail), le client limite déjà beaucoup le risque de se faire avoir. Mais la méthode ne contre pas 100 % des menaces. Des fraudeurs très motivés et compétents peuvent modifier le numéro de téléphone censé recevoir le code ou accéder à la boîte mail pour y recevoir le courrier de validation. C'est en ayant ces problématiques en tête que MasterCard tente une autre approche, avec l'utilisation du selfie.

Évidemment, des interrogations apparaissent : que se passe-t-il si on utilise une photo de moi ? MasterCard dit avoir trouvé une parade en demandant à l'usager, pendant le selfie, de cligner des yeux. Et si une vidéo de moi est utilisée alors ? La parade pourrait être plus difficile à trouver, mais encore faut-il que le fraudeur puisse obtenir une vidéo de la victime, de face, en train de cligner des yeux. Or, elle n'existe peut-être pas.
Et quid des données biométriques qui sont par nature hautement sensibles ? MasterCard assure au Figaro qu'aucune information de cette nature n'est récupérée par le groupe sous sa forme originale. Manifestement, l'image est convertie en une sorte de signature numérique, qui est ensuite transmise à l'entreprise sans que celle-ci ne soit en mesure de faire le chemin inverse pour reconstituer le visage…[lire la suite]

Notre métier : Sensibiliser les décideurs et les utilisateurs aux risques liés à la **Cybercriminalité** et 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).
Denis JACOPINI anime dans toute le France et à l'étranger des conférences, des tables rondes et des formations pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles (Mise en Place d'un Correspondant Informatique et Libertés (CIL) dans votre établissement.
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

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

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

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Original de l’article mis en page : Le paiement par selfie de MasterCard se déploie en Europe – Tech – Numerama

Les données de santé, la nouvelle cible des cybercriminels

Les données de santé, la nouvelle cible des cybercriminels

Face au développement massif des nouvelles technologies, nos données personnelles sont aujourd'hui entièrement informatisées. De notre dossier médical jusqu'à nos données bancaires en passant par nos loisirs et notre consommation quotidienne, chaque minute de nos vies produit une trace numérique sans même que l'on s'en aperçoit.

Pendant des années nos données de santé étaient éparpillées entre médecins, laboratoire d'analyses, hôpitaux, dentistes dans des dossiers cartonnés qui s'accumulaient au coin d'un bureau ou sur une étagère. En 2012 la loi « hôpital numérique » avait permis un premier virage en obligeant la numérisation des données de santé par tous les professionnels pour une meilleure transmission inter-service. Depuis un an, la loi « santé 2015 » oblige à une unification et une centralisation des données de santé dans des serveurs hautement sécurisés constituant ainsi le Big Data.

Une centralisation des données qui n'est pas sans risque

Appliqué à la santé, le Big Data ouvre des perspectives réjouissantes dans le croisement et l'analyse de données permettant ainsi d'aboutir à de véritables progrès dans le domaine médical. Mais cela n'est pas sans risque.

Le statut strictement confidentiel et extrêmement protégé donne à ces données une très grande valeur. Nos données médicales deviennent ainsi la cible d'une nouvelle cybercriminalité, cotées sur le Dark Web.

Le Dark Web ou Deep Web est l'underground du net tel qu'on le connait. Il est une partie non référencée dans les moteurs de recherche, difficilement accessible où le cybertrafic y est une pratique généralisée. Sur le Dark Web les données personnelles sont cotées et prennent ou non de la valeur selon leur facilité d'accès et leur rendement.

Là où les données bancaires détournées sont de plus en plus difficiles à utiliser suite aux nombreuses sécurisations mise en place par les banques, l'usurpation d'identité et la récolte de données médicales prennent une valeur de plus en plus grande. Selon Vincent TRELY, président-fondateur de l'APSSIS, Association pour la Sécurité des Systèmes d'information, interviewer sur France Inter le 8 septembre 2016, le dossier médical d'une personne aurait une valeur actuelle qui peut varier entre 12 et 18 $.

Si l'on rapporte cette valeur unitaire au nombre de dossiers médicaux abrités par un hôpital parisien, on se rend compte que ceux-ci abritent une potentielle fortune pouvant aller jusqu'à des millions de dollars. Aussi pour protéger ces données, les organismes de santé se tournent vers des sociétés certifiées proposant un stockage dans des Datacenters surveillés, doublement sauvegardés, ventilés avec une maintenance 24h/24. Le stockage a donc un coût qui peut varier entre quelques centaines d'euros jusqu'à des centaines de milliers d'euros pour un grand hôpital. Le coût d'hébergement peut alors devenir un vrai frein pour des petites structures médicales où le personnel présent est rarement qualifié pour veiller à la sécurité numérique des données. Et c'est de cette façon que ces organismes deviennent des cibles potentielles pour les cybercriminels.

Des exemples il en existe à la Pelle. Le laboratoire Labio en 2015 s'est vu subtilisé une partie des résultats d'analyse de ses patients, pour ensuite devenir la victime d'un chantage. Les cybercriminels demandaient une rançon de 20 000 euros en échange de la non divulgation des données. Peu de temps après c'est le service de radiologie du centre Marie Curie à Valence qui s'est vu refuser l'accès à son dossier patients bloquant ainsi toute une journée les rendez-vous médicaux initialement fixés. Peu de temps avant, en janvier 2015, la Compagnie d'Assurance Américaine Anthem a reconnu s'être fait pirater. Toutes ses données clients ont été cryptées en l'échange d'une rançon.

Ces pratiques étant nouvelles, on peut s'attendre à une recrudescence de ce type de criminalité dans l'avenir selon les conclusions en décembre 2014 de la revue MIT Tech Review…[lire la suite]

Denis Jacopini anime des **conférences et des formations** et est régulièrement invité à des **tables rondes en France et à l'étranger** pour sensibiliser les décideurs et les utilisateurs aux **CyberRisques** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).

Nous animons **conférences et formations** pour sensibiliser décideurs et utilisateurs **aux risques en informatique**, découvrir et comprendre les **arnaques** et les **piratages informatiques** pour mieux s'en protéger et se **mettre en conformité avec la CNIL** en matière de **Protection des Données Personnelles**. Nos actions peuvent être personnalisées et organisées dans votre établissement.

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

---

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

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

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Original de l'article mis en page : Les données de santé, le nouvel El-Dorado de la cybercriminalité

Comment créer une copie d’écran la moins contestable possible ?

Comment créer une copie d’écran la moins contestable possible ?

La copie d'écran sert souvent d'élément de preuve dans un dossier. Pourtant, sa réalisation demande de prendre un certain nombre de précautions pour éviter qu'elle ne soit contestée (et contestable).

Il m'est arrivé, au début de mon activité d'expert judiciaire en informatique, d'assister des huissiers de justice lors de la constitution de preuves, en matière de publication sur internet.
En clair, il s'agissait souvent d'aider un huissier à faire des copies d'écran.
Puis, avec le temps, les compétences informatiques des huissiers ont fortement augmenté, et il devient rare que l'on me demande de l'aide pour faire une copie d'écran.
Pourtant…
Parfois une copie d'écran peut être refusée par un tribunal, si elle ne présente pas un caractère probant suffisant. Extrait d'un jugement :
« Attendu que si la preuve d'un fait juridique n'est, en principe, et ainsi qu'en dispose l'article 1348 du Code civil, soumise à aucune condition de forme, il demeure néanmoins que lorsqu'il s'agit d'établir la réalité d'une publication sur le réseau internet, la production d'une simple impression sur papier est insuffisante pour établir la réalité de la publication, tant dans son contenu, que dans sa date et dans son caractère public, dès lors que ces faits font l'objet d'une contestation ; qu'en effet, et comme le souligne le défendeur l'impression peut avoir été modifiée ou être issue de la mémoire cache de l'ordinateur utilisé dont il n'est pas justifié que cette mémoire ait été, en l'occurrence, préalablement vidée ; »
Je propose pour ma part une méthode de copie d'écran d'une page web qui me semble respecter les règles de l'art :
Étape 1 : Choisir un ordinateur « sûr » pour établir le constat.
Étape 2 : Vider le cache local.
Étape 3 : Vérifier les DNS.
Étape 4 : Afficher la page incriminée.
Étape 5 : Imprimer la page.
Étape 6 : Recommencer avec un autre navigateur.
Étape 7 : Recommencer avec un autre ordinateur et un autre réseau.
[Plus de détails ?]

Denis Jacopini anime des **conférences et des formations** et est régulièrement invité à des **tables rondes en France et à l'étranger** pour sensibiliser les décideurs et les utilisateurs aux **CyberRisques** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Nous animons **conférences et formations** pour sensibiliser décideurs et utilisateurs **aux risques en informatique**, découvrir et comprendre les **arnaques** et les **piratages informatiques** pour mieux s'en protéger et se **mettre en conformité avec la CNIL** en matière de **Protection des Données Personnelles**.
Nos actions peuvent être personnalisées et organisées dans votre établissement.
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

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

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

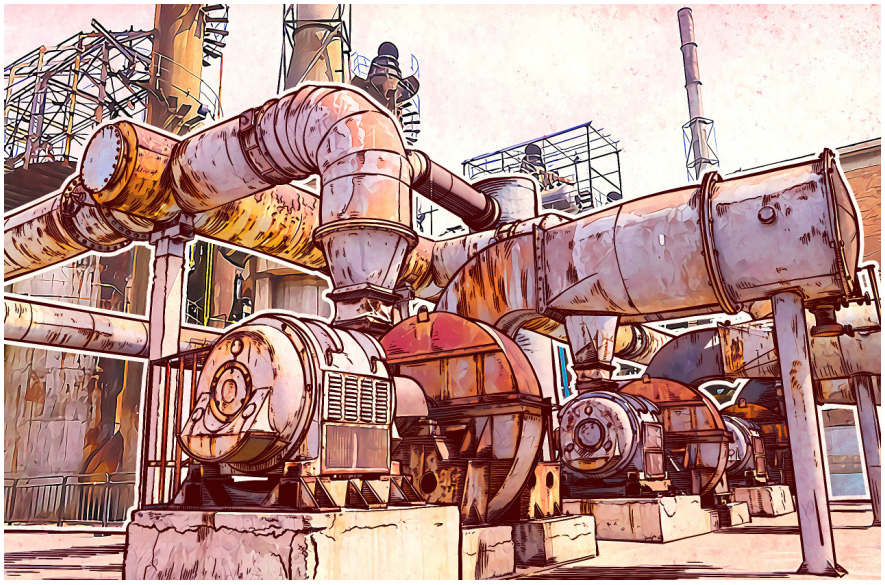
Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Original de l’article mis en page : Contestation d’une copie d’écran. Par Olivier Nerrand, Expert judiciaire.

Piratage de l’électricité, de l’eau et de la nourriture : comment les cybercriminels peuvent ruiner votre vie

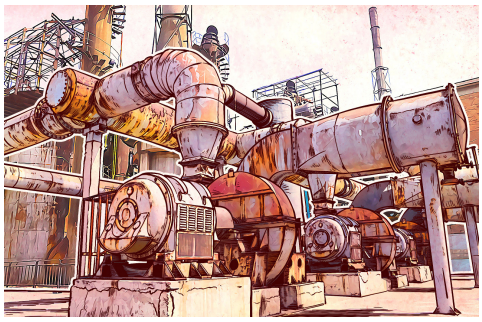


Piratage de l’électricité, de l’eau et de la nourriture : comment les cybercriminels peuvent ruiner votre vie

---

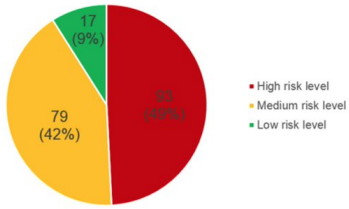
On ne cesse de vous le répéter, il est très important de rester au courant des dernières actualités concernant la cybersécurité et ses menaces. Mieux vaut prévenir que guérir.

Cependant, même ceux qui connaissent tout en matière de cybersécurité, qui utilisent des mots de passe fiables et qui les changent régulièrement, qui reconnaissent des messages d'hameçonnage au premier coup d'œil et qui protègent leurs dispositifs avec une excellente solution de sécurité, même ceux qui font *tout*, ne sont pas totalement à l'abri. Tout simplement parce que nous vivons en société.



Le problème est que nous avons le contrôle sur nos objets personnels, mais pas sur celui des équipements industriels, qui est loin de notre portée.

Vous avez dit cybersécurité ?
Nos experts en cybersécurité ont mené une étude afin de découvrir où nous en sommes concernant la sécurité des systèmes de contrôle industriel.
Shodan, le moteur de recherche pour les dispositifs connectés, nous a montré que 188 019 systèmes industriels dans 170 pays sont accessibles sur Internet. La majorité d'entre eux sont localisés aux Etats-Unis (30,5%) et en Europe, essentiellement en Allemagne (13,9%), Espagne (5,9%) et en France (5,6%).



ICS vulnerabilities in 2015 by risk level (CVSS v.2 and CVSS v.3)

92% (172 982) des systèmes de contrôle industriel (SCI) détectés sont vulnérables. Lamentablement, 87% ont un niveau de risque moyen de bugs et 7% connaissent des problèmes critiques.
Ces cinq dernières années, les experts ont méticuleusement examiné de tels systèmes et y ont découvert de nombreuses failles de sécurité. Durant ce laps de temps, le nombre de vulnérabilités dans les composants SCI a multiplié par dix.
Parmi les systèmes que nos experts ont analysés, 91,6% ont utilisé des protocoles non sécurisés, en donnant l'opportunité aux cybercriminels d'intercepter ou de modifier les données utilisant des attaques de l'homme du milieu.
Egalement, 7,2% (environ 13 700) des systèmes appartiennent à de grandes compagnies aéronautiques, des transports et de l'énergie, pétrolières et gazières, métallurgiques, de l'industrie alimentaire, de la construction et autres secteurs primordiaux.

En d'autres termes, des hackers qualifiés peuvent influencer n'importe quel secteur économique. Leurs victimes (les entreprises piratées) porteraient préjudice à des milliers ou millions de personnes en leur fournissant de l'eau contaminée ou de la nourriture immangeable, ou en leur coupant le chauffage en plein hiver.

Qu'est-ce que cela implique pour nous tous ?

…[lire la suite]

Denis Jacopini anime des **conférences et des formations** et est régulièrement invité à des **tables rondes en France et à l'étranger** pour sensibiliser les décideurs et les utilisateurs aux **CyberRisques** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Nous animons **conférences et formations** pour sensibiliser décideurs et utilisateurs **aux risques en informatique**, découvrir et comprendre les **arnaques** et les **piratages informatiques** pour mieux s'en protéger et se **mettre en conformité avec la CNIL** en matière de **Protection des Données Personnelles**. Nos actions peuvent être personnalisées et organisées dans votre établissement.
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

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

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

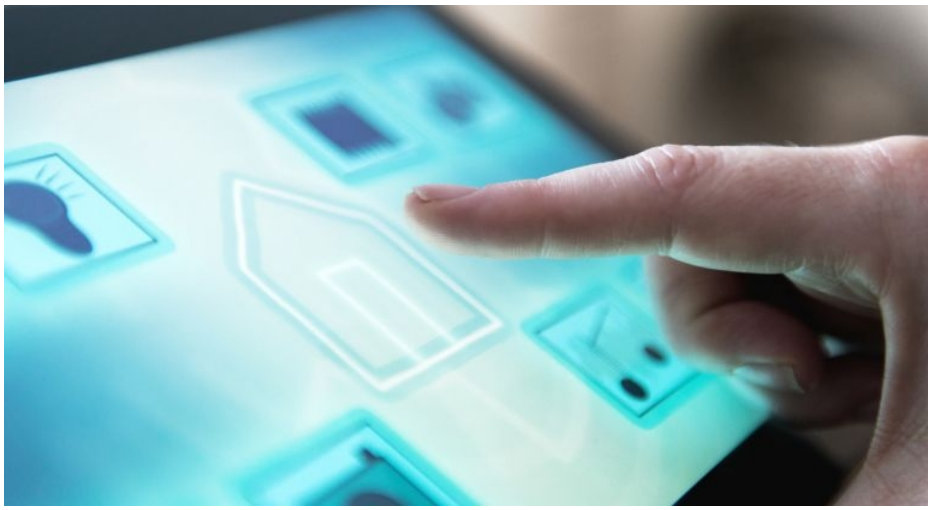
Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Original de l’article mis en page : Piratage de l’électricité, de l’eau et de la nourriture : comment les cybercriminels peuvent ruiner votre vie. | Nous utilisons les mots pour sauver le monde | Le blog officiel de Kaspersky Lab en français.

Jusqu’où les Objets connectés sont les maillons faibles de la cybersécurité ?



Jusqu’où les Objets connectés sont les maillons faibles de la cybersécurité ?

La Chine s'impose parmi les principaux pays créateurs d'objets quotidiens connectés à l'internet, mais elle génère ainsi de gigantesques failles sécuritaires exploitables par des pirates informatiques, a prévenu mardi John McAfee, créateur américain du logiciel antivirus portant son nom.

S'exprimant devant une conférence spécialisée à Pékin, M. McAfee a cité des précédents, dans lesquels des pirates sont parvenus à distance à prendre le contrôle de coffre-forts, de systèmes de chauffage, mais aussi d'ordinateurs de bord d'automobiles ou d'aéroplanes.

« La Chine prend la tête des progrès sur les objets intelligents, depuis les réfrigérateurs jusqu'aux thermostats, et c'est le maillon faible de la cybersécurité », a-t-il martelé, disant vouloir « lever un drapeau rouge » d'avertissement.
« Il y a tellement plus de ces objets, et plus vous en connectez ensemble, plus les risques de piratage augmentent », a encore souligné John McAfee.
L'excentrique septuagénaire avait fait fortune aux débuts d'internet dans les années 1990, après avoir mis au point un logiciel antivirus qui porte son nom et est maintenant la propriété d'Intel.
Plombé par la crise financière de 2008, il avait défrayé la chronique en 2012 après la mort de son voisin au Belize, pays où il vivait à l'époque et qu'il avait fui après l'ouverture d'une enquête de la police locale.
M. McAfee a livré à Pékin un discours au ton sombre et inquiétant, à l'heure où sa nouvelle société MGT Capital se prépare à lancer de nouveaux produits de cybersécurité d'ici la fin de l'année.
« Notre espèce n'a jamais été confrontée jusqu'ici à une menace de cette ampleur. Et pour l'essentiel, nous n'en prenons pas conscience », a-t-il averti.
« Vous pouvez penser que j'exagère, que je tombe dans l'alarmisme. Mais je compte parmi mes amis beaucoup de +hackers+ (pirates) qui ont les capacités de faire d'énormes dégâts si l'envie leur en prend », a-t-il ajouté.
A l'instar de Xiaomi, fabricant de smartphones ayant élargi son offre dans l'électroménager « intelligent », nombre d'entreprises chinoises intègrent désormais une connexion wi-fi à des produits variés, des autocuiseurs pour riz aux purificateurs d'air, permettant aux usagers de les allumer à distance depuis leur téléphone.
De telles connexions créent de graves failles qui accentuent les vulnérabilités de leurs réseaux, selon John McAfee.
Dans un entretien avec des journalistes à Pékin, l'Américain a cependant noté « n'avoir entendu parler d'aucune » attaque informatique de grande ampleur en Chine sur l'année passée, tandis que les Etats-Unis en enregistraient « des centaines ».

Original de l'article mis en page : Objets connectés : le créateur de l'antivirus McAfee met en garde la Chine contre les failles de sécurité | La Provence

---

Position du CERT-FR (Computer Emergency Response Team de

l’ANSSI) vis à vis de Pokemon Go

Position du CERT-ER (Computer Emergency Response Team de l’ANSSI) vis à vis de Pokemon Go

Cyber-risques liés à l'installation et l'usage de l'application Pokémon GoLancé courant juillet par la société Niantic, le jeu Pokémon Go est depuis devenu un phénomène de société, au point d'être installé sur plus de 75 millions de terminaux mobiles dans le monde. Certains acteurs malveillants ont rapidement tenté d'exploiter la popularité du jeu à des fins criminelles. Certaines précautions s'imposent donc avant de pouvoir tenter de capturer un Dracaufeu ou un Lippoutou sans porter atteinte à la sécurité de son ordiphone.

Cyber-risques liés à l'installation et l'usage de l'application Pokémon Go

Lancé courant juillet par la société Niantic, le jeu Pokémon Go est depuis devenu un phénomène de société, au point d'être installé sur plus de 75 millions de terminaux mobiles dans le monde. Certains acteurs malveillants ont rapidement tenté d'exploiter la popularité du jeu à des fins criminelles. Certaines précautions s'imposent donc avant de pouvoir tenter de capturer un Dracaufeu ou un Lippoutou sans porter atteinte à la sécurité de son ordiphone.

Applications malveillantes

Des sociétés spécialisées en sécurité informatique ont mis en évidence la présence de nombreuses fausses applications se faisant passer pour une version officielle du jeu. Ces applications sont susceptibles de naviguer sur des sites pornographiques pour simuler des clics sur des bannières publicitaires, de bloquer l'accès au terminal et de ne le libérer qu'en contrepartie d'une rançon, ou bien même d'installer d'autres codes malveillants. Au vu du nombre d'applications concernées (plus de 215 au 15 juillet 2016), cette technique semble très populaire, en particulier dans les pays où le jeu n'est pas encore disponible via les sites officiels.

Niveau de permissions demandées par l'application

La version initiale du jeu sur iOS présentait un problème au niveau de la gestion des permissions. En effet, le processus d'enregistrement d'un compte Pokemon Go à l'aide d'un compte Google exigeait un accès complet au profil Google de l'utilisateur.
Suite à la prise de conscience de ce problème, la société Niantic a rapidement réagi en précisant qu'il s'agissait d'une erreur lors du développement. Elle propose désormais une mise à jour pour limiter le niveau d'accès requis au profil Google de l'utilisateur. A noter que la version Android du jeu ne semble pas avoir été affectée par ce problème.
Dans le doute, il est toujours possible de révoquer cet accès en se rendant sur la page de gestion des applications autorisées à accéder à son compte Google.

Collecte de données personnelles

De par son fonctionnement, l'application collecte en permanence de nombreuses données personnelles qui sont ensuite transmises au développeur du jeu, par exemple les informations d'identité liées au compte Google ou la position du joueur obtenue par GPS. Certaines indications visuelles (nom de rue, panneaux, etc) présentes sur les photos prises avec l'application peuvent aussi fournir des indications sur la position actuelle du joueur. La désactivation du mode « réalité augmentée » lors de la phase de capture permet de se prémunir de ce type de risques (et accessoirement, de réduire l'utilisation de la batterie de l'ordiphone).

Pokemons et BYOD

Il peut être tentant d'utiliser un ordiphone professionnel pour augmenter les chances de capture d'un Ronflex. Même s'il est souvent délicat de répondre par la négative à une requête émanant d'un VIP, il semble peu opportun de déployer ce type d'application dans un environnement professionnel, en raison des différents risques évoqués précédemment.

Recommandations

Le CERT-FR recommande de n'installer que la version originale du jeu présente sur les boutiques d'Apple et de Google. En complément, il convient de désactiver la possibilité d'installer une application téléchargée depuis un site tiers (sous Android, paramètre « Sources inconnues » du menu « Sécurité »).
Il est également conseillé de vérifier les permissions demandées par l'application. La version originale du jeu nécessite uniquement :
• d'accéder à l'appareil photo pour les fonctionnalités de réalité augmentée ;
• de rechercher des comptes déjà présents sur l'appareil ;
• de localiser l'utilisateur grâce au GPS ou aux points d'accès Wi-Fi ;
• d'enregistrer localement des fichiers sur le téléphone.
Toute autre permission peut sembler suspecte et mettre en évidence la présence sur l'ordiphone d'une version altérée de l'application.
Le CERT-FR suggère de mettre en place un cloisonnement entre l'identité réelle du joueur et celle de dresseur Pokémon. Pour cela, il est possible d'ouvrir un compte directement auprès du Club des dresseurs Pokémon [8] ou bien de créer une adresse Gmail dédiée à cet usage.
Enfin, le CERT-FR déconseille de pratiquer cette activité dans des lieux où le geo-tagging du joueur pourrait avoir des conséquences (lieu de travail, sites sensibles, etc) [9]…[lire la suite]

Original de l'article mis en page : Bulletin d'actualité CERTFR-2016-ACT-031