# #Etude : La révolution des objets connectés approche


#Etude : La révolution des objets connectés approche

**A l'instar d'Internet, la prochaine révolution est en route ! C'est du moins ce que montre le sondage d'Opinion Way pour DistreeConnect. Nouvelles technologies et objets connectés sont de plus en présents dans l'esprit des Français.…**[Lire la suite ]

---

**Notre métier** : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la

Formation Professionnelle n°93 84 03041 84)
Plus d’informations sur sur cette page.

---

Réagissez à cet article

---

# Où en est la protection de nos données personnelles avec la dernière mise à jour Windows 10 ?

Où en est la protection de nos données personnelles avec la dernière mise à jour Windows 10 ?

---

**Quid de la confidentialité des données avec le déploiement de la mise à jour majeure Windows 10 Creators Update ? Cette nouvelle mouture de l'OS de Microsoft apporte son lot de nouvelles fonctionnalités et d'outils, avec un focus sur la création 3D, une démocratisation de la « réalité mixte » (la version de la réalité augmentée de l'éditeur), des améliorations portées à son navigateur Internet Edge…**

Mais la firme de Redmond a pris les devants sur le volet de la confidentialité des données avec un meilleur contrôle via les paramètres de gestion.

Ainsi, les utilisateurs vont avoir plusieurs options pour activer ou désactiver les données de localisation, les données vocales ou les données relatives à la publicité…

Mais l'éditeur va aussi jouer la carte d'une plus grande transparence concernant les données collectées. Même s'il ne sera toujours pas possible d'effectuer un « opt out » du système de collecte de la data.

Cette transparence porte donc sur les informations qui sont collectées et la manière dont elles sont ensuite exploitées.

« Nous fournissons également un résumé détaillé des données que nous collectons auprès des utilisateurs aux niveaux de base et complet de diagnostic, » explique ainsi Microsoft dans un billet dense de blog.

En effet, la firme dirigée par Satya Nadella a décidé de réduire les options de partage des données à deux (au lieu de 3 précédemment) avec les modes « basique » et « plein ».

Selon TechCrunch, le niveau basique envoie 50% moins de données à Microsoft. Tout simplement parce que Microsoft s'est rendu compte qu'autant de données n'étaient pas nécessaires en vue d'obtenir les données de diagnostic dont elle avait besoin.

Sont aussi prévus un ensemble amélioré de descriptions sur chaque paramètre de confidentialité et une déclaration de confidentialité mise à jour…[lire la suite]

*(Crédit photo : @Microsoft)*

---

**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

---

Réagissez à cet article

Source : *Windows 10 Creators Update : encore un effort sur la confidentialité des données – Free Tech & web*

# Le Wifi de votre téléphone permettra aussi de vous pister

| | |
|---|---|
| | Le Wifi de votre téléphone permettra aussi de vous pister |

**Différents projets visent à pister les personnes passant à proximité de capteurs wifi. Ce qui pose notamment la question de l'anonymisation des données.**
Marylin Gobert / La Gazette

Beaucoup de villes cherchent aujourd'hui à devenir intelligentes. Elles sont ainsi truffées de capteurs, de compteurs Linky, d'objets connectés, qui permettent de relever et de communiquer les données. Les smart cities sont devenues de véritables pompes à informations. Mais il ne faudrait pas oublier que la data est au service des citoyens. Elle vise à répondre à leurs besoins en améliorant, par exemple, la qualité du service public. Elle ne doit donc être ni intrusive, ni devenir un moyen de contrôle de la vie privée.
D'où l'importance de la protection des données à caractère personnel, définie par l'article 2 de la loi n° 78-17 du 6 janvier 1978 dite « informatique et libertés » comme « toute information relative à une personne physique identifiée ou qui peut être identifiée directement ou indirectement ».

## Des capteurs d'habitudes

La récente loi du 7 octobre 2016 pour une République numérique a encore renforcé ces principes, en affirmant la nécessaire maîtrise de l'individu sur ses données. La Commission nationale de l'informatique et des libertés (Cnil) veille notamment à leur anonymisation.
L'une des tentations actuelles est de mesurer les flux des passants, de cartographier leurs déplacements au moyen de capteurs des signaux wifi de smartphones.
L'exemple du géant de l'affichage publicitaire, JCDecaux, qui voulait placer des boîtiers dans son mobilier publicitaire, sur l'esplanade de La Défense à Paris, afin de capter les téléphones dans un rayon de 25 mètres, illustre cette tendance. Cela lui aurait permis d'estimer la fréquentation de ce quartier parisien.
Situation semblable à Rennes pour lutter contre la désertification du centre-ville. Une association de commerçants a voulu mettre en place des capteurs de signaux wifi. Le but ? Assurer un maillage de cette zone pour connaître les habitudes des consommateurs et en tirer des moyens de dynamiser le quartier…[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

---

Réagissez à cet article

Source : *L'indispensable anonymisation des données personnelles des passants*

# Limiter les risques venant des drones en les immatriculant. Une bonne idée ?

| | |
|---|---|
| | Limiter les risques venant des drones en les immatriculant. Une bonne idée ? |

**Hostile à une surveillance en réseau, le fabricant DJI propose une immatriculation électronique que seules les forces de l'ordre pourraient exploiter.**
Jean-Michel Normand

L'idée trotte dans la tête de nombre de législateurs. Installer à bord des drones de loisir un système de reconnaissance électronique fait déjà partie de l'arsenal législatif adopté l'an passé par les parlementaires français, sans pour autant que des précisions techniques aient été définies. L'Italie et le Danemark ou la FAA, l'Aviation civile américaine, l'ont également inscrit à leur programme. Dans une proposition qu'il vient de rendre publique, le fabricant de drones chinois DJI préconise une identification électronique *« simple, qui maintient un équilibre entre le respect de la vie privée de l'opérateur du drone et les légitimes préoccupations des autorités relatives à l'utilisation »* de ces appareils.

1.
Plusieurs pays, dont la France, envisagent d'imposer une signature électronique. NIR ELIAS / REUTERS

**« Comparable à une plaque d'immatriculation automobile »**
DJI est favorable à ce que tous les drones commercialisés soient capables d'émettre un signal qui indique leur localisation, mais aussi un code d'identification *« comparable à une plaque d'immatriculation automobile »* en mode électronique. Ce code serait émis sur les bandes de fréquence (2,4 GHz et 5,8 GHz) utilisées pour la liaison entre le drone et la radiocommande du pilote et pour la liaison vidéo. Il suffirait de réaliser une mise à jour des protocoles de contrôles radio existants. L'information pourrait être captée par la police ou un particulier furieux de voir un quadricoptère évoluer au-dessus de sa propriété, à condition qu'il soit équipé d'un récepteur adapté. Il lui faudra alors se tourner vers les forces de l'ordre, seules autorisées (avec les autorités aéroportuaires, notamment) à remonter jusqu'au titulaire de l'immatriculation électronique…[lire la suite]

**Commentaire de Denis JACOPINI :**
Je trouve personnellement l'idée intéressante, encore faut-il que :
1. L'émission de cette information ne puisse pas être perturbée (j'en doute) ;
2. L'émission du code du drone ne puisse pas être modifiée (plus facile) ;
3. Cette procédure soit légiférée et suivie par tous les constructeurs mondiaux.

Ceci n'empêchera pas les groupes les plus obscurs d'utiliser des drones volés non pourvus de cette signature.
A mon avis, la mise en place de ces précautions ne concernent que l'utilisateur lambda, pas ceux que l'on craint actuellement le plus sur le territoire.

---

**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

---

Réagissez à cet article

Source : *Comment immatriculer les drones de loisir*

# Ce vibromasseur connecté muni d’une caméra est vraiment trop facile à hacker

| | |
|---|---|
| | Ce vibromasseur connecté muni d’une caméra est vraiment trop facile à hacker |

**Oui, évidemment on se demande bien qui voudrait hacker ce type d'objet, pour visionner ce type d'images. Mais ainsi va le monde : le Wi-fi de ce vibromasseur connecté se pirate en deux clics.**

On ne le dira jamais assez, mais une connexion WiFi est une porte d'entrée royale pour n'importe quel hacker. Même fermée, elle est très simple à pirater. Ensuite, le pirate peut avoir accès à l'ensemble des données du trafic internet de l'objet connecté.

Photos, identifiants, mots de passe pour un téléphone, mais aussi flux *streaming* pour ce vibromasseur connecté. S'il vient à être piraté, c'est une tout autre intimité qui peut être violée.

## Vibromasseur avec hot spot WiFi

Le vibromasseur Svakom Siime Eye (disponible au prix de 249 dollars) dispose du WiFi et d'une caméra intégrée pour procéder à des *livestreams*. Les chercheurs en sécurité de Pen Test Partners ont découvert que l'interface de l'objet connecté était très simple à hacker pour toute personne se trouvant à portée de la connexion WiFi (et pourvu d'un minimum de connaissance en la matière, cela s'entend).
Un piratage d'autant plus facilité que le mot de passe par défaut de ce point d'accès WiFi est « 88888888 », soit 8 fois le chiffre 8.

## Un piratage enfantin

N'importe quelle personne à proximité du signal peut accéder au flux vidéo. Pire, en poussant leur investigation un peu plus loin, ces chercheurs sont parvenus à accéder au serveur web et à la racine de l'appareil pour configurer une connexion à distance.

Les utilisatrices qui voudraient partager ces instants intimes avec leur partenaire, pourraient se retrouver à faire de même avec leur voisin de palier. Une perspective peu réjouissante.
Le fondateur de Pen Test, Ken Munro, explique qu'il a tenté de contacter la compagnie pendant des mois avant de rendre publique ces informations.
Ce n'est pas la première fois que ce type d'objet connecté est mis au ban : le mois dernier, la société canadienne Standard Innovation a été condamnée à verser 3 millions de dollars à ses clientes pour avoir omis de mentionner qu'elle collectait leurs données personnelles via leur vibromasseur connecté et l'application dédiée.
Auteur : Elodie

---

**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

---

Réagissez à cet article

Source : *Ce vibromasseur connecté muni d'une caméra est vraiment trop facile à hacker*

---

# Alerte : Sérieuse faille WiFi. Mettez à jour vos iPhones avec la IOS 10.3.1


---

**La mise à jour 10.3.1 du système d'exploitation mobile iOS corrige une vulnérabilité permettant d'exécuter du code à distance sur les puces WiFi de Broadcom dans les iPhone, iPad et iPod. Le fabricant de puces a pu obtenir une grâce d'une dizaine de jours avant divulgation de l'exploit par l'équipe sécurité de Google, Project Zero.**

L'iPhone 7 est concerné par la faille WiFi et éligible pour la mise à jour iOS 10.3.1. (crédit : Susie Ochs)

Si vous n'avez pas mis à jour iOS pour vos terminaux mobiles Apple depuis longtemps, voici une bonne occasion de le faire. Apple a en effet lancé la version 10.3.1 de son système d'exploitation pour iPhone, iPad et iPod pour corriger une vulnérabilité permettant à un attaquant d'exécuter du code malveillant distant sur les puces WiFi Broadcom de ces terminaux. Cette vulnérabilité touche la fonction d'authentification dans le protocole 802.11r permettant aux terminaux de se connecter de façon sécurisée entre plusieurs stations de base sans fil d'un même domaine. Les hackers peuvent exploiter cette faille pour exécuter du code au sein même du firmware de la puce WiFi s'ils se trouvent à portée du réseau sans fil des terminaux visés.
Il s'agit là d'une vulnérabilité parmi d'autres trouvées par le chercheur Gal Benjamini de l'équipe de sécurité de Google, Project Zero, dans le firmware des puces Broadcom WiFi. Certaines d'entre elles concernent également les terminaux Android et ont été patchées dans le cadre du bulletin de sécurité Android d'avril. La mise à jour iOS 10.3.1, lancée lundi, est quelque peu inhabituelle car elle vient une semaine à peine après la 10.3 qui apportait pourtant un lot de correctifs touchant différents composants. L'explication pour ce court intervalle entre ces deux mises à jour est à voir du côté du délai pratiqué par Google Project Zero pour dévoiler au public les exploits de failles…[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

---

Réagissez à cet article

Source : *Apple colmate une sérieuse faille WiFi dans iOS – Le Monde Informatique*

# Les services Cloud au centre d’attaques d’entreprises par APT10

| | |
|---|---|
| | Les services Cloud au centre d’attaques d’entreprises par APT10 |

**Le groupe de pirates chinois APT10 a infiltré des services Cloud managés pour remonter aux serveurs des entreprises qui les utilisent.**

La maturité des attaques ciblées contre les entreprises est montée d'un cran. *« Un groupe de piratage a mené l'une des campagnes d'espionnage les plus prolifiques depuis l'APT1 en 2013, employant de nouvelles tactiques pour atteindre une large audience »*, a alerté PwC (Pricewaterhouse Coopers) lundi 3 avril. En collaboration avec BAE Systems et le National Cyber Security Centre (NCSC) britannique, la branche réseau du cabinet d'audit a découvert ce qu'il considère comme *« l'une des plus importantes campagnes mondiales de cyber-espionnage jamais organisées »*. Pas moins.

De quoi s'agit-il ? Du piratage des infrastructures de fournisseurs de services managés à partir desquelles les cyber-attaquants remontent aux serveurs des organisations qui y ont recours. Une opération que PwC a baptisé 'Cloud Hopper'. Les cyber-criminels derrière ces agissements seraient le groupe de hackers chinois APT10. *« PwC et BAE Systems croient que le groupe de piratage largement connu sous le nom 'APT10' a mené la campagne d'espionnage en ciblant les fournisseurs de services informatiques externalisés comme une façon d'accéder aux organisations de leurs clients à travers le monde, leur conférant un accès sans précédent à la propriété intellectuelle et aux données sensibles »*, indique PwC dans son communiqué. APT10 est le nom donné par FireEye à un groupe de pirates chinois également référencé sous les appellations Red Apollo (par PwC UK), CVNX (par BAE), Stone Panda (par CrowdStrike), et menuPass Team (plus globalement).

## Un grand volume de données exfiltrées

Les méthodes d'infection restent relativement classiques et s'appuient sur le spear-phishing, ou harponnage. Cette méthode de phishing ciblé fait appel à des techniques d'ingénierie sociale qui visent à tromper le destinataire d'un e-mail pour l'inciter à installer, à son insu, un malware ou visiter une page infectieuse, à partir desquels les pirates ouvrent une porte d'entrée sur le réseau. Objectif ici : prendre le contrôle des accès d'employés de prestataires Cloud, afin d'exploiter les canaux de communication existant entre les services managés de ces derniers et les serveurs des entreprises clientes. De la grande distribution aux technologies en passant par l'énergie, l'industrie manufacturière, le secteur public ou l'industrie pharmaceutique, tous les grands secteurs sont touchés par cette campagne…[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

---

Réagissez à cet article

Source : *Les services Cloud au centre d'attaques d'entreprises par APT10*

# Alerte : Les revendeurs informatiques de Tech Data France ciblés par un site Internet Frauduleux

Alerte : Les revendeurs informatiques de Tech Data France ciblés par un site Internet Frauduleux

**Chers revendeurs informatiques, attention à la nouvelle arnaque. Les intentions des pirates ne sont pas encore connues, mais les intentions sont forcément malveillantes.**

En tant que revendeur informatique, il est fort probable que vous commandiez votre matériel destiné à la revente ou non chez les principaux et parmis les plus anciens grossistes et importateurs Français : Ingram ou Techdata.
Une récente communication de Techdata, qui nous a été remontée par un précieux partenaire Parisien, nous informe que Techdata vient de lancer l'alerte suivante auprès de ses clients :

**Cher client,**
**Il a été porté à notre connaissance que certains Clients de TECH DATA ont reçu des emails comportant un lien internet vers un site web frauduleux leur demandant :**
**– de s'inscrire à une conférence dans laquelle TECH DATA et d'autres distributeurs participeraient,**
**– de fournir des informations type login et mot de passe de TECH DATA ainsi que d'autres informations sensibles.**
**Le site Web apparaît comme indiqué ci-dessous :**

**Veuillez noter que ce site web n'est d'aucune façon associé à TECH DATA. La sécurité de nos partenaires est une priorité pour TECH DATA et nous n'autorisons aucun tiers à collecter les identifiants de connexion de nos clients.**
**Aussi, actuellement nous œuvrons avec les autorités compétentes pour la fermeture de ce site frauduleux.**
**A ce jour, à notre connaissance les clients européens ne semblent pas affectés, ce site frauduleux visant les clients américains principalement.**
**Cependant, nous comptons sur votre vigilance et vous remercions de nous informer dans le cas où vous recevriez des emails contenant des liens vers ce site internet ou similaires en vous adressant à l'adresse suivante : itsecurity@techdata.com**
**Nous attirons votre attention sur la sophistication et l'augmentation de la cybercriminalité (phishing), dès lors restez vigilants.**
**Nous vous remercions de votre attention et collaboration.**
**Tech Data Europe**

Comme vous pouvez le remarquer, à l'instar de KPMG pourtant spécialisé en audit et conseil dans de nombreux domaines dont la sécurité informatique, pourtant victime d'une arnaque au Président leur ayant coûté plusieurs millions d'Euros (7,6) en 2014, les professionnels de l'informatique sont aussi la cible des pirates.
Nous espérons que, même si la plupart n'ont pas assisté à nos conférences de sensibilisation à la Cybercriminalité, ils sauront à quoi ressemble le loup pour ne pas le laisser rentrer dans la bergerie.

Denis JACOPINI

---

**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

---

Réagissez à cet article

Source : *E-mailing Tech Data France*

---

# Samsung Galaxy S8 ou S8+ : Une première faille de sécurité dénichée


| | |
|---|---|
| | **Samsung Galaxy S8 ou S8+ : Une première faille de sécurité dénichée** |


---

**La semaine dernière, le géant Sud-Coréen Samsung dévoilait ses nouveaux Smartphones Galaxy S8 et S8+. Un enjeu important pour le constructeur qui souhaite retrouver une image de marque suite à ses déboires avec les batteries explosives de son Note 7. Mais alors que les nouveaux modèles S8 et S8+ ne sont pas encore commercialisés, une première faille vient d'être décelée,  le système de reconnaissance faciale peut être en effet trompé par une simple photo.**

# Galaxy S8 : Le système de reconnaissance faciale déjoué par une simple photo

Quelques jours seulement après sa présentation officielle, le Samsung Galaxy S8 est déjà sous le feu des critiques. En effet, une vidéo mise en ligne le 29 mars par la chaîne iDeviceHelp montre un utilisateur déverrouiller un **Samsung Galaxy S8** à l'aide d'une simple photo. Le système de **reconnaissance faciale** censé être un procédé sécurisé montre donc déjà sa première faille !

Avec ses deux nouveaux modèles, le constructeur Samsung avait pourtant misé sur la sécurité avec la présence **d'un système de reconnaissance d'iris**, un lecteur d'empreintes digitales situé désormais au dos de l'appareil ainsi que la reconnaissance faciale, une manière rapide et aisée de déverrouiller le Galaxy S8 ou S8+…[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

---

Réagissez à cet article

Source : *Samsung Galaxy S8 ou S8+ : Une première faille de sécurité dénichée*

# Bug Butter : la plateforme collaborative de mise en relation entre pirates et forces de l’ordre

| | |
|---|---|
| | Bug Butter : la plateforme collaborative de mise en relation entre pirates et forces de l’ordre |

**La plateforme Bug Butter met en relation pirates et membres des forces de l'ordre autour d'une place de marché d'informations sensibles.**

Après les plates-formes de Bug Bounty, qui visent à mettre en relation des experts en cybersécurité avec des entreprises, une nouvelle étape vient d'être franchie dans la « *plateformisation* » des relations humaines : en partenariat avec l'ANSSI, la société OPFOR Intelligence ouvre aujourd'hui Bug Butter, la première plateforme de mise en relation entre pirates et membres des forces de l'ordre.
Bug Butter a pour ambition de fluidifier le processus d'enquête tout en permettant aux pirates de mieux gérer leur capital informationnel et leur image. La plateforme a également pour objectif de pallier le manque de moyen des services d'enquêtes, en offrant à ces derniers un outil simple et transparent capable d'optimiser le taux de résolution des affaires pour un budget donné.
La plateforme se compose de trois parties essentielles : des profils de cybercriminels, des profils de cyber-enquêteurs et, au centre, une place de marché unique en son genre.
Concrètement, Bug Butter permet aux cybercriminels de s'enregistrer sur une plateforme conçue à l'image de LinkedIn : compétences techniques, exploits réalisés, mentors, affiliations récentes avec des groupes de cybercriminels en vue, ils peuvent créer un profil complet et moderne afin d'offrir une vision complète de leurs activités.
Toutefois, et contrairement aux plateformes sociales que l'on connaît actuellement, ce profil reste pour l'essentiel privé : seul le pseudo du pirate est visible par défaut. C'est ensuite au criminel de décider quelles informations il souhaite rendre visibles, à quel prix, et -surtout- à qui.
Car outre les pirates, la plateforme est ouverte aux membres des forces de l'ordre. Ces derniers peuvent eux aussi créer leur profil de manière similaire. Nationalité, unité de rattachement, centres d'intérêt (fraude aux outils de paiement, recel, harcèlement, moeurs, renseignement…), outils maîtrisés (EnCase, i2 Analyze, Palantir…) là aussi tout est fait pour que chaque investigateur puisse donner une vision à 360° de son activité et valoriser son image…[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

---

Réagissez à cet article

Source : *Bug Butter : la plateforme collaborative de mise en relation entre pirates et forces de l'ordre*