# Un malware contamine des smartphones via Facebook Messenger

| | |
|---|---|
| | Un malware contamine des smartphones via Facebook Messenger |

**Un logiciel malveillant a fait son apparition sur l'application de messagerie de Facebook, celui-ci créerait secrètement une monnaie-virtuelle.**

Des chercheurs de la firme de cybersécurité de Trend Micro ont découvert un malware capable de miner de la crypto-monnaie, Monero. Ce virus a d'abord été observé en Corée du Sud, il agirait secrètement depuis Facebook Messenger. Nommé Digmine, ce logiciel ciblerait un maximum d'utilisateurs afin de récolter le plus de Monero possible.

Dans les faits, le malware se présenterait sous la forme d'une vidéo envoyée sur une conversation Messenger et ne serait dangereuse que si l'utilisateur l'ouvre à partir de Google Chrome. Pas de problème si on l'ouvre depuis une autre plateforme – autre navigateur ou depuis un smartphone -, même s'il existe toujours un potentiel risque que les pirates prennent le contrôle du compte Facebook de leur victime.

Crédit : Trend Micro

La présence de Digmine sur une machine pourrait également ralentir celle-ci ou tenter de se propager en contaminant les contacts de l'utilisateur. En effet, les chercheurs de Trend Micro ont affirmé que "Si le compte Facebook de l'utilisateur est configuré pour se connecter automatiquement, Digmine manipulera Facebook Messenger afin d'envoyer un lien vers le fichier aux amis du compte"…[lire la suite]

---



---

Réagissez à cet article

Source : *Un malware contamine des smartphones via Facebook Messenger | geeko*

---

# 25% des cyberattaques cibleront les objets connectés en 2020


| | |
|---|---|
| | **25% des cyberattaques cibleront les objets connectés en 2020** |


---

**L'IoT présente des problématiques de sécurité particulièrement épineuses. La majorité des objets connectés ont fait l'impasse sur la sécurité, avec des options de configuration minimales, voire inexistantes sur le sujet, et une absence de protocoles d'authentification ou d'autorisation. La majorité des objets connectés ne dispose pas d'interface qui permet aux outils de sécurité de s'y installer, ce qui rend quasi-impossible le patching et les mises à jour. Dans ce contexte, il n'est guère étonnant que les experts s'attendent à ce que 25% des cyberattaques ciblent l'Internet des Objets en 2020.**

L'expansion des réseaux IoT (objets connectés) instaure de nouvelles menaces pour la sécurité avec environ 22,5 milliards d'appareils connectés prévus d'ici 2021, selon un rapport de Business Insider. La sécurité représentera donc un défi de taille, mais les gros volumes de données engendrés par l'IoT pourraient en réalité aider les chercheurs à repérer les failles de sécurité. Encore faudrait il que les entreprises déclenchent enfin une cartographie rigoureuse de leur patrimoine informationnel. Selon une nouvelle étude de CyberArk, près de deux tiers des organisations françaises (62 %) ayant été victime d'une cyberattaque n'ont pas avoué à leurs clients que leurs données personnelles avaient été compromises.  Avec l'entrée en vigueur du Règlement Général sur la Protection des Données (RGPD) en mai 2018, les entreprises qui n'agiront pas pour être plus transparentes s'exposeront à d'importantes sanctions.La mise en place du RGPD / GDPR en mai 2018 les incite « fortement »…[lire la suite]

---



---

Réagissez à cet article

Source : *Cyberisques News – Cybersécurité : 25 Prévisions utiles pour 2018*

# Cadeaux de noël : Comprendre les risques liés aux objets connectés, c’est déjà commencer à se protéger

| | |
|---|---|
| | Cadeaux de noël : Comprendre les risques liés aux objets connectés, c’est déjà commencer à se protéger |

**Les années passent et les scandales de sécurité et de vie privée se succèdent à un rythme qui ne semble pas réduire. L'un des secteurs des technologies de l'information semble concentrer la plupart des problèmes : les objets connectés**

Récemment, la CNIL a pointé du doigt des jouets connectés a priori inoffensifs. Le problème ? Ces poupées, équipées de caméra, d'un micro et d'un haut-parleur constituent un cheval de Troie idéal pour n'importe quelle personne malveillante. Ok, mais ont-elles été l'objet d'un piratage ? Pas encore mais un produit similaire s'est récemment fait pirater causant la publication d'un peu plus de 2 millions de messages intimes sur Internet.

Avant de céder à la panique et de déménager dans un joli mais vieux corps de ferme dans le Vercors, quelques ajustements semblent nécessaires…[lire la suite]

---

**LE NET EXPERT**

**• ACCOMPAGNEMENT RGPD (ÉTAT DES LIEUX ⇒ MISE EN CONFORMITÉ)**

- **ANALYSE DE VOTRE ACTIVITÉ**
- **CARTOGRAPHIE DE VOS TRAITEMENTS DE DONNÉES**
- **IDENTIFICATION DES RISQUES**
- **ANALYSE DE RISQUE (PIA / DPIA)**
- **MISE EN CONFORMITÉ RGPD** de vos traitements
- **SUIVI** de l'évolution de vos traitements

**• FORMATIONS / SENSIBILISATION** :

- **CYBERCRIMINALITÉ**
- **PROTECTION DES DONNÉES PERSONNELLES**
- AU **RGPD**
- À LA **FONCTION DE DPO**

**• RECHERCHE DE PREUVES** (outils Gendarmerie/Police)

- ORDINATEURS (**Photos / E-mails / Fichiers**)
- TÉLÉPHONES (récupération de **Photos / SMS**)
- SYSTÈMES NUMÉRIQUES

**• EXPERTISES** & **AUDITS** (certifié ISO 27005)

- TECHNIQUES | JUDICIAIRES | ADMINISTRATIVES
- **SÉCURITÉ** INFORMATIQUE
- SYSTÈMES DE **VOTES ÉLECTRONIQUES**

**Besoin d'un Expert ? contactez-nous**

Notre Expert, Denis JACOPINI, est assermenté, spécialisé en **Cybercriminalité**, **Recherche de preuves** et en **Protection des données personnelles**. Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), en Droit de l'Expertise Judiciaire et certifié en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005), Denis JACOPINI est aussi formateur inscrit auprès de la DDRTEFP (Numéro formateur n°93 84 03041 84).

---

Réagissez à cet article

Source : *Comprendre les risques liés aux objets connectés, c'est déjà commencer à se protéger – Tech – Numerama*

---

# Transmission de données de WHATSAPP à FACEBOOK : mise en demeure publique pour absence de base légale


**La présidente de la CNIL met la société WHATSAPP en demeure de procéder légalement à la transmission des données de ses utilisateurs à FACEBOOK, notamment en obtenant leur consentement. En 2014, la société WHATSAPP a été rachetée par la société FACEBOOK Inc.…**[Lire la suite ]

---

Denis JACOPINI anime des **conférences, des formations** sur la mise en conformité CNIL, des formations sur la protection des données Personnelles et est régulièrement invité à des **tables rondes en France et à l'étranger** pour sensibiliser les

décideurs et les utilisateurs aux **obligations et moyens de se mettre en conformité avec le RGPD, futur règlement européen relatif à la Protection des Données Personnelles** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Plus d'informations sur notre page formations.

---

Réagissez à cet article

---

# HTTPS ou le cadenas du navigateur ne veulent pas dire que le site est fiable !


HTTPS ou le cadenas du navigateur ne veulent pas dire que le site est fiable !

---

**Depuis plusieurs années j'entends des « professionnels » de l'informatique recommander à leur client de bien vérifier la présence d'un cadenas ou d'une adresse qui commence par « https » lorsqu'ils échangent des données sensibles (mots de passe, numéros de CB…). Sans autre conseil, selon Denis JACOPINI, cette recommandation ne vaut rien.**

**Le Net Expert : Qu'indiquent le Cadenas ou le S de httpS ?**

**Denis JACOPINI** : Le **protocole HTTPS** (HyperText Transfer Protocol Secure) est la combinaison du **HTTP** avec un protocole de chiffrement tel que le **TLS** ou le **SSL**. Il est particulièrement utilisé sur le Web par les réseaux sociaux et dans les secteurs bancaires et de l'e-commerce pour sécuriser les pages sensibles (page d'authentification, mon compte, page de paiement).

**Le Net Expert : Qu'apporte alors la sécurité du HTTPS ou du cadenas ?**

**D. J.** : Lorsqu'on navigue sur un site dont l'URL (l'adresse internet) commence par « HTTPS » (par exemple http**s**://www.lenetexpert.fr), ceci ne veut pas dire que le site internet est de confiance ou fiable. Cela signifie simplement que la communication entre votre ordinateur et le site Internet sera chiffrée (cryptée) afin qu'un espion ou un pirate connecté sur votre Wifi ou votre LAN avec des outils d'espionnage numérique (un sniffer ou un Main In The Middle) ne puisse « écouter » ou « capter » le contenu de l'échange. Ceci garanti la confidentialité des échanges entre votre ordinateur et le site Internet et seulement la confidentialité entre votre ordinateur et le site Internet, ni la confiance, ni autre chose.

Il n'y a aucun rapport entre la présence d'un http**s** et la confiance que l'on peut accorder à un site Internet et d'ailleurs, il existe une multitude de moyens de créer une page web accessible via une URL ayant la sécurité http**s**.

• Hébergement gratuit en http**s**

• Hébergement payant créer un site internet sur un hébergement gratuit

• Ajouter un certificat SSL gratuit

• Utiliser un dossier sous un domaine avec certificat

Ainsi, la présence d'un http**s** ou d'un cadenas ne devrait pas être suffisant pour être un cyberacheteur confiant. D'autres éléments devraient être utilisés tels que l'existence d'avis sur le site Internet, l'absence de réponse à la recherche du « nom du site Internet » accolé au mot « arnaque » (sauf si c'est un site qui justement traite des arnaques !).

De plus, une recherche sur le nom de domaine à partir de « whois.com » devrait vous donner des indications sur l'ancienneté du nom de domaine, l'adresse du propriétaire du nom de domaine qui devrait coïncider avec le propriétaire de la boutique dans laquelle vous vous apprêtez à faire vos achats.

Enfin, une boutique en français affichant des conditions générales de ventes en français indiquant que le site internet est soumis à la loi française avec un numéro SIRET facilement vérifiable sur « societe.com »et une rubrique destinée à la protection des données personnelles a de grandes chances de vous assurer une certaine tranquillité.

Tout comme dans le monde des boutiques physiques il existe des cybercommerçants sérieux et fiables mais si vous devez acheter un produit sur Internet et que vous le trouvez sur une boutique moins cher que partout ailleurs, posez-vous des questions. Privilégiez les boutiques de confiance dont le siège social est en France (vous protégeant ainsi par les lois françaises très protectrices des consommateurs). A moins de passer par un tiers de confiance, évitez d'acheter sur les boutiques internet situées dans des pays étrangers en dehors de l'Europe. En cas de litige, risque d'être difficile la contestation.

Certes avoir un cadenas sur votre navigateur et une adresse internet avec un http**s** sont essentiels pour communiquer des informations confidentielles telles que des mots de passe ou des coordonnées de cartes bancaires mais la réputation de la boutique ou sa situation géographique sont des éléments tout aussi importants.

*Les informations contenues dans nos publications sont destinées à vous sensibilisées et augmenter votre niveau de prudence et en aucun cas dans un but de vous inciter à les utiliser dans un but malveillant.*

---



---

Réagissez à cet article

Source : *Denis JACOPINI*

---

# Les infos bancaires de clients CDiscount piratées, 300.000 euros détournés

Les infos bancaires de clients CDiscount piratées, 300.000 euros détournés

---

**Les plaintes s'accumulaient depuis juin pour atteindre un total de 491. Déposées par des clients du site de vente en ligne CDiscount, elles ont amené les enquêteurs sur la piste d'une bande de pirates basée dans la Drôme, a rapporté jeudi France Bleu. Sept personnes arrêtées. Mardi, dans la Drôme, la police a interpellé sept personnes, tous issus d'une même famille. L'opération, menée par une cinquante policiers, a eu lieu à Valence, à Bourg-Lès-Valence et à Loriol-sur-Drôme. Elles ont cependant été remises en liberté car l'enquête n'est pas terminée. Les enquêteurs veulent désormais savoir s'il existe d'autres pirates et si des détournements ont aussi eu lieu sur d'autres sites de ventes en ligne.**

Les plaintes s'accumulaient depuis juin pour atteindre un total de 491. Déposées par des clients du site de vente en ligne CDiscount, elles ont amené les enquêteurs sur la piste d'une bande de pirates basée dans la Drôme, a rapporté jeudi France Bleu.

**Sept personnes arrêtées.** Mardi, dans la Drôme, la police a interpellé sept personnes, tous issus d'une même famille. L'opération, menée par une cinquante policiers, a eu lieu à Valence, à Bourg-Lès-Valence et à Loriol-sur-Drôme. Elles ont cependant été remises en liberté car l'enquête n'est pas terminée. Les enquêteurs veulent désormais savoir s'il existe d'autres pirates et si des détournements ont aussi eu lieu sur d'autres sites de ventes en ligne…[lire la suite]

---



---

Réagissez à cet article

Source : *En piratant les infos bancaires de clients sur CDiscount, des pirates détournent 300.000 euros*

# RGPD : Ca ne se passera plus comme ça !

RGPD : Ca ne se passera plus comme ça !

**Selon une nouvelle étude de CyberArk, près de deux tiers des organisations françaises (62 %) ayant été victime d'une cyberattaque n'ont pas avoué à leurs clients que leurs données personnelles avaient été compromises. Avec l'entrée en vigueur du Règlement Général sur la Protection des Données (RGPD) en mai 2018, les entreprises qui n'agiront pas pour être plus transparentes s'exposeront à d'importantes sanctions.**

« Malheureusement, il n'est pas rare que les organisations décident de cacher l'ampleur des dégâts causés par une cyberattaque. Comme nous l'avons vu lors des violations de données chez Yahoo !, Uber et bien d'autres, les entreprises peuvent soit dissimuler des informations intentionnellement, soit constater que l'attaque a finalement été plus nuisible que précédemment annoncé, déclare Jean-François Pruvot, Regional Director Europe West and South Europe, Sales chez CyberArk. Dès l'année prochaine, ce type de comportement sera lourdement sanctionné, en raison des amendes qui seront infligées en vertu du RGPD en cas de manque de conformité. L'autre point étonnant de cette étude réside dans cette obstination à appliquer des pratiques dépassées en matière de sécurité, et le manque de cohésion entre les leaders commerciaux et les responsables de la sécurité IT, malgré leur capacité à identifier les risques encourus et les cyberattaques qui font sans cesse la une des journaux. »…[lire la suite]

**Complément de Denis JACOPINI :**

À partir du 25 mais 2018 les entreprises, filiales ou agences françaises ont obligation de signaler à la CNIL tout vol de données ou piratage ayant entraîné une exposition des données détenues auprès de personnes non autorisées.

Pour qu'il y ait violation, 3 conditions doivent être réunies :

• Vous avez mis en œuvre un traitement de données personnelles ;

• Ces données ont fait l'objet d'une violation (destruction, perte, altération, divulgation ou un accès non autorisé à des données personnelles, de manière accidentelle ou illicite) ;

• Cette violation est intervenue dans le cadre de votre activité de fourniture de services de communications électroniques (par exemple, lors de la fourniture de votre service de téléphonie ou d'accès à d'internet).

La notification doit être transmise à la CNIL dans les 24h de la constatation de la violation. Si vous ne pouvez pas fournir toutes les informations requises dans ce délai car des investigations complémentaires sont nécessaires, vous pouvez procéder à une notification en deux temps :

Une notification initiale dans les 24 heures de la constatation de la violation ;

Puis, une notification complémentaire dans le délai de 72 heures après la notification initiale.

Le formulaire à utiliser est celui-ci :

https://www.cnil.fr/sites/default/files/typo/document/CNIL_Formulaire_Notification_de_Violations.pdf

---

Besoin d'un **accompagnement pour vous mettre en conformité avec le RGPD ?** ?

Besoin d'une **formation pour apprendre à vous mettre en conformité avec le RGPD** ?

Contactez-nous

---

A Lire aussi :

Mise en conformité RGPD : Mode d'emploi

Formation RGPD : L'essentiel sur le règlement Européen pour la Protection des Données Personnelles

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 étapes

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 : Formation RGPD : L'essentiel sur le règlement Européen pour la Protection des Données Personnelles

---

Réagissez à cet article

Source : CNIL et *Enquête CyberArk : 62 % des entreprises françaises n'ont pas signalé des violations de données à leurs clients – Global Security Mag Online*

# DarkNet : Découverte d’une base de données de 1,4 milliards d’identifiants et mots de passe en clair

DarkNet : Découverte d’une base de données de 1,4 milliards d’identifiants et mots de passe en clair

**Open data chez les cybercriminels ! La découverte a été annoncée par la société spécialisée en sécurité informatique 4iQ. Il s'agit de la plus importante base de données pirate jamais découverte en ligne. Elle pèse 41 Go.**

La découverte de 4iQ date du 5 décembre et la société indique qu'elle se trouve sur un espace du Dark Web, sans préciser l'endroit (on se doute bine pourquoi). La base de donnée en question contient exactement ***1 400 553 869 identifiants et mots de passe en clair***, et un moteur de recherche dédié permet d'y accéder et d'y naviguer. Du vrai open data chez les pirates !…

[…]

[…]

N'oubliez pas les règles de sécurité pour réduire les risques de piratage de vos comptes ne ligne : changez régulièrement vos mots de passe, utilisez un générateur de mot de passe sécurisé (ou activez la double authentification lorsque c'est possible) et stockez vos identifiants / mots de passe de manière sécurisée via un gestionnaire de mot de passe…[lire la suite]

---



---

Réagissez à cet article

Source : *DarkNet : Découverte d’une base de données de 1,4 milliards d’identifiants et mots de passe en clair | UnderNews*

---

# RGPD : Vol de données : la nouvelle norme

RGPD : Vol de données : la nouvelle norme

---

**A six mois de l'entrée en vigueur du nouveau règlement européen sur la protection des données personnelles (RGPD) le 25 mai 2018 prochain, Proofpoint, spécialiste de la cybersécurité, dévoile les résultats de son étude paneuropéenne (Royaume-Uni, France, Allemagne) analysant le niveau de préparation des entreprises.**

Les cyberattaques sont malheureusement devenues monnaie courante pour les entreprises qui doivent désormais intégrer pleinement les risques associés à leurs stratégies de sécurité pour se protéger. A l'image du piratage d'Equifax exposant les données personnelles de plus de 145 millions de citoyens américains ou du ransomware Wannacry ayant affecté plus de 200,000 ordinateurs dans 150 pays, tout le monde est concerné.

La France, semble particulièrement affectée, avec 61% des entreprises françaises qui déclarent avoir subi un vol de données personnelles durant les deux années écoulées (54% au Royaume Uni et 56% en Allemagne) et 78% d'entre elles qui redoutent un vol de données dans les 12 mois à venir (54% au Royaume-Uni et 46% en Allemagne).

**Niveau de préparation RGPD : un décalage évident entre perception et réalité**

Si les décideurs IT français semblent mieux préparés que leurs voisins (51% des répondants français pensent que leur organisation est déjà en conformité avec la réglementation RGPD, contre 45% au Royaume-Uni et 35% en Allemagne), l'étude révèle que plus d'une entreprise française sur cinq (22%) ne sera toujours pas en conformité avec la réglementation lors de son entrée en vigueur en mai 2018 (23% au Royaume-Uni et 34% en Allemagne). Un résultat finalement peu surprenant, considérant que seules 5% des entreprises auraient effectivement mis en place toutes les stratégies de gestion de données nécessaires pour garantir cette mise en conformité.

Les décideurs IT semblent pourtant conscients des enjeux, puisque 66% des répondants confient que leur budget a augmenté en prévision de l'entrée en vigueur de RGPD. Plus de sept entreprises sur dix en Europe ont par ailleurs monté des équipes projet dédiées RGPD et plus d'une sur quatre a désigné un responsable de la protection des données. A l'épreuve des faits, et alors que les entreprises avaient deux ans pour se préparer (adoption de la réglementation en avril 2016), seuls 40% des répondants révèlent que leur organisation a rempli un formulaire de mise en conformité RGPD…[lire la suite]

---



---

Réagissez à cet article

Source : *RGPD : 1 entreprise française sur 5 ne sera pas en conformité ! | UnderNews*

---

# Jouets connectés : Dangers pour votre vie privée dit la CNIL


| | |
|---|---|
| | **Jouets connectés : Dangers pour votre vie privée dit la CNIL** |


---

**La Présidente de la CNIL met en demeure la société GENESIS INDUSTRIES LIMITED de procéder à la sécurisation de jouets connectés à destination d'enfants : la poupée « My Friend Cayla » et le robot « I-QUE ».**

Le robot « I-QUE » et la poupée « My Friend Cayla » sont des jouets dits « connectés ». Ils répondent aux questions posées par les enfants sur divers sujets tels que des calculs mathématiques ou encore la météo. Les jouets sont équipés d'un microphone et d'un haut-parleur et sont associés à une application mobile téléchargeable sur téléphone mobile ou sur tablette. La réponse est extraite d'Internet par l'application et donnée à l'enfant par l'intermédiaire des jouets.

Alertée, en décembre 2016, par une association de consommateurs sur le défaut de sécurité des deux jouets, la Présidente de la CNIL a décidé de réaliser des contrôles en ligne en janvier et novembre 2017. Elle a par ailleurs adressé un questionnaire en mars 2017 à la société située à Hong-Kong.

Ces vérifications ont permis de relever que la société collecte une multitude d'informations personnelles sur les enfants et leur entourage : les voix, le contenu des conversations échangées avec les jouets (qui peut révéler des données identifiantes comme une adresse, un nom…) mais également des informations renseignées dans un formulaire de l'application « My Friend Cayla App ».

Plusieurs manquements à loi Informatique et Libertés ont été constatés dont notamment :

1.

## Le non-respect de la vie privée des personnes en raison d'un défaut de sécurité

Les contrôleurs de la CNIL ont constaté qu'une personne située à 9 mètres des jouets à l'extérieur d'un bâtiment, peut connecter (ou « appairer ») un téléphone mobile aux jouets grâce au standard de communication Bluetooth sans avoir à s'authentifier (par exemple, avec un code PIN ou un bouton sur le jouet).

La personne située à une telle distance est en mesure d'entendre et d'enregistrer les paroles échangées entre l'enfant et le jouet ou encore toute conversation se déroulant à proximité de celui-ci.

La délégation de la CNIL a également relevé qu'il était possible de communiquer avec l'enfant situé à proximité de l'objet par deux techniques :

• soit en diffusant via l'enceinte du jouet des sons ou des propos précédemment enregistrés grâce à la fonction dictaphone de certains téléphones ;

• soit en utilisant les jouets en tant que « kit main libre ». Il suffit alors d'appeler le téléphone connecté au jouet avec un autre téléphone pour parler avec l'enfant à proximité du jouet.

La Présidente a considéré que l'absence de sécurisation des jouets, permettant à toute personne possédant un dispositif équipé d'un système de communication Bluetooth de s'y connecter, à l'insu des enfants et des propriétaires des jouets et d'avoir accès aux discussions échangées dans un cercle familial ou amical, méconnait l'article 1er de la loi Informatique et Libertés selon lequel l'informatique *« ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques ».*

2.

## Le défaut d'information des utilisateurs des jouets

Alors que des informations personnelles sont traitées par la société, les contrôleurs de la CNIL ont constaté que les utilisateurs des jouets ne sont pas informés des traitements de données mis en œuvre par la société…[lire la suite]

---



---

Réagissez à cet article

Source : *Jouets connectés : mise en demeure publique pour atteinte grave à la vie privée en raison d'un défaut de sécurité | CNIL*