

# Une robotique polymorphe et multifonction



Une robotique polymorphe et multifonction

Bientôt les drones se métamorphoseront en quelques secondes en voitures robotiques, prévoient des chercheurs suisses, qui ont mis au point un nouveau type de « matière programmable ». Leur dispositif change de forme à volonté en réagissant à la température...[Lire la suite ]

---

Denis JACOPINI anime des **conférences**, des **formations** en Cybercriminalité et est régulièrement invité à des **tables rondes en France et à l'étranger** pour sensibiliser les décideurs et les utilisateurs aux **Dangers liés à la Cybercriminalité (Arnaques, Piratages...)** pour mieux s'en **protéger** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84). Plus d'informations sur cette page.

---



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

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



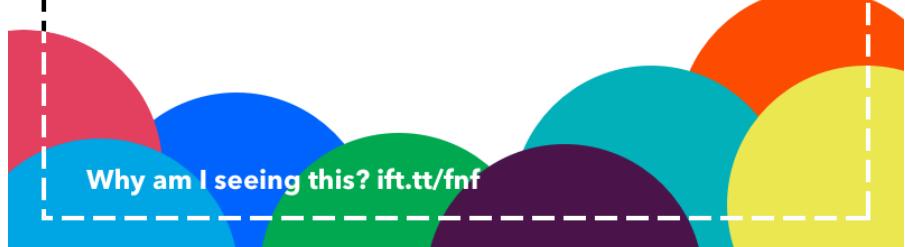
[Contactez-nous](#)

Réagissez à cet article

---

## Une robotique polymorphe et multifonction

### File not found



Why am I seeing this? [ift.tt/fnf](http://ift.tt/fnf)

Une robotique polymorphe et multifonction

Bientôt les drones se métamorphoseront en quelques secondes en

**voitures robotiques, prévoient des chercheurs suisses, qui ont mis au point un nouveau type de « matière programmable ». Leur dispositif change de forme à volonté en réagissant à la température....**[Lire la suite ]

---

Denis JACOPINI anime des **conférences, des formations** en Cybercriminalité et est régulièrement invité à des **tables rondes en France et à l'étranger** pour sensibiliser les décideurs et les utilisateurs aux **Dangers liés à la Cybercriminalité (Arnaques, Piratages...)** pour mieux s'en protéger (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).

Plus d'informations sur cette page.

---



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

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



[Contactez-nous](#)

Réagissez à cet article

---

# Une robotique polymorphe et multifonction



Une robotique polymorphe et multifonction

Bientôt les drones se métamorphoseront en quelques secondes en voitures robotiques, prévoient des chercheurs suisses, qui ont mis au point un nouveau type de « matière programmable ». Leur dispositif change de forme à volonté en réagissant à la température...[Lire la suite ]

---

Denis JACOPINI anime des **conférences**, des **formations** en Cybercriminalité et est régulièrement invité à des **tables rondes en France et à l'étranger** pour sensibiliser les décideurs et les utilisateurs aux **Dangers liés à la Cybercriminalité (Arnaques, Piratages...)** pour mieux s'en **protéger** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84). Plus d'informations sur cette page.

---



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

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



Consultant en Cybercriminalité et en Protection des Données Personnelles

[Contactez-nous](#)

Réagissez à cet article

# Une robotique polymorphe et multifonction

**File not found**

Une robotique polymorphe et multifonction

Why am I seeing this? [ift.tt/fnf](http://ift.tt/fnf)

Bientôt les drones se métamorphosent en quelques secondes en

**voitures robotiques, prévoient des chercheurs suisses, qui ont mis au point un nouveau type de « matière programmable ». Leur dispositif change de forme à volonté en réagissant à la température....**[Lire la suite ]

---

Denis JACOPINI anime des **conférences, des formations** en Cybercriminalité et est régulièrement invité à des **tables rondes en France et à l'étranger** pour sensibiliser les décideurs et les utilisateurs aux **Dangers liés à la Cybercriminalité (Arnaques, Piratages...)** pour mieux s'en protéger (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).

Plus d'informations sur cette page.

---



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

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



[Contactez-nous](#)

Réagissez à cet article

---

# Une robotique polymorphe et multifonction



Une robotique polymorphe et multifonction

Bientôt les drones se métamorphoseront en quelques secondes en voitures robotiques, prévoient des chercheurs suisses, qui ont mis au point un nouveau type de « matière programmable ». Leur dispositif change de forme à volonté en réagissant à la température...[Lire la suite ]

---

Denis JACOPINI anime des **conférences**, des **formations** en Cybercriminalité et est régulièrement invité à des **tables rondes en France et à l'étranger** pour sensibiliser les décideurs et les utilisateurs aux **Dangers liés à la Cybercriminalité (Arnaques, Piratages...)** pour mieux s'en **protéger** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84). Plus d'informations sur cette page.

---



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

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

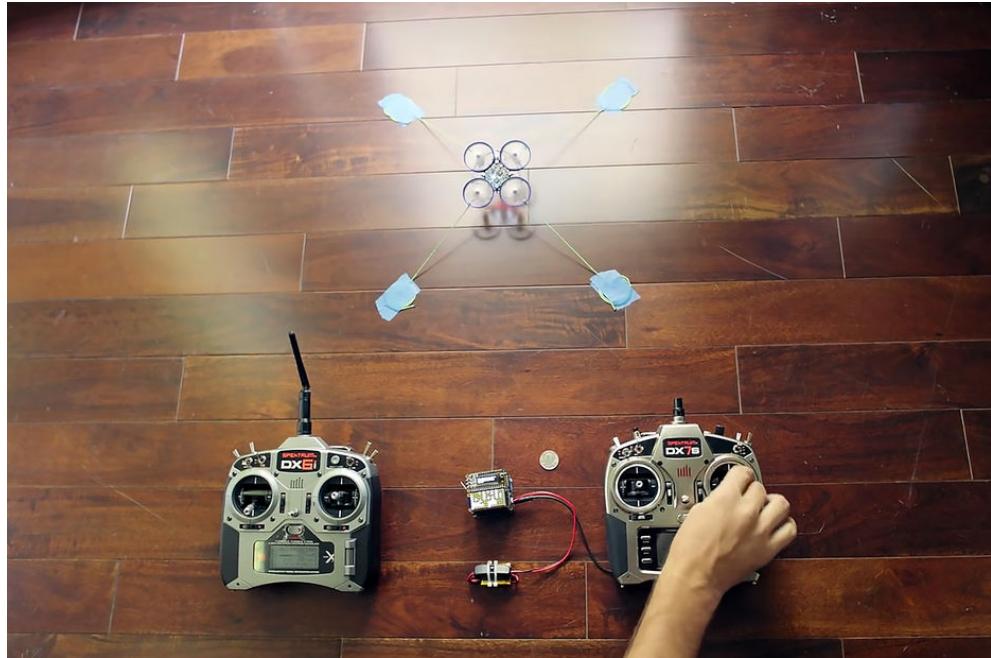


[Contactez-nous](#)

Réagissez à cet article

---

# Un chercheur a découvert comment pirater n'importe quel drone



Un chercheur a découvert comment pirater n'importe quel drone

**Gare à vous si vous possédez un drone ! Un chercheur vient de démontrer qu'il est possible de prendre le contrôle total d'un appareil radiocommandé dès lors qu'il utilise le protocole DSMx, très répandu. Une faille d'autant plus sérieuse qu'il sera très difficile d'y remédier rapidement.**

Les drones récréatifs sont aussi populaires que difficiles à contrôler pour les forces de l'ordre, les sites industriels ou même la DGAC (Direction générale de l'aviation civile). Les choses ne risquent malheureusement pas de s'améliorer avec l'annonce par Jonathan Andersson, un chercheur en sécurité informatique travaillant chez Trend Micro, qu'ils peuvent être facilement piratés en vol.

#### **PRENDRE LE CONTRÔLE DE N'IMPORTE QUEL DRONE**

Il a présenté le 26 octobre à la conférence PacSec 2016 un transmetteur radio qu'il a nommé Icarus. Celui-ci est capable de prendre le contrôle de n'importe quel appareil en vol en détectant puis usurpant sa connexion avec la télécommande, tant qu'elle utilise le protocole DSMx. Et celui-ci est justement très utilisé dans le monde des drones, mais aussi de tout autre type d'appareil à radiocommande (avions, hélicoptères, voitures, bateaux...). Une fois que l'attaquant a pris le contrôle, le propriétaire du drone n'y a plus du tout accès.

#### **PAS DE REMÈDE MIRACLE**

D'un côté, cette technologie pourrait hypothétiquement être utilisée par les autorités pour intercepter de manière sécurisée des drones présentant des risques. Icarus permet en effet d'identifier très précisément chaque appareil en fonction de la fréquence qu'il utilise. Mais de l'autre, elle pourrait tout aussi bien servir à des personnes mal intentionnées, que ce soit pour commettre des actes de délinquances contre des entreprises utilisant des drones, précipiter un appareil grand public sur des passants, voire pirater les drones qu'utilisent les forces de l'ordre...

La balle est désormais dans le camp des constructeurs, mais il n'y aura pas de solution miracle. La majorité des équipements concernés ne pourra pas être mise à jour et les sécuriser impliquerait de devoir changer à la fois l'émetteur et le récepteur. Quant à l'arrivée d'un nouveau protocole de communication plus sécurisé, elle n'est qu'une solution à long terme, qui prendra des années à se mettre en place.

Comme le rapporte Ars Technica, c'est la première fois qu'un chercheur fait la démonstration publique d'une solution complète de ce type, même si plusieurs expériences auraient été réalisées en privé par le passé. Le problème, c'est que même si la démonstration de Jonathan Andersson n'est qu'une preuve de concept, il semble probable que ce type d'appareil se retrouve tôt ou tard dans la nature

#### **DÉMONSTRATION D'ICARUS EN VIDÉO**

[[Lien vers l'article original de l'Usine Digitale](#)]

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, contenus, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



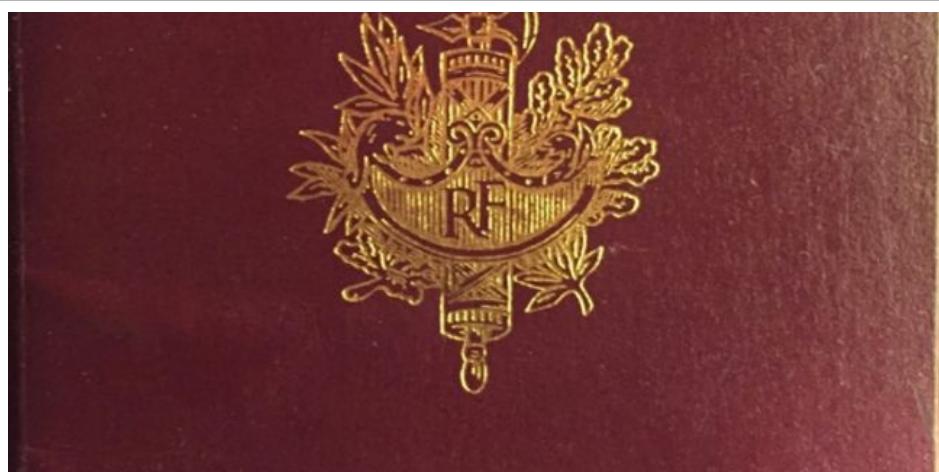
[Contactez-nous](#)

Réagissez à cet article

Original de l'article mis en page : [Vidéo] Un chercheur a découvert comment pirater n'importe quel drone

---

**60 millions de Français  
fichés dans une base de  
données commune des titres  
d'identité**



**60 millions  
de Français  
fichés dans  
une base de  
données  
commune des  
titres  
d'identité**

## **Un décret publié pendant le pont de la Toussaint officialise la création d'un gigantesque fichier national.**

Soixante millions de Français glissés, à l'occasion d'un week-end de pont de la Toussaint, dans une même base de données : un décret paru au Journal officiel dimanche 30 octobre, et repéré par le site NextImpact, officialise la création d'un « traitement de données à caractère personnel commun aux passeports et aux cartes nationales d'identité ». En clair, les données personnelles et biométriques de tous les détenteurs d'une carte d'identité ou d'un passeport seront désormais compilées dans un fichier unique, baptisé « Titres électroniques sécurisés » (TES). Cette base de données remplacera à terme le précédent TES (dédié aux passeports) et le Fichier national de gestion (dédié aux cartes d'identité), combinés dans ce nouveau fichier.

La base de données rassemblera ainsi des informations comme la photo numérisée du visage, les empreintes digitales, la couleur des yeux, les adresses physiques et numériques... Au total, la quasi-totalité des Français y figurera, puisqu'il suffit de détenir ou d'avoir détenu une carte d'identité ou un passeport pour en faire partie – les données sont conservées quinze (pour les passeports) à vingt ans (pour les cartes d'identité)...[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.



[Contactez-nous](#)

Réagissez à cet article

Original de l'article mis en page : 60 millions de Français fichés dans une base de données commune des titres d'identité

# Les protections de Windows complètement inefficaces à la technique AtomBombing !



Les protections de Windows complètement inefficaces à la technique AtomBombing !

**Des chercheurs en sécurité ont découvert un mécanisme qui exploite une propriété propre à Windows pour en contourner tous les mécanismes de protection.**

Une véritable bombe atomique pour l'intégrité de Windows. Une équipe de chercheurs de la société de sécurité israélienne Ensilo déclare avoir trouvé un moyen qui permet à un code malveillant de contourner toutes les barrières de sécurité possibles et inimaginables de l'OS de Microsoft. Et quelle que soit sa version. En l'occurrence, les experts ont effectué leurs travaux sur Windows 10.

La technique, qu'ils ont dénommée « AtomBombing » exploite les « Atom Tables ». Inhérentes au système d'exploitation, ces tables permettent aux applications de stocker les données et y accéder. Elles peuvent aussi être utilisées pour organiser le partage des informations entre les applications. « *Nous avons découvert qu'un attaquant pouvait écrire du code malveillant dans une table atom et forcer un programme légitime à récupérer ce code depuis la table*, explique le responsable de l'équipe de recherche Tal Liberman. Nous avons également constaté que le programme légitime, maintenant infecté du code malveillant, peut être manipulé pour exécuter ce code. » De plus amples détails sur la technique d'intrusion sont présentés sur cette page.

## Pas de correctif possible

Ce n'est évidemment pas le premier cas connu de technique d'injection de code pour pénétrer le système et affaiblir son intégrité. Mais ces techniques s'appuient généralement sur des vulnérabilités de l'OS et la manipulation de son utilisateur amené, sans en avoir conscience, à déclencher l'exécution d'un code malveillant à travers un programme, comme un navigateur par exemple, pour contourner les barrières de sécurité.

Mais rien de tout cela dans le cas présent. « *AtomBombing est exécuté simplement en utilisant les mécanismes sous-jacents à Windows. Il n'est pas nécessaire d'exploiter les bugs ou les vulnérabilités du système d'exploitation*, assure le chercheur. Comme la question ne peut être résolue, il n'y a pas de notion de correctif. Ainsi, la réponse pour atténuer [le risque] serait de plonger dans les appels des API et de surveiller les activités malveillantes. » Autrement dit, pas de correctif possible mais du monitoring système en temps réel en quelque sorte (comme en propose au passage Ensilo). L'autre solution serait que Microsoft modifie l'architecture de Windows. Ce qui n'est pas prévu dans l'immédiat.

Ensilo reste discret – et c'est bien normal – sur la méthode pour injecter le code. A notre sens, l'exécution d'un tel script nécessite soit la complicité involontaire de son utilisateur (ce qui n'est pas nécessairement le plus compliqué), soit l'accès direct à une machine non protégée. En cas de succès, l'AtomBombing fait alors tomber toutes les barrières de protection selon les niveaux de restriction, peut accéder à des données spécifiques, y compris les mots de passe chiffrés, ou encore s'installer dans le navigateur pour en suivre toutes les opérations. Explosif !

---

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 : <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.

# Pourquoi les objets connectés sont un danger pour l'Internet ?



Pourquoi les objets connectés sont un danger pour l'Internet ?

---

Plusieurs grands sites Internet ont vu leurs services perturbés vendredi soir suite à une attaque contre une partie de l'infrastructure du réseau global. Cette attaque est partiellement imputable car elle n'est que la dernière manifestation d'un phénomène en place assez longtemps : le piratage d'objets connectés qui menacent pour constituer des réseaux offensifs. Un filtre de DDOS sera difficile à empêcher.

Une attaque de grande ampleur a eu lieu vendredi 21 octobre 2016, mettant hors service pendant quelques heures plusieurs grands sites Internet comme Amazon, Netflix, Twitter, Reddit, Spotify ou Tumblr. Ces sites n'étaient pas directement sous le coup d'une attaque, ils ont été les victimes collatérales d'une attaque contre Dyn, une entreprise dont les services font d'elle une infrastructure critique d'Internet : Dyn gère un service DNS (système de nom de domaine), qui permet de corrélérer un nom de domaine (comme « [voile-digital.fr](#) ») avec une adresse IP et vice versa.

Ce qui est notable ici, c'est qu'il ne s'agissait pas d'une attaque sophisticated, soigneusement mise en œuvre par un groupe d'experts. Non, il s'agissait d'une attaque par déni de service distribué (DDoS) – autrement dit une attaque ayant pour but de rendre un service indisponible au moyen d'informations fausses – s'appuyant principalement sur le botnet Mirai, qui a identifié le cabinet d'analyse Flappoint. Les botnets ne sont pas nouveaux, il s'agit de réseaux de machines dont un malveillant a pris le contrôle et qui peuvent être utilisées à tout moment pour mener une attaque coordonnée. Traditionnellement, les attaques informatiques visent des ordinateurs dont les noms à jour de sécurité n'avaient pas été faites. Mais les progrès en matière d'automatisation et de sofware d'attaque modernes ont rendu ces réseaux tout à fait utilisables pour ce type d'attaques.

La différence avec Mirai, c'est qu'il s'attaque aux objets connectés. Son mode opérant est un peu plus simple : il parcourt Internet en cherchant à se connecter à toutes les adresses telles qu'il trouve avec une liste de passe par défaut (dont le classique admin/admin). Une fois l'appareil infecté, Mirai en bloque certains ports pour empêcher qu'on en reprenne le contrôle. Le behavior est basique, rapide, efficace, et surtout disponible gratuitement pour quiconque souhaite s'amuser avec, car son créateur a rendu le code public. De plus, contrairement aux ordinateurs, un botnet d'objets connectés n'a vraiment utilité réelle autre qu'effectuer des attaques par déni de service. Le fait que les objets connectés ont tendance à être silencieux 24h/24 et 7/7 facilie aussi cet usage.

**Impact de l'attaque contre Dyn, réalisée par Level3 Communications**

Le résultat est une arme dont la puissance est absolument démesurée par rapport à son accessibilité. En septembre 2016, le blog du journaliste spécialisé Brian Krebs avait été frappé par une attaque record atteignant un débit de 1.2Gb/s. Une semaine plus tard, c'est l'hébergeur français OVH qui avait été visé, avec une puissance de frappe estimée à 1,7Gb/s. L'attaque contre Dyn, survenue un mois plus tard, semble être à nouveau mondiale d'un cran. Quels sont les objets connectés utilisés par Mirai ? On y trouve beaucoup de caméras de surveillance et d'enregistreurs numériques (DVR), principalement fabriqués par une seule entreprise : Hangzhou Kangnian Technology. A noter que d'autres botnets pourraient également avoir participé à l'attaque. De connaît l'existence d'au moins un autre botnet au fonctionnement similaire à Mirai, baptisé Bashlight.

Le problème est que ces appareils sont pratiquement impossibles à protéger en l'état. Pour une partie d'entre eux, les identifiants sont codés « en dur » dans le firmware et ne sont pas modifiables. Et même pour les autres, le fait qu'ils utilisent le protocole telnet (un ligne de commande, sans interface graphique) les rend difficile à configurer pour les utilisateurs. D'après une analyse de Flappoint, plus de 515 000 objets connectés seraient aujourd'hui vulnérables et susceptibles d'être incarcérés dans un botnet. Certains experts ont proposé des solutions radicales, notamment de développer un malware plus rapide que Mirai, capable d'infecter un objet connecté et de le saboter pour le mettre définitivement hors service. Une sécurité aussi draconienne que point de vue démontre l'utopique, mais qui souligne à quel point la situation démontre l'inefficacité.

Il y a eu beaucoup de succès au garde face au danger que représente l'Internet des Objets, mais, comme souvent, celles-ci n'ont servi à rien. Poser l'« il est clair que l'usage des objets connectés n'est pas prêt de s'arrêter », il est imprudent que les acteurs majeurs de cette industrie mettent en place des normes et des bonnes pratiques au plus tôt, faute de quoi l'Internet des Objets continuera à dévorer l'Internet tout court, et ce de plus en plus.

**Notre métier : Sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la Protection des Données Personnelles (Adresser à la Direction du travail de l'Infolys et de la Formation Professionnelle n°92 04 60641 84).**

**Plus d'informations sur : <http://www.level3expert.fr/> formations cybercriminalité-protection des données personnelles**

**Denis JACOPINI anime dans toute la France et à l'international 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 Liberté (CIL) dans votre établissement).**

**Denis JACOPINI**  
  
**Le Net Expert**  
**INFORMATIQUE**  
**Cyberdissuasion**  
Réagissez à cet article

Original de l'article mis en page : Le retour des botnets ou pourquoi les objets connectés sont un danger pour l'Internet

# Quelles sont les messageries qui protègent le mieux vos données personnelles ?



Quelles sont les messageries qui protègent le mieux vos données personnelles ?

**Apple, Google, Snapchat, BlackBerry, ou encore le Chinois Tencent, tous ces géants du web proposent à leurs utilisateurs des messageries instantanées. Aujourd'hui, ce sont plusieurs milliards de personnes qui les utilisent quotidiennement. Au sein de ceux-là, des minorités opprimées, des militants pour les droits de l'Homme, des dissidents politiques, des lanceurs d'alertes... Mais comment ces messageries protègent-elles nos données ?**

Amnesty International a rendu un rapport accablant sur la question, dans lequel elle effectue un classement des messageries privées.

### Classement des messageries privées

Quelle messagerie privée est la plus sécurisée selon le classement d'Amnesty International ?

Entreprises	Messageries	Siège	Nombre d'utilisateurs	Classement Amnesty (sur 100)
Apple	iMessage, Facetime	USA	Inconnu, mais 1 milliard d'iPhone vendus	67
Blackberry	Blackberry Messenger	Canada	100 millions	20
Facebook	Facebook Messenger, WhatsApp	USA	1 milliard chacune	73
Google	Allo, Duo, Hangouts	USA	Inconnu, mais plus de deux milliards d'utilisateurs Google	53
Kakao Inc	Kakao Talk	Corée du Sud	49 millions	40
Line	Line	Japon	218 millions	47
Microsoft	Skype	USA	300 millions	40
Snapchat	Snapchat	USA	200 millions	26
Telegram	Telegram Messenger	Allemagne	100 millions	67
Tencent	QQ, We Chat	Chine	697 millions, 853 millions	0
Viber media	Viber	Luxembourg	250 millions	47

Source: Amnesty Internationale [Récupérez les données](#)

Créé avec [Datawrapper](#)

### Classement Amnesty International

Les onze grandes entreprises évaluées affichent toutes des engagements écrits en termes de protection de la vie privée. Et pourtant, aucune n'est irréprochable, toutes ne respectent pas les normes internationales en vigueur et peu proposent un niveau élémentaire de protection. Facebook, Apple ou Google sont en haut du classement, quand Microsoft, Snapchat, ou Tencent font figure de mauvais élèves. L'ONG a mis au point un barème.

### Les critères du classement

Amnesty International attribue une note de 0 à 100 aux entreprises, selon leur résultat sur cinq critères provenant des normes internationales en la matière. Trois sont primordiaux pour assurer la sécurité des données personnelles.

Les entreprises sont jugées sur leur capacité à reconnaître les menaces contre la vie privée et la liberté d'expression. En clair, que mettent-elles en place pour protéger les droits de leurs utilisateurs ?

Elles doivent ensuite appliquer par défaut le chiffrement de bout en bout. Une question au cœur des préoccupations d'Amnesty International. L'ONG estime que seul le chiffrement de bout en bout est apte à protéger la vie privée. Ici, seul l'émetteur et le receveur détiennent la clef de chiffrement. Les acteurs intermédiaires du processus (fournisseur d'accès, entreprise de messagerie) n'ont donc pas accès au contenu de la conversation.

Les messageries doivent enfin rendre publiques les informations sur les demandes de données d'utilisateurs par des gouvernements et refuser de contourner les clefs de chiffrements.

### Facebook, Apple, Telegram et Google en tête

La messagerie de Facebook est la mieux classée, avec un score de 73 points. Le bébé de Mark Zuckerberg totalise environ un milliard de fidèles quotidiens. C'est lui qui offre le plus de garanties à ses utilisateurs. Mais ses deux messageries ne sont pas équivalentes. Si WhatsApp propose un chiffrement de bout en bout par défaut (l'utilisateur n'a pas à choisir, c'est automatique), cette option récente de Facebook Messenger doit être activée.

Apple cumule 67 points. La marque à la pomme offre un chiffrement de bout en bout sur ses deux messageries (iMessenger et Facetime). Mais Amnesty International relève qu'elle « devrait adopter un protocole de chiffrement plus ouvert qui permette une vérification indépendante complète ».

Telegram est deuxième ex aequo, avec 67 points aussi. Ce nom vous dit quelque chose ? C'est normal, cette messagerie a beaucoup defrayé la chronique car elle est l'application de messagerie instantanée la plus prisée des milieux djihadistes. Elle perd des points car son système de chiffrement n'est pas automatique et doit être activé.

Vient ensuite Google avec un score de 53. Le moteur de recherche est critiqué par Amnesty International car ses trois messageries instantanées ne proposent pas toutes des systèmes de chiffrement.

Les quatre entreprises qui caracolent en tête se sont toutes publiquement prononcées contre les moyens de contournement des clés de chiffrement par les États. Et toutes, à l'exception de Telegram, préviennent leurs utilisateurs des demandes faites par les gouvernements.

### Skype, Snapchat et Tencent, les mauvais élèves

Snapchat, c'est cette messagerie qui permet de s'envoyer une photo ou un texte sur un temps très court. Skype, propriété de Microsoft, c'est celle qui vous permet de faire des appels vidéo. Les deux applications sont mauvaises élèves aux quatrième et troisième plus mauvaises places.

Aucun chiffrement de bout à bout n'est proposé par les deux géants, qui présentent tous deux un système « très vulnérable », selon Amnesty. Les deux sont utilisées par des millions de jeunes quotidiennement, un public très menacé et très exposé à la cybercriminalité.

BlackBerry occupe l'avant-dernière place. La messagerie privée canadienne n'offre pas un système de chiffrement de bout en bout, elle le vend. Ainsi, si on ne paie pas, on n'est pas protégé sur BlackBerry. Qui plus est, d'après le site américain Vice, BlackBerry aurait donné sa clef de chiffrement à la police canadienne qui a alors pu intercepter des messages.

À la dernière place, on retrouve Tencent, le mastodonte chinois. L'entreprise accuse un score de 0 point. Aucun des critères n'est rempli et les données personnelles de plus d'un milliard et demi de personnes ne sont absolument pas protégées, conséquence de la censure que subit l'Internet chinois. En 2013, un développeur de Tencent confiait au journal *Le Monde*, « Les autorités ont le privilège d'accéder aux historiques, donc elles savent tout sur vous dès lors que vous utilisez nos services. » Le ton est donné...[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.

Original de l'article mis en page : Quelles sont les messageries qui protègent le mieux vos données personnelles ?

– La Voix du Nord