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]

Réagissez à cet article

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

---

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

---

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

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]

Réagissez à cet article

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

---

L’Internet des objets, ce piège de cristal

L’Internet des objets, ce piège de cristal

Encore une fois, l'actualité technologique nous démontre que l'Internet des objets est un problème de sécurité de masse en devenir.

Vous le savez sans doute si vous suivez mes articles, je suis un tantinet sceptique quant à la montée de l'Internet des objets, soit le mariage entre l'Internet et les objets du quotidien. Non pas que je doute des possibilités offertes par les systèmes qui émergeront de cette tendance, bien au contraire. Ce sont plutôt les problèmes de sécurité qu'ils engendreront qui me laissent quelque peu pantois.

Imaginez les grands titres : «Incapables de regarder le Canadien de Montréal à cause d'un maliciel». Je vous jure, là, les gens vont débarquer dans les rues.

Lorsqu'on prend du recul et qu'on regarde ce qui se passe, nous sommes littéralement en train de nous créer notre propre piège de cristal : c'est bien beau et reluisant à l'extérieur, mais un gros problème se cache à l'intérieur. Nous sommes en train de devenir dépendants de systèmes extrêmement poreux. Or, je ne serais pas surpris de voir que bon nombre d'objets connectés que l'on considère comme des «acquis» finissent par tomber en otage aux mains d'un Hans Gruber en puissance qui décide tout simplement de nous faire cracher le cash pour retrouver le contrôle desdits objets.
Ça semble peut-être bien théorique en ce moment, mais la journée où des voitures, des frigos, des systèmes de chauffages, ou des téléviseurs cesseront de fonctionner pour la simple et bonne raison qu'ils seront tombés entre les griffes d'un quelconque cryptorançongiciel remâché, ça risque de déranger pas mal de monde, et pire, en inquiéter encore plus. Imaginez les grands titres dans les tabloïds : «Incapables de regarder le Canadien de Montréal à cause d'un maliciel». Je vous jure, là, les gens vont débarquer dans les rues.

Die Harder

Le pire dans tout ça, c'est qu'on est véritablement devant une chronique de mort annoncée. Déjà, on a constaté que certains objets connectés pouvaient être massivement piratés par toutes sortes de moyens. Il y a quelques mois de cela, on découvrait par exemple que des ampoules et des serrures connectées ***pouvaient être ciblées et exploitées par des pirates informatiques malintentionnés****. On imagine déjà le potentiel de ce genre de vulnérabilités pour la sécurité résidentielle. Pourtant, on en est qu'aux débuts en ce qui concerne les problèmes dans les systèmes de sécurité.*

(Photo : ***Frédéric Bisson****)*

Tout récemment, on a d'ailleurs vécu le comble de l'ironie dans les systèmes de sécurité alors que pas moins de 25 000 caméras de surveillance ont fait partie ***d'un réseau de botnets lançant des attaques par déni de services****. Grosso modo, des pirates informatiques ont été en mesure de pirater des caméras de surveillance mal sécurisées, de les fédérer dans un réseau sous un serveur de commandement et de contrôle et de les réutiliser pour commettre des attaques informatiques ultérieures. C'est-y pas beau ça!?*

Pourtant, on avait déjà eu des signes avant-coureurs de ce genre d'attaques. Des réseaux de botnetsconstruits avec des caméras de surveillance avaient déjà ***été découverts dans des analyses précédentes****. Des analyses qui démontraient par ailleurs que ces objets connectés étaient passablement poreux.*
Et on est loin d'être sortis du bois, je vous en passe un papier. Non seulement il existe ***des moteurs de recherche permettant de trouver les objets connectés*** *présents sur Internet, mais en plus, on a des petits génies informatiques qui se mettent à les* ***géolocaliser en utilisant des drones****. Donc, si vous aviez espoir que ça ralentirait quelque peu, détrompez-vous.*

Pourtant, je ne suis pas le seul qui a des problèmes de sommeil par rapport à cette situation. En 2014, Europol prédisait ***qu'un meurtre mené par Internet allait probablement se produire dans les prochains mois****. Bon, moi je n'irais pas jusqu'à faire une prédiction temporelle, mais c'est clair que, tôt ou tard, un truc du genre va finir par arriver. Je ne suis pas certain que ce sera un événement intentionnel, mais considérant la vitesse à laquelle on intègre des objets connectés dans le réseau de la santé, ce n'est qu'une question de temps avant que quelqu'un meurt suite à un incident informatique.*

Marche ou crève

Bon, j'ai beau couiner et geindre, c'est bien dommage, mais on ne changera pas pour autant les avancées technologiques. Le néo-luddisme ne sert strictement à rien dans ce cas; il faudra à terme que l'industrie atteigne un niveau de maturité suffisant pour construire les objets connectés avec une architecture centrée sur la sécurité. En attendant, on est dû pour quelques coups fumants de piratage et de prises d'otages numériques.
En fait, la vraie question que l'on doit se poser est celle du «retour sur investissement». Dans le cas du secteur de la santé par exemple. Oui, c'est clair que des gens finiront par mourir dus à des problèmes liés à l'informatique. Cependant, il faut aussi considérer l'autre côté de la médaille, c'est-à-dire combien de personnes ont été sauvées par ces mêmes systèmes informatiques.
Il en va de même avec les gestes que posent John McClane dans la série Die Hard. Oui, il finit par causer beaucoup de dommages et par tuer beaucoup de monde au cours de ses aventures, mais il sauve également la vie de centaines de victimes innocentes.

Yippee Ki-Yay Mother$&@%!*
Article original de Benoît Gagnon

Réagissez à cet article

Original de l'article mis en page : L'Internet des objets, ce piège de cristal | Branchez-vous

---

Vous avez eu un drone en

cadeau à Noël, voici vos nouveaux droits, devoirs et obligations

	**Vous avez eu un drone en cadeau à Noël, voici vos nouveaux droits, devoirs et obligations**

Le 23 décembre, la DGAC (Direction Générale de l'Aviation Civile) a mis en ligne les évolutions réglementaires en matière de drones, aéromodèles, etc. Elles se veulent plus lisibles et mieux adaptées aux besoins.

Si le Père Noël vous apporte un drone, voici quelque chose qui devrait vous intéresser : ce que vous avez le droit de faire ou non avec, les règles à respecter, etc.

Tout d'abord, sachez que deux textes datant du 17 décembre 2015 définissent désormais la réglementation pour l'usage de drones. Il s'agit d'un arrêté relatif à la conception, aux conditions d'utilisation et aux qualifications des télépilotes et d'un autre arrêté relatif aux conditions d'insertion dans l'espace aérien.
Comme le rappelle la DGAC, les deux textes font la distinction entre les différents pilotes : professionnels ou non. Par exemple, « lorsque cette utilisation est limitée au loisir et à la compétition, on parle d'aéromodèles ». Ce sont les drones achetés dans les grandes surfaces ou des boutiques high-tech. D'autre part, on évoque les drones réservés à une utilisation professionnelle.

Règles basiques

Si l'espace aérien est libre en-dessous de 150 mètres, il faut toutefois respecter certaines consignes basiques :
• Voler en dehors des agglomérations et des rassemblements de personnes ou d'animaux ;
• Voler en dehors des zones proches des aérodromes ;
• Et voler en dehors d'espaces aériens spécifiquement réglementés qui figurent sur les cartes aéronautiques.
• Il est également interdit de survoler des villes ou des rassemblements de personnes sans autorisation préfectorale.
• Dans tous les cas, le « télépilote d'un drone est responsable des dommages causés par l'évolution de l'aéronef ou les objets qui s'en détachent aux personnes et aux biens de la surface (article L.61613-2 du code des transports) ».

Protection de la vie privée

Le texte compte tout un tas d'autres interdits. Notamment, les personnes sourdes ne peuvent pas piloter d'aéromodèles puisqu'un pilote doit toujours être en mesure de détecter visuellement et auditivement les autres drones. Il est aussi interdit de voler la nuit, ou de piloter un drone depuis une voiture.

La DGAC rappelle aussi que la « prise de vue aérienne est réglementée par l'article D133-10 du code de l'aviation civile », afin de veiller à la protection de la vie privée. Une amende de 45 000 euros et d'un an d'emprisonnement est prévue s'il y une volonté manifeste de porter atteinte à l'intimité de la vie privée d'autrui.

Réagissez à cet article

Source : *Un drone à Noël ? Voici vos nouveaux droits et devoirs*

Le français Seolane détecte et neutralise les drones malveillants

Le français Seolane détecte et neutralise les drones malveillants

L'entreprise a développé une station fixe au sol qui détecte la signature électromagnétique de ces engins volants. Sa solution intègre aussi un drone volant fourni par le groupe Eca qui se chargera d'identifier et de filmer le pilote avec une caméra embarquée.

Ce drone intervient dès lors que la station fixe a détecté un drone malveillant. © Seolane

Le survol illégal de drones au-dessus de bases militaires, centrales nucléaires et autres sites sensibles a mis à jour la nécessité d'identifier et de neutraliser les intrus. « *Ce marché devrait peser d'ici cinq ans entre 500 millions et un milliard d'euros* », estime Wilfrid Rouger, le fondateur et directeur général de Seolane une PME française créée en 2007 à Maisons-Laffitte (Yvelines).
Constituée d'une dizaine de personnes, l'entreprise est spécialisée dans l'intégration de systèmes de détection de signaux et de géolocalisation pour le transport et la sécurité. Le mois dernier, elle a remporté la première édition du concours Startup Challenge organisé le mois dernier par le salon Milipol, dédié à la sûreté des Etats.
Le prix récompense sa solution Dronelnt qui détecte, caractérise, traque et neutralise les drones malveillants avec une station fixe au sol. En cas de survol illégal d'un site, cette dernière va détecter la signature électromagnétique du drone et le localiser par radiogoniométrie. Une technique qui recourt à plusieurs capteurs pour localiser la position du drone par triangulation.
Drone fourni par Eca.
« *Nous avons lancé ce développement technologique il y a deux ans* », indique Wilfrid Rouger. Ce dernier a noué un partenariat avec le groupe Eca qui fournit un drone d'intervention. Fonctionnant de concert avec la station au sol, ce dernier dispose d'une autonomie allant jusqu'à 1h30 selon le modèle. Pour identifier le pilote et le filmer, l'engin volant embarque une caméra qui fonctionne de jour comme de nuit.
« *Plusieurs tests ont été réalisés avec succès avec la Gendarmerie nationale sur différents sites dont une centrale nucléaire* », fait valoir le directeur général de Seolane qui reçoit des demandes provenant de sites Seveso, aéroports et autres bases militaires qui s'inquiètent de l'explosion annoncée des vols illégaux de drones et des menaces terroristes.

Réagissez à cet article
Source : http://www.expoprotection.com/site/FR/L_actu_des_risques_malveillance__incendie/Zoom_article,I1602,Zoom-c1901a7c9c9d76e3b257db6e81734942.htm
Par Eliane Kan

DroneDefender, un fusil anti-drone qui brouille les ondes | Le Net Expert Informatique

DroneDefender, un fusil anti-drone qui brouille les ondes

Aux États-Unis, un fusil d'un nouveau genre a été mis au point. Celui-ci envoie des ondes pour brouiller les fréquences entre l'opérateur et son drone, pour obliger ce dernier à se poser.

Souvenez-vous : à l'automne 2014 et pendant l'hiver 2015, l'actualité a été marquée par de nombreux incidents impliquant des drones. Ces petits aéronefs ont en effet été aperçus en train de survoler tout un tas de sites sensibles, allant des centrales nucléaires au palais de l'Élysée, en passant par l'ambassade des États-Unis à Paris, l'Assemblée nationale et certains lieux très fréquentés par les touristes.
Mais la riposte s'organise. Face à ces survols illicites, des entreprises réfléchissent au meilleur moyen de neutraliser les drones. C'est le cas par exemple de Boeing, qui a mis au point une version compacte de son système d'interception par laser. C'est aussi le cas de son rival Airbus, qui propose pour sa part un brouilleur ciblé des fréquences.

UN FUSIL BROUILLEUR D'ONDES

C'est cette dernière approche qui a été retenue par Dan Stamm. L'homme a en effet mis au point une sorte de fusil, le «Battelle DroneDefender», qui peut contraindre un aéronef à se poser d'urgence. En effet, au lieu de tirer des cartouches pour l'abattre, celui-ci perturbe les fréquences de contrôle entre l'opérateur et son appareil. C'est ce que l'inventeur explique à Motherboard, qui consacre un reportage sur ce projet.

Le Battelle DroneDefender « fait en quelque sorte croire au drone qu'il est hors de portée. Celui-ci active alors ses protocoles de sécurité qui incluent une de ces trois options : il va se maintenir en vol stationnaire jusqu'à ce que le pilote retrouve la liaison avec son drone, il va se poser de façon à pouvoir être récupéré par son propriétaire ou alors il va retourner à son point d'origine ».

SÉCURISER DES ÉVÈNEMENTS PONCTUELS

Dans la vidéo de démonstration, nous pouvons voir que l'utilisateur du Battelle DroneDefender doit maintenir en permanence le canon de son arme pointé vers le drone jusqu'à ce qu'il touche le sol. Ici, c'est un modèle Phantom conçu par le fabricant DJI qui a été utilisé. La portée effective du Battelle DroneDefender est de 400 mètres, selon la fiche technique publiée sur le site de Battelle.
Pour Dan Stamm, son arme peut servir à sécuriser des évènements ponctuels tout en évitant de déployer des dispositifs particulièrement encombrants. C'est un dispositif qui peut être utilisé par exemple par un policier pour neutraliser un drone, tandis que son collègue se rend au niveau de la zone d'atterrissage pour l'empêcher de redécoller. Il peut être embarqué dans une voiture de patrouille, mais aussi dans un hélicoptère.
En Europe, des travaux sont aussi menés pour améliorer la détection et la neutralisation des drones. La piste des brouilleurs de signaux GPS est l'une des plus prometteuses, mais il en existe d'autres, comme l'utilisation de canons à eau, de lance-filets ou de puces d'immatriculation pour retrouver le propriétaire du drone.

Denis JACOPINI est Expert Informatique, conseiller et formateur en entreprises et collectivités et chargé de cours à l'Université.
Nos domaines de compétence :
• **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
• **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
• **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.
Contactez-nous

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source :
http://www.numerama.com/sciences/126526-dronedefender-un-fusil-anti-drone-qui-brouille-les-ondes.html

A la découverte de Skynet, le programme américain d’assassinats par drones | Le Net Expert Informatique

Un poste de travail à la NSA. (PAULJ.RICHARDS/AFP)

A la découverte de Skynet, le programme américain d’assassinats par drones

Skynet est un programme utilisé pour identifier des membres d'Al-Qaida puis les tuer avec des drones. « Le Monde » révèle en détails comment fonctionne le principe.

Les agents de la NSA ne manquent pas d'humour… noir. Ils ont appelé Skynet, du nom du système informatique incontrôlable de « Terminator », leur programme chargé d'analyser les métadonnées d'appels téléphoniques pour tenter de détecter des activités suspectes. Selon « Le Monde », qui a exploité les documents révélés en avril par Edward Snowden, Skynet a été déployé au Pakistan pour identifier des membres d'Al-Qaida, puis les tuer à coups de drones télécommandés. Le quotidien révèle en détails comment fonctionne ce programme.

Collecter des données sur le mode de vie des cibles

Cela commence par une collecte massive de métadonnées, principalement celles des compagnies de téléphone mobile (lieu, temps de conversation…). Au total, ce sont 80 catégories de données qui sont extraites puis analysées. « L'hypothèse fondamentale est que le mode de vie des cibles à identifier diffère fortement de celui des citoyens ordinaires », écrit « Le Monde ».

Séparer « terroristes » et « innocents » grâce à des algorithmes

Skynet s'appuie également sur la « vérité de terrain », un lot de données dans lequel les utilisateurs de téléphones mobiles ont été classés en deux catégories : « terroristes » et « innocents ». Mais comment savoir qui est terroriste et qui est innocent ? Les documents de l'agence suggèrent que Skynet utilise les données personnelles de membres connus d'Al-Qaida afin d'établir un profil type de terroriste, à lequel est comparé l'ensemble des autres profils.

Une série d'algorithmes produit ensuite un score pour chaque individu, avec un seuil prédéterminé : si le score d'un individu est supérieur au seuil, c'est un terroriste, et si son score est inférieur, il est innocent.

« En fonction des données de la 'vérité de terrain', la NSA s'offre une marge de sécurité en choisissant un seuil garantissant que seul un certain pourcentage de 'terroristes' seront formellement classés comme tels », indique « Le Monde ». Selon les documents divulgués par Edward Snowden, l'agence a choisi 50 % : la moitié des « terroristes » sont des innocents ou des « faux négatifs » ; la moitié des « innocents » sont des terroristes, soit des « faux positifs ».

Des résultats « invalides »

En comparant les données de 100.000 individus à sept téléphones de terroristes connus, la NSA détermine un pourcentage de « faux positifs ». Là où on avait 50% de faux négatifs, l'algorithme détermine finalement 0,18% de faux positifs ou même 0,008 % pour sa version améliorée.

« En réalité, ces résultats sont scientifiquement invalides », note « Le Monde ». « Cette méthode ne permet pas la généralisation souhaitée, car les 100.000 individus sont choisis au hasard, alors que les sept terroristes proviennent d'un lot déjà connu. […] Il aurait fallu mélanger les 'terroristes' à la population générale avant de choisir un échantillon au hasard, mais cela ne serait pas pratique, à cause de leur nombre minuscule – sept au total. »

Cette erreur qui peut paraître insignifiante est en fait très importante : « 0,008 % de la population du Pakistan représente près de 15.000 'innocents' accusés à tort – tandis que, dans le même temps, 50 % des 'terroristes' ne seront pas visés, car leur score est inférieur au seuil fixé arbitrairement ».

On ignore toutefois si tous les individus classés comme « terroristes » par Skynet sont ensuite systématiquement visés par des drones.

Source :
http://tempsreel.nouvelobs.com/les-internets/20151020.OBS7967/comment-marche-skynet-le-programme-americain-d-assassinats-par-drones.html
Par A. S.

Une plaque d'immatriculation

LED pour identifier les drones | NewZilla.NET | Le Net Expert Informatique

30	**Une plaque d'immatriculation LED pour identifier les drones**

Des chercheurs de l'université de Berkeley (Californie) ont mis au point une solution pour faciliter l'identification de ces objets volants dont l'activité est plus en plus vécue comme une nuisance.

Ils sont un facteur de stress pour les ours sauvages. Ils empêchent les pompiers, les forces de polices d'intervenir correctement pour circonscrire un feu ou rechercher un suspect par hélicoptère. Et ne parlons pas des avions de ligne…
Ils? Ce sont ces drones dont l'activité est, en raison d'un manque de régulation, de plus en plus perçue comme une nuisance, tant par le grand public que par les autorités. Et l'on pourrait mentionner, pour ajouter au chaos qui vient, les projets de livraison par drones sur lesquels planchent aujourd'hui des entreprises comme Google ou Amazon.
Bref, s'ils veulent continuer à faire partie de notre quotidien, l'activité des drones devra à terme faire l'objet de contrôles renforcés. Aux Etats-Unis, certains fabricants de ces objets, de plus en plus accessibles car de moins en moins cher, ont déjà mis en place des "no fly" zones, où les drones ont par exemple interdiction de voler au-dessus de… la Maison Blanche ou du Congrès à Washington.

Identifiable à l'oeil nu
D'autres acteurs du marché verraient bien des drones contrôlés via des balises beacon. Mais la solution la plus innovante et la plus porteuse nous vient de l'université de Berkeley (Californie) où des chercheurs ont développé ce qui s'apparente à une plaque d'immatriculation.
Lightcense (en référence aux "license plates", les plaques d'immatriculation aux Etats-Unis) est une plaque d'immatriculation qui fonctionne par LED. Des LED dont la vitesse de clignotement permettrait d'identifier l'appareil concerné. Une identification à l'oeil nu dans un rayon de 100 mètres le jour, ou bien via une application de smartphone.

Source : http://www.newzilla.net/2015/08/19/une-plaque-dimmatriculation-led-pour-identifier-les-drones/

Les drones de Parrot peuvent facilement se faire hacker |

Le Net Expert Informatique

Les drones de Parrot peuvent facilement se faire hacker

Il y a quelques semaines, nous vous faisons part des piratages de voitures et encore plus tôt dans l'année, d'avions… Aujourd'hui, c'est au tour des drones Parrot de succomber aux hackers !

Ou plutôt à un hacker. Ryan Satterfield, connu pour sa chaîne Planet Zuda, qui a profité de la Def Con pour faire une démonstration. À l'aide de son smartphone et d'une simple clef, il a réussi à faire atterrir un AR.Drone 2.0.
Les drones de la société française n'ont malheureusement que trop peu de protections. Ces derniers tournent sous Linux avec des ports WiFi et Telnet ouverts, sans nécessiter un quelconque mot de passe pour s'y relier…. Il suffit de s'y connecter en utilisant le port 23 et de rentrer la commande « kill 1″. De suite, le drone redescend sur terre. Parrot a précisé qu'elle était consciente de ces failles de sécurité, mais n'a pourtant pas annoncé de correctif. Notez que le dernier drone, le Parrot Bebop, serait lui aussi touché, a annoncé le chercheur Michael Robinson.

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : http://www.journaldugeek.com/2015/08/17/les-drones-de-parrot-peuvent-facilement-se-faire-hacker
Par 4ugeek