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

---

Les développeurs Linux victimes d'une attaque DDoS

Les développeurs réunis cette semaine lors de la conférence Linux Plumbers de Santa Fe (Nouveau Mexique) ont été victimes d'une attaque par déni de service distribué (DDoS), rapporte ZDNet.com.…[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 sur cette page.

Réagissez à cet article

IoT : Le malware Mirai fait des émules

IoT : Le malware Mirai fait des émules

Sécurité : Utilisé pour infecter des objets connectés, souvent peu sécurisés, Mirai utilise une méthode qui a prouvé son efficacité et que d'autres cybercriminels reprennent aujourd'hui à leur compte.…[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 sur cette page.

Réagissez à cet article

Piratage informatique : 3 hôpitaux anglais obligés de transférer les patients

Piratage informatique : 3 hôpitaux anglais obligés de transférer les patients

Un incident qualifié de « majeur ». En Grande-Bretagne, des interventions chirurgicales programmées et des admissions de patients ont dû être annulées dans trois hôpitaux après une infection par un virus informatique du réseau informatique de ces établissements.…[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 sur cette page.

Réagissez à cet article

Piratage informatique : 3 hôpitaux anglais obligés de transférer les patients

Un incident qualifié de « majeur ». En Grande-Bretagne, des interventions chirurgicales programmées et des admissions de patients ont dû être annulées dans trois hôpitaux après une infection par un virus informatique du réseau informatique de ces établissements.…[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 sur cette page.

Réagissez à cet article

Piratage informatique : 3 hôpitaux anglais obligés de transférer les patients

Un incident qualifié de « majeur ». En Grande-Bretagne, des interventions chirurgicales programmées et des admissions de patients ont dû être annulées dans trois hôpitaux après une infection par un virus informatique du réseau informatique de ces établissements.…[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 sur cette page.

Réagissez à cet article

Piratage informatique : 3 hôpitaux anglais obligés de transférer les patients

Un incident qualifié de « majeur ». En Grande-Bretagne, des interventions chirurgicales programmées et des admissions de

patients ont dû être annulées dans trois hôpitaux après une infection par un virus informatique du réseau informatique de ces établissements.…[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 sur cette page.

Réagissez à cet article

Piratage informatique : 3 hôpitaux anglais obligés de transférer les patients

Piratage informatique : 3 hôpitaux anglais obligés de transférer les patients

Un incident qualifié de « majeur ». En Grande-Bretagne, des interventions chirurgicales programmées et des admissions de patients ont dû être annulées dans trois hôpitaux après une infection par un virus informatique du réseau informatique de ces établissements.…[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 sur cette page.

Réagissez à cet article

---

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 NextInpact, 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

---

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 !

Réagissez à cet article

Original de l’article mis en page : AtomBombing, le code insensible aux systèmes de protection de Windows