

Quelles failles pour les voitures connectées ?



Quelles
failles
pour les
voitures
connectées

L'édition du salon de l'auto interpelle le grand public sur les nouveaux pirates de la route. Voitures connectées : les cybercriminels dans l'angle mort ?

Nul doute, la voiture connectée est encore l'une des stars du salon de l'auto cette année. Comme tout ce qui attire à internet et aux objets connectés, il est légitime de se poser quelques questions notamment sur la sécurité liée au partage des données ainsi qu'à cette forme de déplacement autonome. Un véhicule connecté est en effet doté d'un accès à Internet ainsi que, plus généralement, d'un réseau local sans fil. L'accès Web offre divers services supplémentaires tels que la notification automatique des embouteillages, la réservation de parking, la surveillance du style de conduite (pouvant par ailleurs avoir une incidence sur le montant des primes d'assurance automobiles) etc.

De multiples raisons peuvent motiver les cybercriminels à tenter de pirater des voitures connectées :
L'appât du gain : Il s'agit de bloquer l'accès au véhicule jusqu'à ce la victime paie une rançon.
L'espionnage : l'activation du micro ou de la caméra équipant le véhicule peut donner accès à des informations exclusives et des données sensibles.

La violence physique : les attaques peuvent avoir pour but de blesser le conducteur, ses passagers, ou encore d'endommager d'autres véhicules sur la route.

C'est en analysant ses raisons que la société russe développe une approche de la sécurité interne des véhicules connectés. Elle repose sur deux principes : D'abord l'isolement veille à ce que deux entités indépendantes (applications, pilotes, machines virtuelles) ne puissent interférer l'une avec l'autre en aucune façon. Ensuite, le contrôle des communications signifie que deux entités indépendantes ayant à communiquer dans le système doivent le faire conformément à des règles de sécurité. L'utilisation de techniques de cryptographie et d'authentification pour l'envoi et la réception des données fait également partie intégrante de la protection du système.

Pour respecter notre travail, merci de ne reprendre que l'intro. Pour lire la suite de cet article original [direction](#) ->

<http://www.datasecuritybreach.fr/voitures-connectees-cybercriminels-langle-mort/#ixzz4MV1xJas6>

Under Creative Commons License: Attribution Non-Commercial No Derivatives

Follow us: @datasecub on Twitter

...[[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 la 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 : Voitures connectées : les cybercriminels dans l'angle mort ? – Data Security Breach