Sécurité : des hackers testent le contrôle à distance d'une Jeep

A l'ère de la voiture connectée, voici une troublante expérience : la prise de contrôle à distance d'un véhicule. Un journaliste de **Wired** a accepté de conduire une **Jeep Cherokee** (SUV) de **Chrysler** pour mener cette expérience déroutante avec la complicité de deux hackers : Charlie Miller (Twitter) et Chris Valasek (Idactive).

Voyez les résultats sur la vidéo YouTube: la climatisation du véhicule s'active à l'insu du conducteur, une image des hackers apparaît sur l'écran de navigation, puis la radio s'allume avec le volume sonore qui s'intensifie et les essuie-glaces qui se mettent à fonctionner sans rien demander. Pour achever la démo, les deux hackers coupent le moteur à distance alors que le journaliste cobaye se trouve sur une autoroute du Missouri. Bon, quelques précautions ont été prises pour éviter un accident mais c'est convaincant.

Pour Chrysler, il fallait réagir. Le constructeur propose à ses clients une mise à jour du logiciel de navigation Uconnect sur ses gammes de véhicules à installer par clé USB : « une réactualisation logicielle pour améliorer la sécurité électronique du véhicule », précise-t-il laconiquement.

Des véhicules connectés donc vulnérables

Avec le développement des véhicules connectés voire autonome, cette expérience de Wired démontre que des failles peuvent s'immiscer dans les dispositifs multimédia embarqués. Selon FranceTVInfo, les travaux de Charlie Miller et Chris Valasek auraient même incité deux sénateurs américains à déposer une proposition de loi pour renforcer la sécurité IT des voitures.

C'est un nouveau champ d'investigation pour la sécurité IT : les failles de sécurité dans les voitures connectées. Fin mars, dans le cadre de la session Black Hat Asie à Singapour, le développeur Eric Evenchick (ex-collaborateur de Tesla) a présenté un kit logiciel open source associé à une carte d'interface pour détecter ces vulnérabilités dans les véhicules. Au-delà des systèmes de navigation, les dispositifs embarqués de divertissement numérique (infotainment) sont également à surveiller. Selon la BBC, NCC Group serait en mesure de démontrer qu'il est possible de hacker un véhicule en envoyant des données par l'intermédiaire d'une liaison de radio numérique (DAB). Le cabinet de consulting dans la sécurité IT basé à Manchester devrait faire une démo à la session Black Hat USA qui sera organisée à partir de début août à Las Vegas, souligne ITespresso.

A lire aussi :

Le FBI présente la voiture autonome comme l'arme fatale

Sécurité des voitures connectées : l'inquiétude des experts grandi

La sécurité des voitures connectées étudiée sur toutes les coutures