Piratage d'une Corvette à distance : le Français Mobile Devices s'explique

Dans une interview accordée à nos confrères de *ITespresso* (appartenant au même groupe de presse que *Silicon.fr*), Mobile Devices, une société française qui produit de petits boîtiers pour le suivi de flottes de véhicules, revient sur le piratage d'une Corvette – marque appartenant au groupe Chevrolet. Rappelons que cette prise de contrôle à distance par des chercheurs de l'Université de Californie en sécurité exploite une faille d'un des *dongles* produits par Mobile Devices. L'équipe du professeur Stefan Savage explique, pour ses tests, avoir acheté ces boîtiers auprès de Metromile, un distributeur des produits Mobile Devices aux Etats-Unis qui fournit notamment Uber aux Etats-Unis. Via l'envoi d'un simple SMS spécialement conçu pour cet appareil, les chercheurs sont parvenus à prendre le contrôle de fonctions essentielles du véhicule, comme le freinage (voir la vidéo).

Ainsi propulsée sur le devant de la scène, la firme française, qui commercialise une plate-forme logicielle pour les projets de voitures connectées, tente aujourd'hui d'éteindre l'incendie. Fondateur et Pdg de Mobile Devices, Aaron Solomon explique à nos confrères que ce piratage résulte d'une négligence dans l'implémentation du boîtier. « *Les dongles sont livrés aux constructeurs et aux intégrateurs en mode programmation*, dit le dirigeant. *Cela leur permet d'implémenter leurs propres services. Mais pour pouvoir programmer, il faut que la sécurité soit désactivée* ». Autrement dit, selon le dirigeant, si le *dongle* avait été basculé en mode 'production' (censé verrouiller les accès) comme cela aurait dû être le cas, l'accès externe par SMS aurait été impossible.

« Le buzz va changer les choses »

Et le Pdg d'esquisser une solution pour éviter d'autres mésaventures de ce type. Les *dongles* de Mobile Devices sont en effet connectés aux serveurs l'entreprise, cette dernière peut donc contrôler si la sécurité est effectivement active. Pour des questions de confidentialité des clients, cette pratique n'avait pas cours jusqu'à présent. Mais « *avec le buzz autour de la Chevrolet, les choses vont changer* », veut croire Aaron Solomon. L'entreprise a par ailleurs produit un patch comblant la vulnérabilité spécifique mise en évidence par les chercheurs. Le Pdg assure que tous ses clients seront couverts par ce correctif d'ici à la fin août.

Le piratage mis en œuvre par les chercheurs de l'Université de Californie cible un boîtier connecté à OBD2 (On Board Diagnostics), interface créée à l'origine pour le contrôle du respect des normes antipollution et pour laquelle de nombreux industriels proposent, aujourd'hui, des solutions avant tout destinées aux entreprises spécialisées dans la gestion de flotte ou aux assureurs (pour les solutions de Pay-as-you-drive). Un créneau où on retrouve la PME française installée à Villejuif (94). Dans l'Hexagone, Mobile Devices équipe ainsi environ 5 000 taxis, ainsi que des poids lourds et bennes à ordure. Elle est également à l'origine de la clef 3G exploitée par PSA pour ses Peugeot Connected Apps (sur interface USB cette fois). La société indique toutefois travailler principalement à l'export.

A lire aussi :

Jeep Cherokee piratée : Blackberry dédouane son OS embarqué QNX
Hacker les voitures connectées ? C’est en Open Source
PSA Peugeot Citroën ouvre ses voitures connectées aux éditeurs