Hack de la Jeep Cherokee, le retour, malgré les mises à jour…

Les deux experts qui avaient piraté une Jeep Cherokee récidivent dans le cadre de la Black Hat en démontrant une attaque sur le même véhicule.

En 2015, la Black Hat avait vu deux spécialistes en sécurité, Charlie Miller et Chris Valasek, prendre le contrôle à distance d'une Jeep Cherokee de 2014. Un exploit qui a obligé Chrysler, propriétaire de Jeep, à procéder à un rappel de près de 1,4 million de véhicules. Une opération de mise à jour coûteuse pour le constructeur automobile. Il en a profité aussi pour lancer un Bug Bounty, avec des primes allant de 150 à 1500 dollars.

Un programme auquel les deux experts ne pourront pas concourir. Car ils démontrent à la Black Hat 2016 que la sécurité des voitures connectées n'est toujours pas optimale, malgré les récentes mises à jour. Dans une présentation, ils présentent une attaque contre la même Jeep Cherokee de 2014. A la différence de l'année dernière, cette attaque n'est pas menée à distance, mais avec un accès physique à la voiture. Néanmoins, le duo précise qu'avec du temps elle pourrait être réalisée via un terminal embarqué ou à distance via une liaison sans fil.

Blocage des freins et coup de volant intempestif

Une fois dans la voiture, Charlie Miller a branché son ordinateur sur le réseau du véhicule, nommé bus CAN, via un port situé sous le tableau de bord. Ce réseau envoie des instructions aux différents capteurs (consommation, confort, détection de panne, etc). L'accès à ce réseau est normalement sécurisé avec le patch de sécurité élaboré l'année dernière à la suite du premier piratage de la Jeep. Il semble que des failles subsistent et les deux spécialistes ont pu contourner certains garde-fous.

Parmi les actions réalisées, ils ont bloqué les freins. Charlie Miller s'est servi du mode maintenance pour rendre inopérant le freinage. D'habitude ce blocage des freins ne peut s'opérer qu'à une faible vitesse soit 5 miles par heure. Dans une vidéo, le duo roule sur une route de campagne et d'un coup (après un compte à rebours) le volant se met à tourner à 90 degrés plantant la Jeep dans le fossé. Pour se faire, Charlie Miller s'est servi de la fonction tourner le volant dans la fonction parking automatique (qui se fait habituellement en marche arrière et à faible vitesse). Concrètement pour réaliser leur piratage, les deux experts se sont attaqués à la fois aux bus CAN, mais surtout en ciblant directement les ECU (electronic control units) dont un a été placé en mode maintenance et un autre utilisé pour envoyer des commandes malveillantes.

Interrogé par nos confrères de Wired, Chrysler ne considère pas cette attaque comme un danger pour la sécurité des véhicules. En premier lieu, elle nécessite un accès physique à la voiture. De plus, les experts ont utilisé une Jeep Cherokee ne disposant pas de la dernière version du logiciel embarqué d'infotainment (vecteur de leur première attaque en 2015). Les experts précisent que même avec la dernière version, cette attaque est toujours possible.

Article original de Jacques Cheminat

Réagissez à cet article

Original de l’article mis en page : Direction, frein : les hackers de Jeep récidivent à la Black Hat