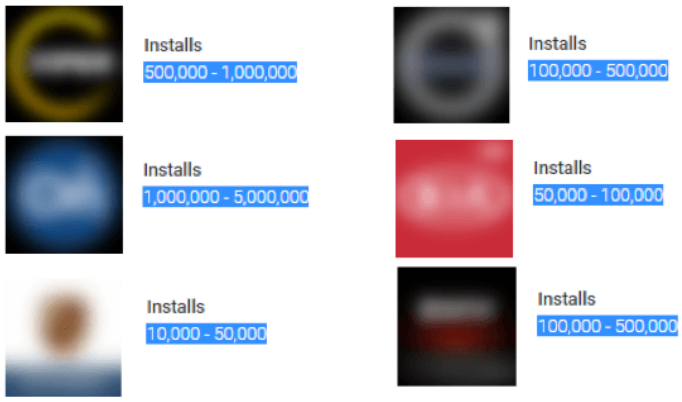
Véhicules connectés : 7 applications de commande à distance passées au crible

Qui prend le contrôle de notre voiture à notre insu ? Les chercheurs de Kaspersky Lab ont testé sept applications de commande à distance de véhicules développées par de grands constructeurs.

27 mars 2017

Les chercheurs de Kaspersky Lab ont examiné la sécurité des applications de commande à distance des modèles de plusieurs grands constructeurs automobiles. Les experts de la société ont ainsi découvert que toutes ces applications présentent un certain nombre de problèmes de sécurité, susceptibles de permettre à des criminels de causer des dommages significatifs aux propriétaires de voitures connectées.



Exemples d'applications populaires

Ces dernières années, les véhicules ont commencé à se connecter activement à Internet, qu'il s'agisse de leurs systèmes d'infodivertissement ou de leurs systèmes critiques, tels que le verrouillage des portières ou l'allumage, désormais accessibles en ligne. Au moyen d'applications mobiles, il devient possible d'obtenir les coordonnées géographiques du véhicule ainsi que son trajet, ou encore d'en ouvrir les portes, de faire démarrer le moteur et de prendre le contrôle d'autres équipements embarqués. Il est indéniable que ces fonctionnalités sont extrêmement utiles, mais comment les constructeurs protègent-ils ces applications contre le risque de cyberattaques ?

Afin de répondre à cette question, les chercheurs de Kaspersky Lab ont testé sept applications de commande à distance de véhicules développées par de grands constructeurs et téléchargées des dizaines de milliers de fois, voire jusqu'à cinq millions dans certains cas*. Ils ont ainsi découvert que **chacune des applications examinées présentait plusieurs problèmes de sécurité.**

Parmi les problèmes de sécurité décelés :

- **Aucune défense contre une rétroingénierie de l'application.** En conséquence, des utilisateurs malveillants peuvent en comprendre le fonctionnement et y détecter une vulnérabilité leur permettant d'accéder à l'infrastructure côté serveur ou au système multimédia du véhicule.
- **Aucun contrôle d'intégrité du code**, ce qui offre à des criminels la possibilité d'incorporer leur propre code informatique dans l'application afin de remplacer le programme d'origine par un faux.
- **Aucune technique de détection des accès Root**. Les droits Root octroient aux chevaux de Troie des capacités quasi illimitées et laissent l'application sans défense.
- **Absence de protection contre les techniques de superposition d'application**, ce qui permet à des applications malveillantes d'afficher des fenêtres de phishing pour dérober les identifiants des utilisateurs.
- **Stockage des identifiants et mots de passe en clair.** Grâce à cette faiblesse, un criminel peut s'approprier les données d'un utilisateur avec une relative facilité.

Une fois qu'il a réussi à exploiter une vulnérabilité, un pirate peut prendre le contrôle de la voiture, déverrouiller les portières, désactiver l'alarme et, en théorie, voler le véhicule.
Dans chaque cas, le vecteur d'attaque nécessite en plus certaines étapes préparatoires, consistant par exemple à inciter l'utilisateur par ruse à installer une application malveillante, spécialement conçue pour obtenir un accès Root au système et au programme du véhicule. Cependant, alors que les experts de Kaspersky Lab ont abouti dans leurs recherches à lad découverte de diverses applications malveillantes qui ciblent des identifiants de banque en ligne et d'autres informations sensibles, il est peu probable que cela pose un problème à des criminels aguerris dans les techniques d'ingénierie sociale, s'ils devaient décider de s'en prendre aux propriétaires de voitures connectées.

« *La principale conclusion de notre étude est que, dans leur état actuel, les applications commandant les véhicules connectés ne sont pas prêtes à résister aux attaques de malware. Lorsque l'on considère la sécurité d'une voiture connectée, il ne faut pas se cantonner à l'infrastructure côté serveur. Nous pensons que les constructeurs automobiles s'exposent aux mêmes risques que les banques avec leurs applications. Au départ, les applications des banques en ligne n'intégraient pas toutes les fonctions de sécurité que nous avons répertoriées. Après de multiples cas d'attaques contre des applications bancaires, de nombreux établissements ont amélioré la sécurité de leurs produits. Par bonheur, nous n'avons pour l'instant détecté aucun cas d'attaque contre des applications de véhicules, ce qui signifie que les constructeurs ont encore le temps de faire ce qu'il faut. Mais nous ignorons combien de temps exactement. Les chevaux de Troie modernes se caractérisent par une très grande flexibilité : un jour ils peuvent se comporter comme un banal adware et, le lendemain, facilement télécharger une nouvelle configuration permettant de cibler de nouvelles applications. La surface d'attaque est particulièrement vaste en l'occurrence* », **commente Victor Chebyshev, Expert en sécurité chez Kaspersky Lab.**

Les chercheurs de Kaspersky Lab conseillent aux utilisateurs d'applications pour voitures connectées de prendre les précautions suivantes afin de protéger leur véhicule ainsi que leurs données privées contre d'éventuelles cyberattaques :

- Ne « rootez » pas votre appareil Android sous peine d'offrir des capacités quasi illimitées aux applications malveillantes.

- Désactivez la possibilité d'installer des applications provenant d'autres sources que les boutiques officielles.
- Tenez à jour le système d'exploitation de votre appareil afin de réduire les vulnérabilités dans le logiciel et les risques d'attaque.
- Installez une solution de sécurité éprouvée afin de protéger votre appareil contre les cyberattaques.

Kaspersky Lab s'intéresse depuis longtemps sur le sujet et a d'ailleurs écrit plusieurs articles :

- La Tesla Model S piratée à distance
- Piratage de voitures : une réelle menace ?
- Panique au volant : votre Jeep peut être piratée pendant que vous conduisez.

Pour en savoir plus sur les dangers menaçant pour les véhicules connectés, lisez le blog à ce sujet sur le site Securelist.com.

** Selon les statistiques Google Play.*

À propos de Kaspersky Lab

Kaspersky Lab est une société de cybersécurité mondiale fondée en 1997. L'expertise de Kaspersky Lab en matière de « Threat Intelligence » et sécurité informatique vient perpétuellement enrichir la création de solutions et de services de sécurité pour protéger les entreprises, les infrastructures critiques, les gouvernements et les consommateurs à travers le monde. Le large portefeuille de solutions de sécurité de Kaspersky Lab comprend la protection avancée et complète des terminaux et un certain nombre de solutions et de services de sécurité dédiés afin de lutter contre les menaces digitales sophistiquées et en constante évolution. Les technologies de Kaspersky Lab aident plus de 400 millions d'utilisateurs et 270 000 clients à protéger ce qui compte le plus pour eux.
Pour en savoir plus : www.kaspersky.fr.

Pour en savoir plus : www.kaspersky.com/fr/
Pour plus d'informations sur l'actualité virale :
http://www.securelist.com
Salle de presse virtuelle Kaspersky Lab :
http://newsroom.kaspersky.eu/fr/

Blog français de Kaspersky Lab :
http://blog.kaspersky.fr/