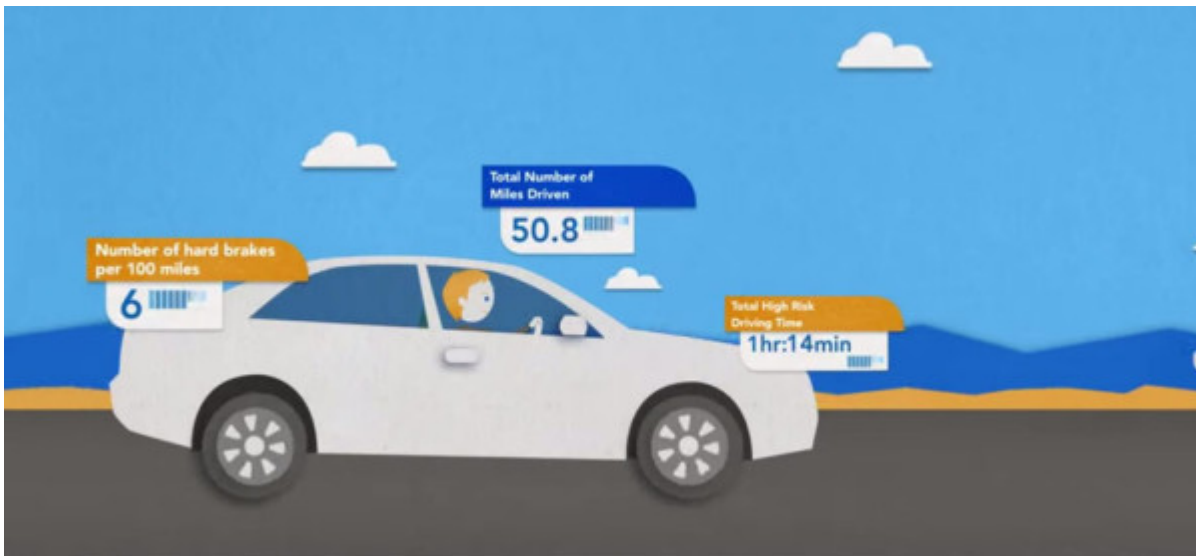


Αυτοκίνητα, υποψήφια θύματα hacking

/ [Πεμπτούσια](#)

Image not found or type unknown



Δύο εκατομμύρια αυτοκίνητα στις ΗΠΑ είναι ευάλωτα σε επιθέσεις hacking, καθώς εντοπίστηκε σε συσκευή που αποστολή της είναι η καταγραφή της οδικής συμπεριφοράς των οδηγών των οχημάτων στα οποία είναι τοποθετημένη.

Μια συσκευή που χρησιμοποιείται από τη Progressive Insurance για τη συλλογή πληροφοριών σχετικά με την οδική συμπεριφορά των πελατών της βρέθηκε να είναι επισφαλής και να επιτρέπει τον απομακρυσμένο έλεγχο του οχήματος.

Η συσκευή με την ονομασία Snapshot, συνδέεται στη θύρα OBD II του αυτοκινήτου προκειμένου να παρακολουθήσει τις ενέργειες του οδηγού, όπως ο τρόπος που φρενάρει. Οι πληροφορίες αυτές αποστέλλονται στους διακομιστές της εταιρείας έτσι ώστε αυτή να δημιουργήσει μια προσαρμοσμένη πολιτική ασφάλισης.

Η θύρα OBD II είναι διαθέσιμη σε όλα τα **αυτοκίνητα** και τα ελαφρά φορτηγά οχήματα που έχουν κατασκευαστεί και πωλούνται στις Ηνωμένες Πολιτείες από το 1996, προσφέρουν επικοινωνία στις συμβατές συσκευές μέσω του διαύλου CAN.

Η [ευπάθεια](#) βρέθηκε από τον ερευνητή ασφάλειας Corey Thuen, ο οποίος χρησιμοποιώντας ένα exploit και αντίστροφη μηχανική στο firmware της συσκευής

ανακάλυψε ότι μπορούσε να αναλάβει τον έλεγχο του εξεταζόμενου αυτοκινήτου.

Ο ερευνητής ανέφερε ότι συνδέοντας το laptop του στη συσκευή μπόρεσε ξεκλειδώσει τις πόρτες του αυτοκινήτου, να εκκινήσει τον κινητήρα και να ελέγξει λεπτομέρειες σχετικά με τον κινητήρα. Η ελλιπής ασφάλεια στο firmware της συσκευής μπορεί να γίνει αντικείμενο εκμετάλλευσης από έναν εισβολέα μέσω απομακρυσμένης επίθεσης [man-in-the-middle](#) (MitM).

Η εταιρεία μέχρι στιγμής δεν έχει προβεί σε κάποια κίνηση, όμως έχει καλέσει τον ερευνητή να τους εκθέσει τα ευρήματά του έτσι ώστε από κοινού διευθετηθούν.

Πηγή: [Secnews.gr](#)

Φωτ.: Youtube