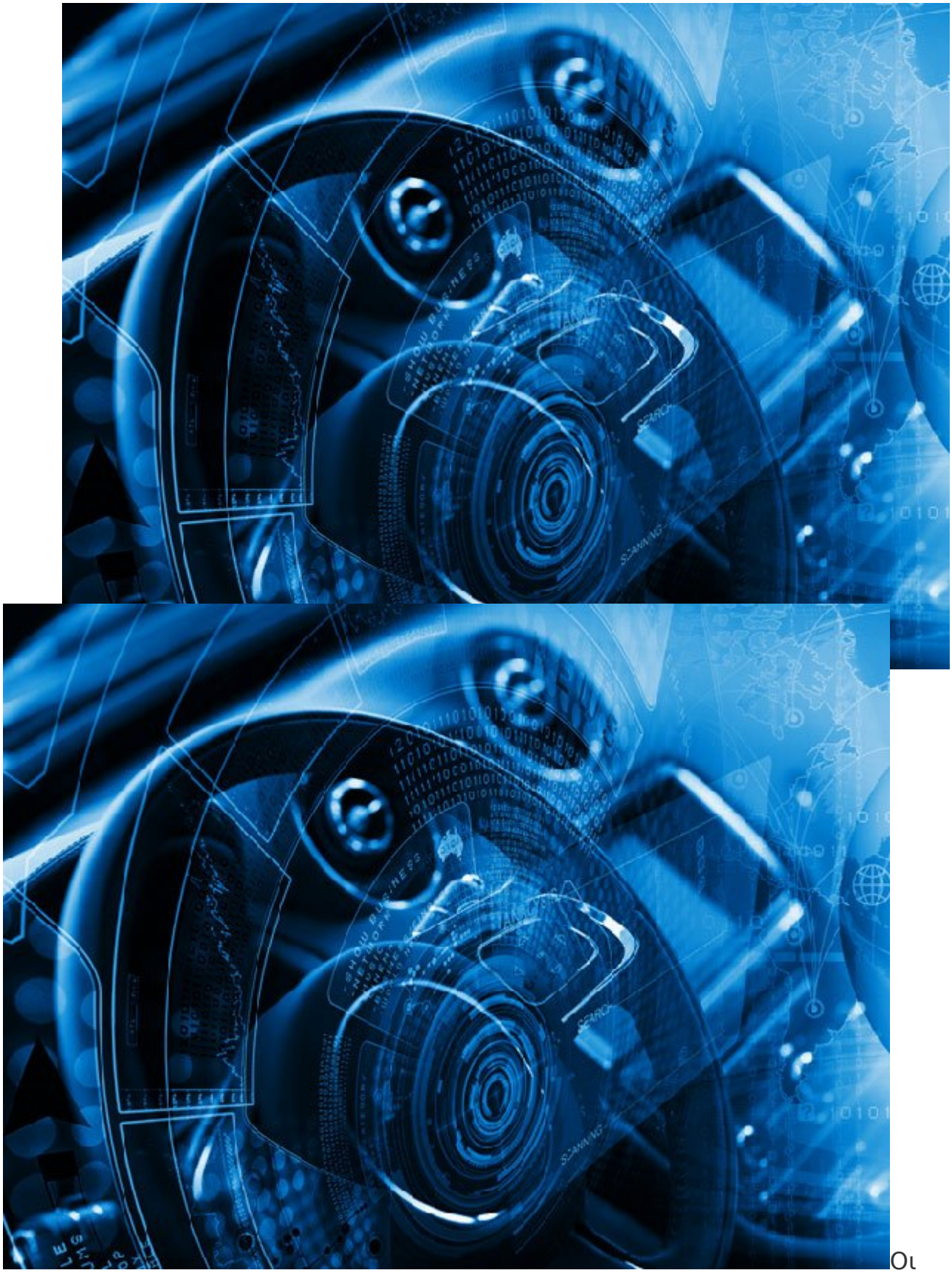
25 Φεβρουαρίου 2017

Συνδεδεμένα αυτοκίνητα: ποιος ελέγχει το αυτοκίνητό σας εν αγνοία σας;

/ Επιστήμες, Τέχνες & Πολιτισμός



Οι

ερευνητές της **Kaspersky Lab** έχουν εξετάσει την ασφάλεια εφαρμογών για τον απομακρυσμένο έλεγχο αυτοκινήτων από πολλούς διάσημους κατασκευαστές αυτοκινήτων. Ως αποτέλεσμα, οι ειδικοί της εταιρείας έχουν ανακαλύψει ότι όλες οι εφαρμογές περιέχουν μια σειρά θεμάτων ασφαλείας που μπορεί δυνητικά να επιτρέψουν σε εγκληματίες να προξενήσουν σημαντική ζημία σε ιδιοκτήτες συνδεδεμένων αυτοκινήτων.

Κατά τη διάρκεια των τελευταίων ετών, έχει ξεκινήσει η ενεργή σύνδεση των αυτοκινήτων στο Διαδίκτυο. Η συνδεσιμότητα περιλαμβάνει όχι μόνο τα συστήματα ενημέρωσης και ψυχαγωγίας τους, αλλά και τα κρίσιμα συστήματα του οχήματος, όπως κλειδαριές θυρών και σύστημα ανάφλεξης, τα οποία είναι πλέον προσβάσιμα στο Διαδίκτυο. Με τη βοήθεια των mobile εφαρμογών, είναι πλέον δυνατόν να ληφθούν οι συντεταγμένες της θέσης του οχήματος, καθώς και η διαδρομή του, αλλά και το άνοιγμα των θυρών, η εκκίνηση του κινητήρα και ο έλεγχος πρόσθετων συσκευών στο εσωτερικό του αυτοκινήτου. Από τη μία πλευρά, αυτές οι λειτουργίες είναι εξαιρετικά χρήσιμες. Από την άλλη, πώς οι κατασκευαστές έχουν διασφαλίσει αυτές τις εφαρμογές απέναντι στον κίνδυνο των ψηφιακών επιθέσεων;

Προκειμένου να το ανακαλύψουν, οι ερευνητές της Kaspersky Lab εξέτασαν επτά εφαρμογές απομακρυσμένου ελέγχου αυτοκινήτων που αναπτύχθηκαν από τους μεγαλύτερους κατασκευαστές αυτοκινήτων, και τις οποίες, σύμφωνα με στατιστικά στοιχεία του Google Play, έχουν «κατεβάσει» χρήστες δεκάδες χιλιάδες φορές, και σε ορισμένες περιπτώσεις, έως και πέντε εκατομμύρια φορές. Η έρευνα ανακάλυψε ότι η κάθε μία από τις εξεταζόμενες εφαρμογές περιείχε διάφορα ζητήματα ασφαλείας.

Ο κατάλογος των θεμάτων ασφαλείας που ανακαλύφθηκαν περιλαμβάνει:

- Απουσία άμυνας απέναντι σε εφαρμογές αντίστροφης μηχανικής. Ως αποτέλεσμα, οι κακόβουλοι χρήστες μπορούν να κατανοήσουν πώς λειτουργεί η εφαρμογή και να εντοπίσουν μια ευπάθεια που θα τους επιτρέψει να αποκτήσουν πρόσβαση σε υποδομές από την πλευρά του server ή σε σύστημα πολυμέσων του αυτοκινήτου.
- Απουσία ελέγχου ακεραιότητας κώδικα, ο οποίος είναι σημαντικός διότι επιτρέπει στους εγκληματίες να ενσωματώσουν δικό τους κώδικα στην εφαρμογή και να αντικαταστήσουν το αρχικό πρόγραμμα με ένα πλαστό.
- Απουσία τεχνικών ανίχνευσης “rooting”. Τα δικαιώματα “root” παρέχουν σε Trojans σχεδόν απεριόριστες δυνατότητες και αφήνουν την εφαρμογή

ανυπεράσπιστη.

- Έλλειψη προστασίας έναντι των τεχνικών επικάλυψης εφαρμογών. Αυτό βοηθά τις κακόβουλες εφαρμογές να προβάλλουν παράθυρα phishing και να κλέβουν τα στοιχεία σύνδεσης των χρηστών.
- Αποθήκευση των στοιχείων σύνδεσης και των κωδικών πρόσβασης σε μορφή απλού κειμένου. Χρησιμοποιώντας αυτή την αδυναμία, ένας εγκληματίας μπορεί να κλέψει τα δεδομένα των χρηστών σχετικά εύκολα.
- Μετά την επιτυχή παραβίαση, ο εισβολέας μπορεί να αποκτήσει τον έλεγχο του αυτοκινήτου, να ξεκλειδώσει τις πόρτες, να απενεργοποιήσει το συναγερμό ασφαλείας και, θεωρητικά, να κλέψει το όχημα.

Σε κάθε περίπτωση, ο φορέας της επίθεσης θα πρέπει να πραγματοποιήσει κάποιες επιπλέον προετοιμασίες, όπως να δελεάσει τους χρήστες των εφαρμογών ώστε να εγκαταστήσουν ειδικά διαμορφωμένες κακόβουλες εφαρμογές, οι οποίες στη συνέχεια θα εισβάλουν στη συσκευή και θα αποκτήσουν πρόσβαση στην εφαρμογή του αυτοκινήτου.

Ωστόσο, όπως οι ειδικοί της Kaspersky Lab έχουν συμπεράνει από την έρευνα σε πολλές άλλες κακόβουλες εφαρμογές που στοχεύουν σε online τραπεζικές συναλλαγές και σε άλλες σημαντικές πληροφορίες, αυτό είναι απίθανο να αποτελεί πρόβλημα για τους εγκληματίες με εμπειρία σε τεχνικές κοινωνικής μηχανικής, αν αποφασίσουν να στραφούν ενάντια στους ιδιοκτήτες των συνδεδεμένων αυτοκινήτων.

Όπως δήλωσε ο **Victor Chebyshev**, ειδικός σε θέματα ασφάλειας της Kaspersky Lab,

> “Το κύριο συμπέρασμα της έρευνάς μας είναι ότι, στη σημερινή τους κατάσταση, οι εφαρμογές για τα συνδεδεμένα αυτοκίνητα δεν είναι έτοιμες να αντιμετωπίσουν τις επιθέσεις κακόβουλου λογισμικού. Εάν κάποιος σκεφτεί την ασφάλεια ενός συνδεδεμένου αυτοκινήτου, δεν θα πρέπει να εξετάσει μόνο την ασφάλεια των υποδομών από πλευράς του server. Αναμένουμε ότι οι κατασκευαστές αυτοκινήτων θα πρέπει να ακολουθήσουν τον ίδιο δρόμο που έχουν χαράξει οι τράπεζες με τις εφαρμογές τους. Αρχικά, οι εφαρμογές για online τραπεζικές συναλλαγές, δεν είχαν όλα τα χαρακτηριστικά ασφαλείας που αναφέρονται στην έρευνα μας. Σήμερα, μετά από πολλαπλές περιπτώσεις επιθέσεων εναντίον τραπεζικών εφαρμογών, πολλές τράπεζες έχουν βελτιώσει την ασφάλεια των προϊόντων τους. Ευτυχώς, δεν έχουμε ακόμη εντοπίσει κανένα κρούσμα επιθέσεων ενάντια σε εφαρμογές

αυτοκινήτων, πράγμα που σημαίνει ότι οι πωλητές αυτοκινήτων εξακολουθούν να έχουν χρόνο για να ρυθμίσουν τα πράγματα σωστά. Πόσο χρόνο έχουν ακριβώς είναι άγνωστο. Τα σύγχρονα Trojans είναι πολύ ευέλικτα – τη μια μέρα μπορούν να λειτουργούν σαν κανονικό adware, και την επόμενη μέρα μπορούν εύκολα να κατεβάσουν μια νέα ρύθμιση που θα τους δώσει τη δυνατότητα να στοχεύουν σε νέες εφαρμογές. Η επιφάνεια επίθεσης στην προκειμένη περίπτωση είναι πραγματικά μεγάλη”

Οι ερευνητές της Kaspersky Lab συμβουλεύουν τους χρήστες των εφαρμογών συνδεδεμένων αυτοκινήτων να ακολουθούν τις παρακάτω συμβουλές προκειμένου να προστατεύσουν τα αυτοκίνητά και τα προσωπικά τους δεδομένα από πιθανές ψηφιακές επιθέσεις:

- Αποφύγετε να κάνετε «root» στην Android συσκευή σας, καθώς αυτό θα ανοίξει σχεδόν απεριόριστες δυνατότητες σε κακόβουλες εφαρμογές
- Απενεργοποιήστε τη δυνατότητα εγκατάστασης εφαρμογών από άλλες πηγές εκτός από τα επίσημα app stores.
- Αναβαθμίστε με την τελευταία έκδοση το λειτουργικό σύστημα της συσκευής σας, προκειμένου να μειωθούν οι ευπάθειες του λογισμικού και να μειωθεί ο κίνδυνος επίθεσης.
- Τοποθετήστε μια δοκιμασμένη λύση ασφάλειας για την προστασία της συσκευής σας από ψηφιακές επιθέσεις.

Πηγή: offsite.com.cy