31 Ιανουαρίου 2015

# Play Store: τα δημοφιλέστερα apps δεν είναι ασφαλή

/ Πεμπτουσία

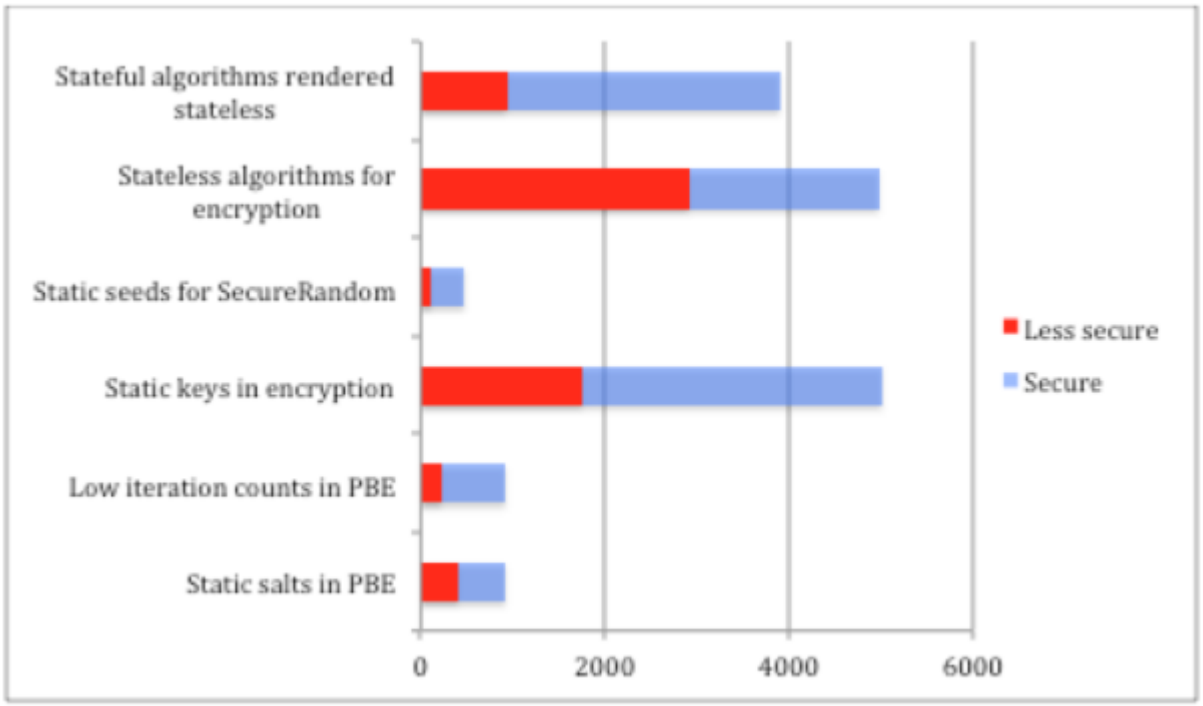
Image not found or type unknown

**Δωρεάν *apps* στο Google Play Store, με περισσότερες από ένα εκατομμύριο λήψεις, έχουν βρεθεί να έχουν ευάλωτα συστήματα κρυπτογράφησης για την προστασία των ευαίσθητων πληροφοριών που αποθηκεύουν.**

Μια ανάλυση σχετικά με τα 9,339 πιο δημοφιλή δωρεάν apps που είναι διαθέσιμα στο επίσημο store Android, αποκαλύπτει ότι περίπου το 62% από αυτά, (5,147), αποτυγχάνουν να εξασφαλίσουν και να ασφαλίσουν κατάλληλα τα εμπιστευτικά στοιχεία του χρήστη και θα μπορούσε να επιτρέψει σε κάποιον εισβολέα να κλέψει τις προστατευόμενες πληροφορίες αξιοποιώντας τα διάφορα αδύνατα σημεία.

Ερευνητές στο FireEye, πραγματοποίησαν τη δοκιμή στο δείγμα που πληρούσε τα κριτήρια δημοτικότητας που αναφέρονται παραπάνω από 22 Νοεμβρίου 2014 και μετά.

Οι εμπειρογνώμονες ασφάλειας μελέτησαν τα τρωτά σημεία που σχετίζονται με την έλλειψη υψηλής εντροπίας, με αλγόριθμους κρυπτογράφησης και κωδικούς πρόσβασης βασισμένους σε κάποια κρυπτογράφηση.




Το μεγαλύτερο μέρος των προϊόντων που βρέθηκε κρυπτογραφικά ανασφαλές χρησιμοποιεί αλγόριθμους για κρυπτογράφηση, πράγμα που σημαίνει ότι ένα δεδομένο έχει την ίδια ακριβώς απόδοση κάθε φορά αυτό κρυπτογραφείται. Έτσι ένας εισβολέας θα μπορούσε χρησιμοποιώντας ένα λεξικό να βρει την αρχική συμβολοσειρά, χωρίς την ανάγκη να γνωρίζει τα κλειδιά που χρησιμοποιούνται για την κρυπτογράφηση.

Στη περίπτωση χαμηλής εντροπίας που σχετίζονται με αδυναμίες, το FireEye αναφέρει 1,762 apps, που χρησιμοποιούν στατικό κλειδί για την κρυπτογράφηση των πληροφοριών, που θα μπορούσε να εξαχθεί, για να αντιστραφεί η διαδικασία.

918 προϊόντα βρέθηκαν να στηρίζουν τη προστασία δεδομένων σε μηχανισμούς με κωδικούς πρόσβασης. 409 από αυτά, χρησιμοποιούν στατική κρυπτογράφηση με τυχαία ακολουθία χαρακτήρων, για να γίνει πιο δύσκολο να βρεθεί, το password. Αν το παραγόμενο password έχει μια σταθερή μεταβλητή, ο αλγόριθμος είναι αδύναμος και οι πληροφορίες μπορεί να εξαχθούν εύκολα.

Πηγή: Secnews.gr