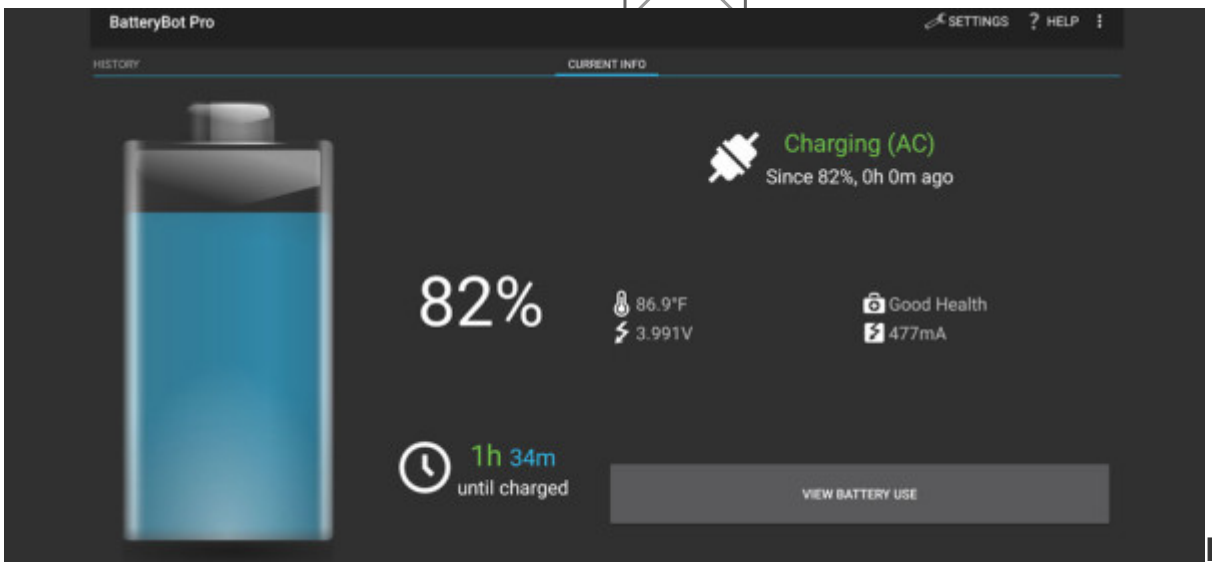
19 Ιουλίου 2015

Πλαστό App απειλεί τα κινητά

/ Πεμπτουσία

Image not found or type unknown



Μια νέα μορφή mobile malware που σχεδιάστηκε για πολλαπλές κακόβουλες δραστηριότητες έχει εμφανιστεί, υπό μορφή καμουφλαρισμένου app που είναι αντίγραφο του έγκυρου app BatteryBot Pro.To fake app θα παράσχει την ίδια λειτουργία στο θύμα με αυτή της γνήσιας έκδοσης του BatteryBot Pro, αλλά την ίδια στιγμή εκτελεί κακόβουλη δραστηριότητα στο υπόβαθρο.

Κυρίως, αν και το app φαίνεται ότι λειτουργεί κανονικά, στο back-end προσπαθεί να φορτώσει διάφορες ad libraries, παραδίδοντας τελικά μια click-fraud campaign.

Σύμφωνα με το Zscaler, άλλες λειτουργίες περιλαμβάνουν το ad fraud, SMS fraud, και την εγκατάσταση επιπλέον κακόβουλων APKs.
Η κακόβουλη εφαρμογή δείχνει να δουλεύει κανονικά. Η κύρια δραστηριότητα είναι ίδια με αυτή του γνήσιου app, αλλά όταν χτυπά ο χρήστης κάνει κλικ στο "View Battery Use," το malware στέλνει αιτήματα στο command and control server για να ανακτήσει τους short codes για τους premium-rate SMS numbers. Το συνολικό κόστος των μηνυμάτων που στέλνονται θα προστεθούν στον λογαριασμό του χρήστη.

Το App αφαιρέθηκε από το Play Store αμέσως μόλις η Google ενημερώθηκε για την

κακόβουλη δραστηριότητά του, αλλά για εκείνους που το εγκατέστησαν ήδη τα νέα είναι άσχημα.

Μετά την εγκατάσταση του κακόβουλου app, απαιτείται administrative access, η οποία επιτρέπει στον developer του malware να έχει τον πλήρη έλεγχο της συσκευής του θύματος. Και το να τρέχει με administrator privileges σημαίνει ουσιαστικά ότι ο χρήστης και κάτοχος της μολυσμένης συσκευής δεν μπορεί να το αφαιρέσει μετά την εγκατάσταση.

Τα καμουφλαρισμένα πλαστά Android apps είναι όλα πάρα πολύ κοινά μεταξύ τους. Ενώ το γνήσιο BatteryBot Pro app απαιτούσε το ελάχιστο των αδειών χρήσης, το fake app απαιτούσε πλήρη admin access με σκοπό να αποκτήσει τον πλήρη έλεγχο της συσκευής του θύματος.

Για αυτό το λόγο οι χρήστες πρέπει να είναι υποψιασμένοι και ιδιαίτερα προσεκτικοί και να ερευνούν πολύ για τις άδειες χρήσης προτού αποφασίσουν να εγκαταστήσουν μια εφαρμογή στην κινητή συσκευή τους.

Πηγή: SecNews.gr