21 Ιουλίου 2015

Νέο malware εκμεταλλεύεται την πρόσβαση σε Android

/ Πεμπτουσία

Image not found or type unknown

WROCLAW, POLAND - AUGUST 26, 2014: Photo of a Samsung Galaxy S2 Android smartphon

Image not found or type unknown

Ερευνητές από την εταιρεία ασφαλείας για smartphones, LookOut, που εδρεύει στο San Francisco, και ερευνά θέματα για την ασφάλεια τόσο των ιδιωτών όσο και των επιχειρήσεων, εντόπισαν κακόβουλο λογισμικό, με την ονομασία "AndroRATIntern". Το εν λόγω λογισμικό καταχράται την υπηρεσία πρόσβασης σε *Android* συσκευές, ώστε να υποκλέψει ευαίσθητα δεδομένα από μολυσμένα smartphones.

Μετά την ανακάλυψη αυτής της απειλής, η εταιρία LookOut, ειδοποίησε τόσο τη LINE όσο και τη Google. Η απάντηση σε αυτό ήταν ότι τα συστήματα της LINE δε κινδυνεύουν και ότι όλοι οι χρήστες της Lookout είναι ασφαλείς.

Σύμφωνα με τους ερευνητές, το AndroRATIntern είναι τύπου surveillanceware που αναπτύχθηκε από το λογισμικό AndroRAT malware toolkit και πωλείται στο εμπόριο ως το "AndroidAnalyzer". Μάλιστα όπως αναφέρεται είναι το πρώτο malware για Android, που παραβιάζει την υπηρεσία πρόσβασης ώστε να υποκλέψει δεδομένα.

Το κακόβουλο λογισμικό στοχεύει κυρίως την Ιαπωνική αγορά. Μπορεί να συλλέξει μια ευρεία ποσότητα δεδομένων από μολυσμένες συσκευές, συμπεριλαμβανομένων της LINE, που επιτρέπει στους χρήστες να πραγματοποιούν φωνητικές κλήσεις, αλλά και βίντεο κλήσεις, να στέλνουν μηνύματα. Η πρόσβαση που έχει το λογισμικό είναι στα μηνύματα, στην επικοινωνία δεδομένων, στα αρχεία κλήσεων, στα SMS, στον ήχο, στα βίντεο, στις φωτογραφίες, στην SD κάρτα και τέλος στην τοποθεσία του χρήστη μέσω του GPS.

Οι ερευνητές αναφέρουν επίσης ότι το AndroRATIntern, πρέπει να εγκατασταθεί στη συσκευή, γεγονός που απαιτεί επαφή με το smartphone και έτσι δε μπορεί να εξαπλωθεί με drive-by-download campaigns.

Για την ασφάλεια των χρηστών οι ερευνητές προτείνουν τη χρήση κωδικού για το

άνοιγμα της συσκευής, καθώς και τη χρήση ενημερωμένου λογισμικού ασφαλείας για τον εντοπισμό malware που πιθανόν να έχουν γίνει download στο smartphone.

Πηγή: SecNews.gr