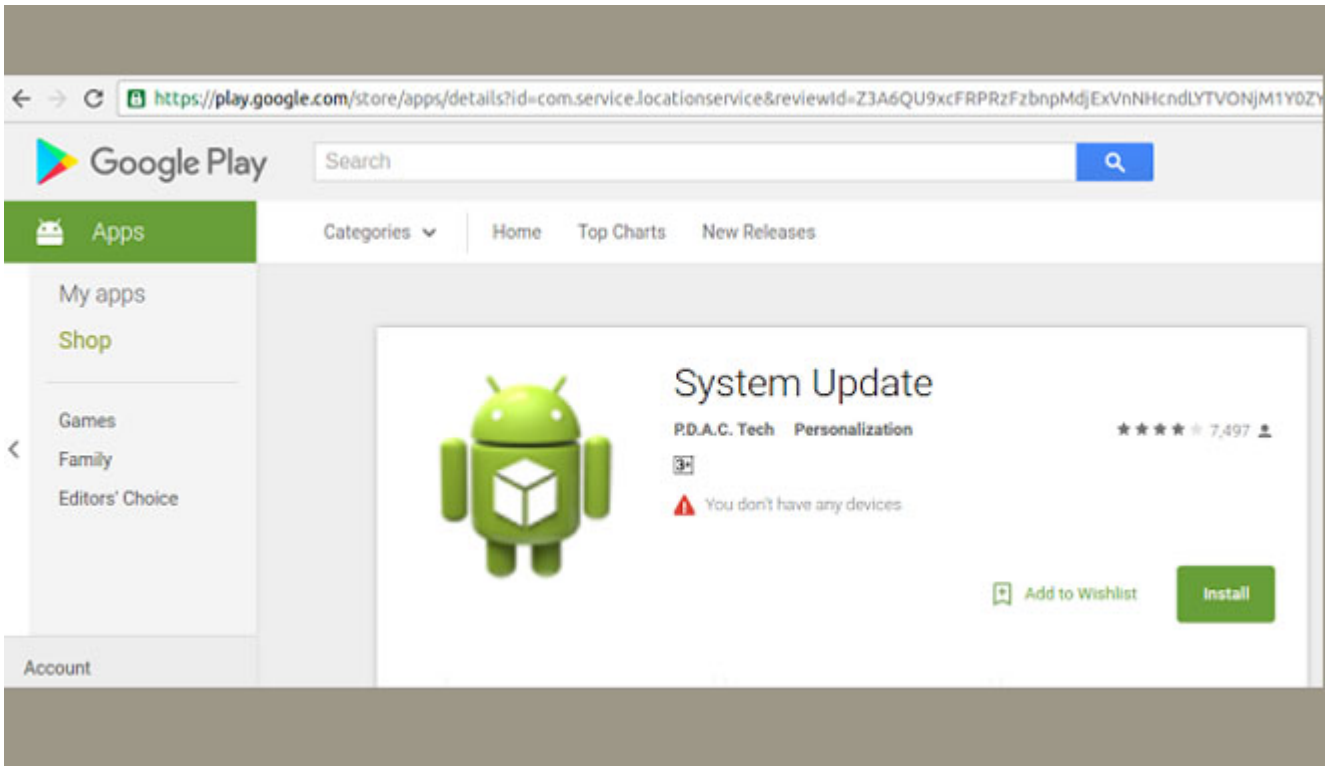
23 Απριλίου 2017

# «System Update» app: έχει μολύνει εκατομμύρια Android συσκευές!

/ Πεμπτουσία

Image not found or type unknown




Ένα βασικό στοιχείο που οι χρήστες Android θα πρέπει να γνωρίζουν για τις συσκευές τους, είναι ότι οι ενημερώσεις συστήματος έρχονται αυτόματα και δεν απαιτούν τη λήψη και εγκατάσταση οποιουδήποτε εργαλείου ή εφαρμογής. Αυτό είναι κάτι που όπως φαίνεται αγνοούσαν εκατομμύρια χρήστες, καθώς στην προσπάθειά τους να λάβουν τις πιο πρόσφατες ενημερώσεις λογισμικού, έπεσαν θύματα μιας καλοσχεδιασμένης απάτης, κατεβάζοντας μια εφαρμογή Android με spyware.

Σύμφωνα με ερευνητές ασφάλειας της Zscaler, η εφαρμογή «System Update» διατίθετο ως νόμιμο app στο Google Play Store. Το app υποσχόταν ψευδώς πρόσβαση στις πιο πρόσφατες ενημερώσεις λογισμικού Android (κάτι φυσικά που δεν μπορεί να επιτευχθεί μέσω οποιασδήποτε εφαρμογής τρίτου).

Το πιο ανησυχητικό είναι πως η κακόβουλη εφαρμογή είχε ανέβει στο διαδικτυακό

κατάστημα εφαρμογών της Google από το 2014, αριθμώντας περισσότερες από 1 έως 5 εκατομμύρια λήψεις. Η εφαρμογή έχει πλέον καταργηθεί από το Play Store, όμως εκτιμάται πως σε διάστημα 3 ετών κατάφερε να προκαλέσει μεγάλη ζημιά, μολύνοντας εκατομμύρια συσκευές με spyware.

Μεταξύ των δυνατοτήτων της κακόβουλης εφαρμογής ήταν η παρακολούθηση της ακριβούς γεωγραφικής θέσης των θυμάτων (geolocation), κάτι που θα μπορούσε να χρησιμοποιηθεί για ένα ευρύ φάσμα κακόβουλων δραστηριοτήτων.

“Η εφαρμογή απεικονίζεται ως μια ενημερωμένη έκδοση συστήματος (System Update) και η αποστολή πληροφοριών τοποθεσίας σε τρίτους δεν αναφέρεται στην περιγραφή της”, επισημαίνει η Zscaler .

Όπως προκύπτει και από τα σχόλια των χρηστών που είχαν κατεβάσει την εφαρμογή, μετά την εκκίνησή της εμφανιζόταν το εξής μήνυμα: “Δυστυχώς, το System Update έχει σταματήσει”, και στη συνέχεια τερματιζόταν η λειτουργία της. Αυτό δεν σημαίνει πως η εφαρμογή σταματούσε πραγματικά να λειτουργεί. Αντ ‘αυτού το spyware δημιουργούσε ένα νέο Android service και έτρεχε στο παρασκήνιο, ανακτώντας πληροφορίες σχετικά με την τοποθεσία των χρηστών (geolocation) και σαρώνοντας για τυχόν νέα εισερχόμενα μηνύματα SMS.

Σύμφωνα με τους ερευνητές όταν η εφαρμογή εντόπιζε κάποιο μήνυμα με την εντολή “get faq” (το οποίο αποστελλόταν από τους εγκληματίες) τότε ξεκινούσε η εκτέλεση μιας επιπρόσθετης σειράς κακόβουλων εντολών.

Πηγή: Secnews.gr