10 Απριλίου 2021

Η επικίνδυνη εφαρμογή στα Android που ‘κλέβει’ τα δεδομένα σας

/ Επιστήμες, Τέχνες & Πολιτισμός

Εταιρία ασφαλείας κινητών τηλεφώνων εντόπισε app στα Android που λέει πως κάνει update, αλλά αν το ‘κατεβάσετε’ δίνετε πρόσβαση σε ό,τι υπάρχει μέσα στη συσκευή σας. “Είναι το πιο εκλεπτυσμένο κακόβουλο λογισμικό που έχουμε δει έως σήμερα”.

Η εφαρμογή που λέει πως κάνει update, 'μπαίνει' στο κινητό σας και 'κλέβει' ό,τι υπάρχει σε αυτό.
SHUTTERSTOCK

Στα Android υπάρχει μια εφαρμογή με το όνομα 'System Update'. Δεν είναι όμως, αυτό που φαίνεται. Δηλαδή, αναβάθμιση συστήματος. Όπως ανακάλυψαν ερευνητές της εταιρίας ασφαλείας κινητών τηλεφώνων Zimperium, είναι κακόβουλη εφαρμογή που λέει ότι θα κάνει επικαιροποίηση, αλλά αν την 'κατεβάσετε' θα κλέψει όλα τα δεδομένα που έχετε στο τηλέφωνο και θα παρακολουθεί όλες τις κινήσεις που κάνετε σε αυτό.

Πρόκειται για τεράστια εφαρμογή spyware, με τη Zimperium να κατατάσσει το app στην κατηγορία Remote Access Trojan (RAT), μια ευρεία κατηγορία κακόβουλων λογισμικών που επιτρέψει στους χάκερ την πρόσβαση και το χειρισμό της συσκευής σας, από απόσταση.Ο CEO της Zimperium, Σριντάρ Μιτάλ δήλωσε πως πιστεύει ότι πρόκειται για 'στοχευμένη επίθεση. Είναι το πιο εκλεπτυσμένο RAT που έχουμε δει. Ξοδεύτηκε πολύς χρόνος και προσπάθεια στη δημιουργία αυτής της εφαρμογής. Πιστεύουμε ότι υπάρχουν κι άλλες που λειτουργούν κατά τον ίδιο τρόπο και προσπαθούμε να τις βρούμε το συντομότερο δυνατό".

Τι μπορεί να 'κλέψει'
Από γραπτά μηνύματα και αρχεία βάσης δεδομένων, έως αρχεία καταγραφής κλήσεων και επαφές. Όπου 'γραπτά μηνύματα', δεν περιορίζεται μόνο στα messages, αλλά φτάνει και σε εκείνα στο Whatsapp, από όπου μπορεί να κλέψει εικόνες και βίντεο -συν τις όποιες άλλες πληροφορίες. Το System Update δίνει στους χάκερ πρόσβαση σε ό,τι υπάρχει στο smartphone σας (φωτογραφίες,

ιστορικό), συμπεριλαμβανομένου του πού είστε (GPS location). Επίσης, μπορεί να ανοίξει το μικρόφωνο και να σας ηχογραφήσει την ώρα που είστε σε μια κλήση. Ενεργοποιείται κάθε φορά που δέχεται πληροφορία η συσκευή στην οποία έχει εγκατασταθεί.

Τι κάνει όσα ‘κλέβει’
Αφότου πάρει ό,τι θέλει να πάρει από το smartphone σας, ανεβάζει ό,τι θέλει να ανεβάσει αυτός που ‘μπαίνει’ στη συσκευή σας στο C&C server (είναι υπολογιστής που ‘βγάζει’ οδηγίες στις ψηφιακές συσκευές που έχουν ‘μολυνθεί’ και μπορεί να δημιουργήσει ισχυρά δίκτυα ‘μολυσμένων’ συσκευών, στο πλαίσιο σχεδίου εκβιασμού ή πώλησης δεδομένων) , σε κρυπτογραφημένο αρχείο ZIP. Μετά διαγράφει τα αποδεικτικά στοιχεία -και όσα έχει κάνει.

Πηγή: news247.gr