9 Μαρτίου 2019

Συσκευές που χακάρουν κινητά τηλέφωνα κυκλοφορούν ελεύθερα στην αγορά

/ Επιστήμες, Τέχνες & Πολιτισμός



Ελεύθερες στο εμπόριο κυκλοφορούν συσκευές, οι οποίες μπορούν πολύ εύκολα να χακάρουν τα smartphones και τα laptop.

Διαβάστε επίσης: Με αυτή την εφαρμογή μπορείς να κατασκοπεύσεις το κινητό και το Facebook του συντρόφου σου

Ένας πωλητής του eBay βρέθηκε σε μια δημοπρασία στη Μεγάλη Βρετανία και βρήκε μια παράξενη συσκευή, που δεν είχε την παραμικρή ιδέα τι έκανε. Ο πωλητής παράτησε τη συγκεκριμένη συσκευή στο γκαράζ του για πολλούς μήνες.

Όμως πριν από λίγο καιρό κατάλαβε τι ακριβώς κάνει αυτή η συσκευή. Το περίεργο «μαραφέτι» ήταν ένα πολύ ακριβό τεχνολογικό δημιούργημα του Ισραήλ, με την ονομασία Cellebrite UFED.



Η συγκεκριμένη συσκευή χρησιμοποιείται από την Αστυνομία σε όλο τον κόσμο, για να «σπάει» την προστασία συσκευών που χρησιμοποιούν λογισμικών iOS και Android, ώστε να εξαγάγει δεδομένα.

Η ομοσπονδιακή κυβέρνηση των ΗΠΑ δίνει εκατομμύρια στη Cellebrite για να έχει στα χέρια της αυτήν την τεχνολογία, αλλά στο eBay τα συστήματα της συγκεκριμένης εταιρείας πωλούνται για ποσά μεταξύ 100 και 1.000 δολαρίων, αναφέρει άρθρο του Forbes.Τα τελευταίας τεχνολογίας Cellebrite ξεκινούν από 6.000 δολάρια.

Η Cellebrite δεν είναι ευχαριστημένη με το γεγονός ότι οι μεταχειρισμένες αυτές συσκευές της πωλούνται με τέτοια άνεση στην αγορά. Μάλιστα, την περασμένη Τρίτη, δύο πηγές από τη βιομηχανία εγκληματολογίας προώθησαν στο Forbes μια επιστολή που καταδεικνύει πόσο επικίνδυνη για τα προσωπικά δεδομένα είναι η μεταπώληση αυτών των εξαιρετικά δημοφιλών συσκευών χακαρίσματος.

Αντί, λοιπόν, να επιστρέψουν τα UFEDs στη Cellebrite, ώστε να μπορούν να βγουν με τον σωστό τρόπο εκτός λειτουργίας, φαίνεται ότι οι Αρχές ή άλλα άτομα που έχουν αποκτήσει τα μηχανήματα αυτά, δεν φροντίζουν για τον σωστό... παροπλισμό τους. Οι ερευνητές στο διαδίκτυο προειδοποιούν ότι θα μπορούσαν να διαρρεύσουν πολύτιμα δεδομένα από αυτά τα ισχυρά εργαλεία πειρατείας.

Σύμφωνα με το δημοσίευμα, ο Μάθιου Χίκεϊ, ερευνητής στον κυβερνοχώρο και συνιδρυτής της Ακαδημίας Hacker House, αγόρασε δώδεκα συσκευές UFED και τις εξέτασε για τυχόν δεδομένα. Ανακάλυψε ότι το αυτά περιείχαν πληροφορίες σχετικά με τις συσκευές που αναζητήθηκαν, την ίδια την αναζήτηση, αλλά και το είδος των δεδομένων που καταργήθηκαν.

Πηγή: **pagenews.gr**