7 Ιουνίου 2016

Χάκερ βρίσκει bug που αφήνει τον καθένα να κλέψει δις από μια τράπεζα!

/ Επιστήμες, Τέχνες & Πολιτισμός

Ένας Ινδός ηθικός χάκερ βρήκε διάφορα bugs σε μια εφαρμογή για Τράπεζα που θα μπορούσε να επιτρέψει σε οποιονδήποτε να κλέψει $25 δις. Μια άγνωστη τράπεζα ήταν τυχερή που ένας ηθικός hacker βρήκε ελαττώματα και τους ενημέρωσε σχετικά. Αν ερχόταν με κακό σκοπό, θα μπορούσε να είχε φύγει κατά $25 δισεκατομμύρια πλουσιότερος.

Στα τέλη του περασμένου έτους, ο ερευνητής ασφαλείας, Sathya Prakash, ανακάλυψε μια σειρά από κρίσιμα θέματα ευπάθειας στην τραπεζική εφαρμογή για

κινητά μιας άγνωστης τράπεζας που του επέτρεπε να κλέψει χρήματα από οποιονδήποτε ή από όλους τους πελάτες της με τη βοήθεια μόνο λίγων γραμμών κώδικα.

Ωστόσο, ο Prakash αμέσως επικοινώνησε με την εν λόγω τράπεζα και της έκρουσε τον κώδωνα του κινδύνου σχετικά με τα σοβαρά ελαττώματα στο mobile banking app της. Επίσης, τη βοήθησε να διορθώσει τα bugs, αντί να εκμεταλλευτεί τα κενά ασφαλείας για να κλέψει χρήματα από την τράπεζα που έχει περίπου $25 δισεκατομμύρια σε καταθέσεις.

Σύμφωνα με τον Prakash, όταν ανέλυσε την εφαρμογή της τράπεζας, βρήκε ότι είχε πολλά σφάλματα. Ο Prakash ανακάλυψε ότι η εφαρμογή δεν διαθέτει Certificate Pinning, επιτρέποντας κάθε man-in-the-middle εισβολέα να υποβαθμίσει την SSL σύνδεση και να «αιχμαλωτίσει» requests σε μορφή απλού κειμένου χρησιμοποιώντας δόλο εκδίδοντας πιστοποιητικά. Αυτό το σφάλμα του επέτρεπε να δει εύκολα τα αρχεία των τραπεζικών πελατών, όπως το τρέχον υπόλοιπο του λογαριασμού τους και τις καταθέσεις τους μόνο αυτοματοποιώντας και μαντεύοντας το αναγνωριστικό του πελάτη.

Αυτό ήταν μόνο η αρχή όμως, και όταν ο ίδιος συνέχισε το ψάξιμο και βρήκε ένα μεγάλο σφάλμα που του επέτρεπε να επιλέξει οποιοδήποτε λογαριασμό μέσω του App και να μεταφέρει τα χρήματα από τον εν λόγω λογαριασμό στο λογαριασμό κάποιου άλλου. Ο Prakash διαπίστωσε ότι το mobile banking app είχε ανασφαλή αρχιτεκτονική login, επιτρέποντάς του να εκτελέσει κρίσιμες δράσεις για λογαριασμό του κατόχου του στοχευμένου λογαριασμού χωρίς να γνωρίζει τον κωδικό σύνδεσης, όπως να βλέπει το τρέχον υπόλοιπο του λογαριασμού και των καταθέσεων του θύματος, καθώς και να προσθέσει ένα νέο δικαιούχο και κάνοντας παράνομες μεταφορές.

Ο Prakash ανακάλυψε, επίσης, ότι το τραπεζικό app δεν έλεγχε αν το συγκεκριμένο ID πελάτη ή το Transaction Authorisation PIN (MTPIN) στην πραγματικότητα ανήκε στον αποστολέα. Το MTPIN χρησιμοποιείται από τις τραπεζικές συναλλαγές για τη μεταφορά κεφαλαίων ή τη δημιουργία ενός νέου τραπεζικού λογαριασμού / προθεσμιακής κατάθεσης.

Ο Prakash δοκίμασε με επιτυχία αυτό το ελάττωμα, χρησιμοποιώντας τους λογαριασμούς των γονιών του. Μόλις δοκίμασε και επιβεβαίωσε τις αδυναμίες, αντί να εκμεταλλευτεί την κατάσταση, έστειλε ένα e-mail με υπευθυνότητα την τράπεζα στις 13 Νοεμβρίου, 2015. Η τράπεζα έλαβε γνώση της ανακάλυψής του και αμέσως ενημέρωσε το banking App για να επιδιορθώσει τα ελαττώματά του. Ωστόσο, ο Prakash ούτε πληρώθηκε γενναιόδωρα για την ανακάλυψη του bug ούτε

του απονεμήθηκαν συγχαρητήρια από την τράπεζα για την εξοικονόμηση εκατομμυρίων, αν όχι δισεκατομμυρίων.

Πηγή: secnews.gr