29 Οκτωβρίου 2015

Κινητά τηλέφωνα: κίνδυνος υποκλοπής μέσω ραδιοκυμάτων

Επιστήμες / Πληροφορική & Internet

Χρησιμοποιώντας την απλή μέθοδο της αποστολής ραδιοκυμάτων σε iPhone ή Android κινητό, χρησιμοποιώντας το καλώδιο των ακουστικών του ως κεραία που ανιχνεύει τα ραδιοκύματα και τα αναμεταδίδει στο λογισμικό αναγνώρισης φωνής του λειτουργικού συστήματος, χάκερς είναι πλέον σε θέση να αναγκάσουν, σιωπηρά, το τηλέφωνο να πραγματοποιεί κακόβουλες ενέργειες, με την προϋπόθεση ότι ο χρήστης δεν κοιτάζει την οθόνη του, κατά την εξέλιξη της διαδικασίας αυτής.

Οι José Lopes Esteves και Chaouki Kasmi, δύο ερευνητές ασφαλείας του Anssi (Agence Nationale de la Sécurité des Systèmes d'Information), έναν γαλλικό εθνικό οργανισμό αφιερωμένο στην IT ασφάλεια, έχουν δημιουργήσει μια ειδική κατασκευή που αποτελείται από μια κεραία, ένα USRP ραδιόφωνο, έναν ενισχυτή και ένα laptop που τρέχει το GNU Radio λογισμικό. Αυτή η κατασκευή είναι σε θέση να στείλει τα ραδιοκύματα σε ένα iPhone ή ένα Android με τα ακουστικά ακόμα επάνω του, χρησιμοποιώντας το καλώδιο των ακουστικών ως κεραία που ανιχνεύει τα ραδιοκύματα και τα αναμεταδίδει στο λογισμικό αναγνώρισης φωνής του λειτουργικού συστήματος.

Οτιδήποτε επιτρέπεται να κάνουν τα Siri και Google Now, οι βοηθοί φωνής για iOS και Android αντίστοιχα, μπορεί να τα κάνει και ο χάκερ. Αυτό περιλαμβάνει την αποστολή κειμένων, πραγματοποίηση τηλεφωνικών κλήσεων, άνοιγμα των ιστοσελίδων, εγκατάσταση εφαρμογών και ούτω καθεξής.

Ωστόσο, υπάρχουν κάποιοι περιορισμοί σε αυτήν την επίθεση όπως έχετε ήδη ενδεχομένως φανταστεί. Πρώτα απ' όλα, λειτουργεί μόνο μόνο όταν είναι συνδεδεμένα τα ακουστικά στη συσκευή και τα ακουστικά έχουν ενσωματωμένο μικρόφωνο δηλαδή δεν είναι απλά για να ακούει κανείς μουσική.

Δεύτερον, η κατασκευή είναι αρκετά ογκώδης και έχει μειωμένη εμβέλεια επίθεσης. Εάν ο εισβολέας θέλει να χρησιμοποιήσει μια μικρή κατασκευή, τότε δεν θα είναι σε θέση να φθάσει τηλέφωνα σε απόσταση μεγαλύτερη των 2 μέτρων. Αν θέλει να χρησιμοποιήσει ολόκληρη την κατασκευή, τότε θα χρειαστεί ένα αυτοκίνητο για να την κρύψει και να τη μετακινήσετε, όμως σε αυτή την περίπτωση, θα είναι σε θέση να τη χρησιμοποιήσει σε μια απόσταση των 5 μέτρων. Μπορείτε να δείτε πόσο μεγάλη είναι η κεραία είναι από το βίντεο που ακολουθεί:

Η επίθεση δεν θα λειτουργήσει για τις εκδόσεις Google Now και Siri (iPhone 6s) που έχουν ρυθμιστεί να αναγνωρίζουν τη φωνή του ιδιοκτήτη τους. Επιπλέον, για κλειδωμένα τηλέφωνα, το χαρακτηριστικό του βοηθού φωνής πρέπει να είναι ενεργοποιημένο για την lockscreen.

Σε παλαιότερα iPhones, όπου η Siri μπορεί να ενεργοποιηθεί από το παρατεταμένο πάτημα ενός κουμπιού στα ακουστικά, οι hackers θα πρέπει επίσης να μιμηθούν αυτό το ηλεκτρικό σήμα όταν στέλνουν ραδιοκύματα, καθιστώντας την επίθεση ακόμη πιο περίπλοκη.

Τι πρέπει να γίνει;

Για την προστασία από αυτό τον τρόπο επίθεσης, οι ερευνητές ενθαρρύνουν τους χρήστες να μην αφήνουν τα ακουστικά τους συνδεδεμένα στις συσκευές τους όταν δεν χρησιμοποιούνται. Επιπλέον, θα πρέπει επίσης να χρησιμοποιούν ακουστικά χωρίς μικρόφωνο και να ενεργοποιήσουν το λογισμικό φωνητικής βοήθειας μόνο όταν το χρειάζονται.

Για τους κατασκευαστές, οι ερευνητές συστήνουν καλύτερη θωράκιση των καλωδίων των ακουστικών, εφαρμογή λειτουργιών αναγνώρισης φωνής για όλες τις υπηρεσίες που χρησιμοποιούν τη φωνητική βοήθεια, προσθέτοντας έναν αισθητήρα για την ανίχνευση αφύσικης ηλεκτρομαγνητικής δραστηριότητας και επιπλέον ενθαρρύνουν τους χρήστες να χρησιμοποιούν προσαρμοσμένες εντολές

για την ενεργοποίηση του βοηθού φωνής, αντί του κλασικού “Hey Siri” και “OK Google“.

Πηγή: secnews.gr

http://bitly.com/1P69cgc