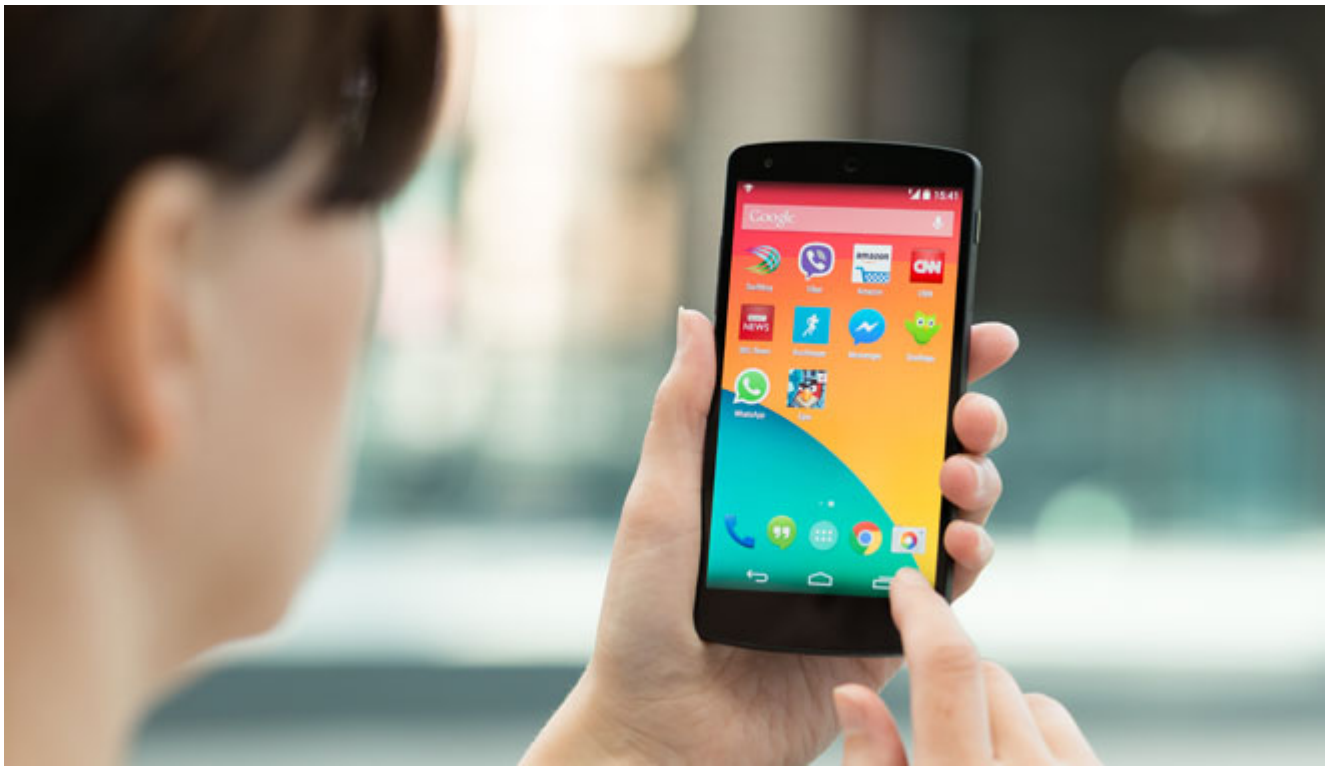
24 Σεπτεμβρίου 2016

Android Trojan – κίνδυνος για τα δεδομένα σας στον Chrome

/ Πεμπτουσία

Image not found or type unknown



Μια Android malware οικογένεια που φέρει το αναγνωριστικό Trojan-Banker.AndroidOS.Tordow.a (Tordow για αυτό το άρθρο) δημιουργεί θύματα παντού, μολύνοντας smartphones, rootάροντας συσκευές χρηστών και στη συνέχεια, κλέβοντας ευαίσθητες πληροφορίες και ανεβάζοντάς τες στον server του malware συγγραφέα.

Τα σημάδια αυτής της malware οικογένειας εμφανίστηκαν τον Φεβρουάριο του 2016, όταν οι πρώτες μολύνσεις άρχισαν να ξεπροβάλλουν, κυρίως λόγω του ότι οι χρήστες έκαναν λήψη Android εφαρμογών από ανεπίσημα third-party app καταστήματα.

Ο Anton Kivva, malware αναλυτής της Kaspersky Lab λέει ότι οι περισσότερες από τις εφαρμογές που εξαπλώνουν το Tordow είναι κλώνοι πιο δημοφιλών Android εφαρμογών, όπως οι VKontakte, DrugVokrug, Pokemon Go, Telegram,

Odnoklassniki ή Subway Surf. Οι απατεώνες παίρνουν αυτές τις εφαρμογές, ξε-πακετάρουν (unpack) τον πηγαίο κώδικά τους, προσθέτουν τον δικό τους κακόβουλο κώδικα στο εσωτερικό, τις ξαναδημιουργούν (repack) και ανεβάζουν τους νέους τους κλώνους σε third-party app καταστήματα. Οι χρήστες που κατεβάζουν αυτές τις εφαρμογές ασυναίσθητα ενεργοποιούν τον κακόβουλο κώδικα μέσα σε αυτές όταν τις εκκινήσουν για πρώτη φορά.

Ο Kivva λέει ότι αυτός ο κώδικας είναι στην πραγματικότητα ένα είδος downloader που φέρνει κακόβουλο κώδικα στη συσκευή του χρήστη. Κάπου σε αυτόν τον κώδικα υπάρχει ένα πακέτο που περιέχει ένα exploit που βοηθά το κακόβουλο λογισμικό να αποκτήσει root προνόμια στην συσκευή. Μετά την απόκτηση root πρόσβασης, το Tordow έχει τον πλήρη έλεγχο πάνω στη συσκευή. Ο ερευνητής λέει ότι βρήκε κακόβουλες λειτουργίες στο εσωτερικό του πηγαίου κώδικα του trojan που οδηγούσαν σε διάφορες κακόβουλες ικανότητες, όπως η ικανότητα να κλέψει επαφές, να πραγματοποιήσει τηλεφωνικές κλήσεις και να στείλει, κλέψει και διαγράψει SMS μηνύματα.

Επιπλέον, το trojan μπορεί να κατεβάσει και να εκτελέσει αρχεία στη συσκευή, να εγκαταστήσει ή να αφαιρέσει εφαρμογές, να μπλοκάρει την πρόσβαση σε μια συγκεκριμένη ιστοσελίδα, να μετονομάσει τα αρχεία στη συσκευή, να φορτώσει τα αρχεία από τη συσκευή σε έναν online server και να κάνει επανεκκίνηση του smartphone.

Οι γνώστες λένε ότι ένα από τα τοπικά αρχεία που στοχεύει να κλέψει το Tordow είναι η βάση δεδομένων του Android stock browser και του Chrome για Android. Αυτή η βάση δεδομένων περιέχει το ιστορικό περιήγησης του χρήστη, αλλά και τους κωδικούς του. Άλλα αρχεία-στόχοι είναι και οι φωτογραφίες του χρήστη.

Ωστόσο, τίποτα από όλα αυτά δεν αποτελεί νέο, καθώς δεν είναι το πρώτο Android trojan που έρχεται εξοπλισμένο με δυνατότητες rooting, ούτε το πρώτο που μπορεί να κλέψει τις φωτογραφίες και το ιστορικό περιήγησης από τη συσκευή του χρήστη.

Για παράδειγμα, το Android.Loki trojan μπορεί, επίσης, να rootάρει συσκευές, ενώ το Marcher Android trojan μπορεί να κλέψει τα διαπιστευτήρια σύνδεσης από μια πληθώρα Android εφαρμογών. Άλλα Android trojans που μπορούν να rootάρουν συσκευές είναι τα Godless, Ztorg, Libskin, Matrix, Rootnik και Shuanet.

Πηγή: Secnews.gr