Η ESET ανακάλυψε το πρώτο botnet σε Android που ελέγχεται μέσω Twitter

Οι ερευνητές της ESET ανακάλυψαν ένα backdoor Trojan που επιτίθεται σε Android το οποίο ελέγχεται μέσω tweets. Ανιχνεύεται από την ESET ως Android/Twitoor, και είναι η πρώτη κακόβουλη εφαρμογή που χρησιμοποιεί το Twitter αντί του παραδοσιακού διακομιστή C&C (command-and-control).

Αφού ξεκινήσει, το Trojan κρύβει την παρουσία του στο σύστημα και ελέγχει τον καθορισμένο λογαριασμό Twitter σε τακτά χρονικά διαστήματα για εντολές. Με βάση τις λαμβανόμενες εντολές, μπορεί είτε να κατεβάσει κακόβουλες εφαρμογές ή να αλλάξει το C&C λογαριασμό Twitter σε ένα άλλο.

«Η χρήση του Twitter για τον έλεγχο ενός botnet είναι ένα καινοτόμο βήμα για την πλατφόρμα Android» επισημαίνει ο Lukáš Štefanko, ο ερευνητής malware της ESET που ανακάλυψε την κακόβουλη εφαρμογή.

Σύμφωνα με τον Štefanko, τα κανάλια επικοινωνίας που βασίζονται στα κοινωνικά δίκτυα είναι δύσκολο να εντοπιστούν και αδύνατον να εμποδιστουν πλήρως, ενώ ταυτόχρονα είναι εξαιρετικά εύκολο για τους απατεώνες να ανακατευθύνουν εκ νέου την επικοινωνία σε άλλο λογαριασμό.

Το Twitter χρησιμοποιήθηκε για πρώτη φορά για τον έλεγχο

botnets των Windows το 2009. *«Σχετικά με το χώρο των Android, αυτό το μέσο απόκρυψης είχε παραμείνει ανεκμετάλλευτο μέχρι τώρα. Στο μέλλον, όμως statuses, μπορούμε να αναμένουμε ότι οι «κακοί» θα προσπαθήσουν να κάνουν χρήση των Facebook status ή να εκμεταλλευτούν το LinkedIn και άλλα κοινωνικά δίκτυα»,* προβλέπει ο Štefanko.

Το Android / Twitoor είναι ενεργό από τον Ιούλιο του 2016. Δεν μπορεί να βρεθεί σε οποιοδήποτε επίσημο κατάστημα εφαρμογών Android – σύμφωνα με τον Štefanko– αλλά μάλλον εξαπλώνεται μέσω SMS ή μέσω κακόβουλων URL. Υποδύεται μια εφαρμογή porn player ή εφαρμογή MMS αλλά χωρίς την λειτουργικότητα. Αντ' αυτού, κατεβάζει διάφορες εκδόσεις κακόβουλου λογισμικού για mobile banking. Ωστόσο, αυτοί που διαχειρίζονται το botnet μπορούν να ξεκινήσουν τη διάδοση και άλλων κακόβουλων προγραμμάτων ανά πάσα στιγμή, συμπεριλαμβανομένου και ransomware, σύμφωνα με το Štefanko.

«Το Twitoor αποτελεί ένα άλλο παράδειγμα του ότι οι εγκληματίες του κυβερνοχώρου συνεχώς καινοτομούν. Οι χρήστες του Διαδικτύου θα πρέπει να διατηρούν ασφαλείς τις δραστηριότητές τους με καλές λύσεις ασφάλειας τόσο για υπολογιστές όσο και για φορητές συσκευές», καταλήγει ο Lukáš Štefanko.

Περισσότερες πληροφορίες στο σχετικό blogpost στο blog της ESET, WeLiveSecurity.