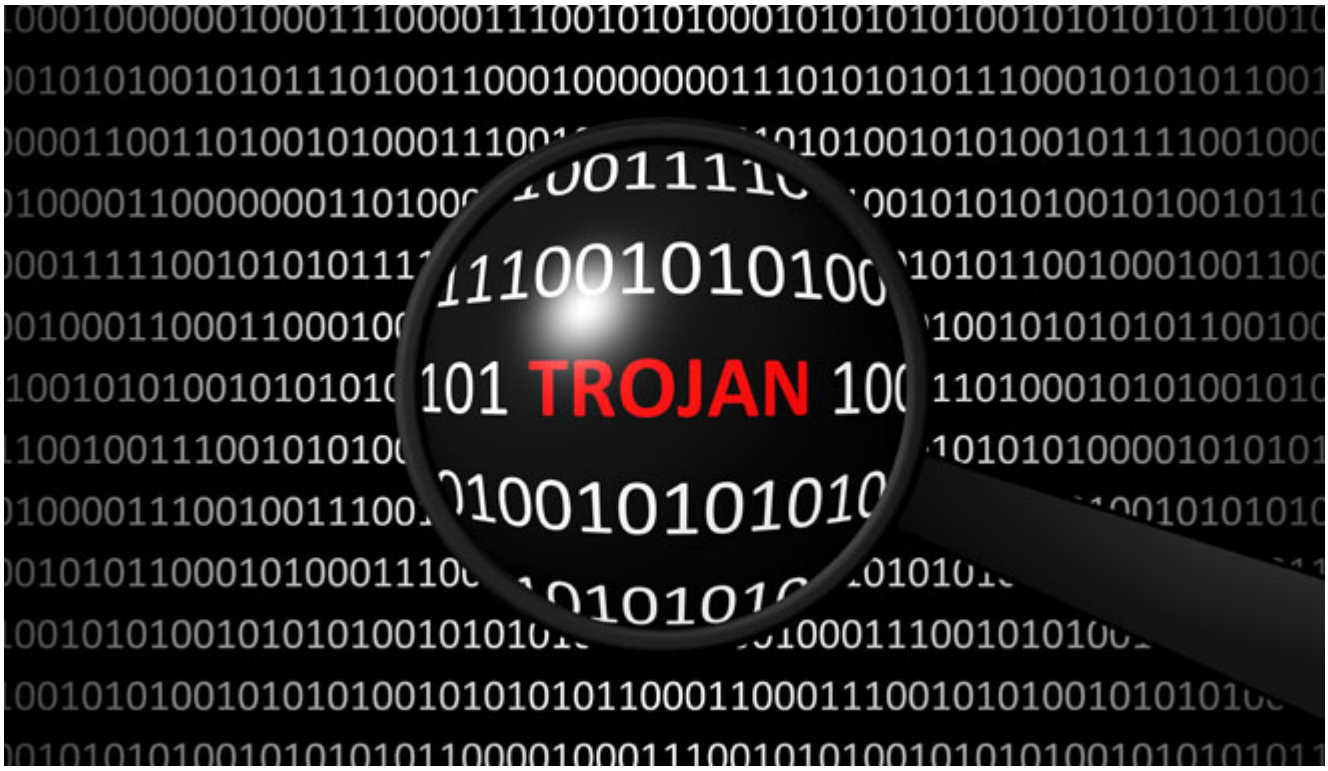
30 Μαρτίου 2017

Κορυφαία απειλή: Mobile διαφημιστικά Trojans

/ Πεμπτουσία

Image not found or type unknown



Τα Mobile Trojans ανακηρύχτηκαν νικητές την χρονιά που μας πέρασε. Το 2016, υπήρξε σχεδόν τριπλάσια άνοδος των ανιχνεύσεων mobile κακόβουλου λογισμικού σε σύγκριση με το 2015. Συγκεκριμένα, εντοπίστηκαν συνολικά 8,5 εκατομμύρια κακόβουλες εγκαταστάσεις. Αυτό σημαίνει ότι μέσα σε μόλις ένα χρόνο, απελευθερώθηκε ένας όγκος που αντιστοιχεί στο 50% όλων των κακόβουλων λογισμικών που εντοπίστηκαν τα προηγούμενα 11 έτη (15,77 εκατομμύρια την περίοδο 2004-2015).

Πρωτοστάτες ήταν τα mobile διαφημιστικά Trojans που αποτελούν σήμερα τα 16 εκ των 20 κορυφαίων κακόβουλων λογισμικών, σε σχέση με τα 12 το 2015. Αυτά είναι τα ευρήματα της ετήσιας έκθεσης της Kaspersky Lab με τίτλο «Mobile Virusology», στην οποία επισημαίνεται και η εξέλιξη των Trojans στον τομέα του mobile banking. Ειδικοί αξιωματούχοι του Interpol Global Complex for Innovation (IGCI) συνεισέφεραν στην έκθεση με με μία ανάλυση για το mobile κακόβουλο λογισμικό που υπάρχει στο Dark Web.

Το 2016, τα προϊόντα της Kaspersky Lab που παρέχουν ασφάλεια για mobile συσκευές ανέφεραν:

- Περίπου 40 εκατομμύρια προσπάθειες για επιθέσεις mobile κακόβουλου λογισμικού, με πάνω από 4 εκατομμύρια χρήστες Android να προστατεύονται (το αντίστοιχο νούμερο ήταν 2,6 εκατομμύρια το 2015)
- Πάνω από 260.000 ανιχνευμένα πακέτα εγκαταστάσεων mobile ransomware Trojans (μία αύξηση σχεδόν 8,5 φορές, από χρόνο σε χρόνο)
- Περισσότεροι από 153.000 μοναδικοί χρήστες στοχοποιήθηκαν από mobile ransomware (μία αύξηση 1,6 φορές μεγαλύτερη σε σύγκριση με το 2015)
- Πάνω από 128.000 mobile banking Trojans εντοπίστηκαν (περίπου 1,6 φορές περισσότερα από το 2015)

Διαφημιστικά Trojan: έχουν κάνει ήδη root τη συσκευή σας;

Οι πιο διαδεδομένοι τύποι Trojan το 2016 ήταν σε μορφή διαφημίσεων, αντιστοιχώντας στα 16 από τα 20 κορυφαία κακόβουλα λογισμικά. Αυτά τα Trojans είναι σε θέση να καταργήσουν βασικά δικαιώματα rooting, επιτρέποντας στα κακόβουλα λογισμικά όχι μόνο να προβάλουν με επιθετικό τρόπο διαφημίσεις στις «μολυσμένες» συσκευές, συχνά καθιστώντας αδύνατη τη χρήση τους, αλλά επίσης και να εγκαθιστούν κρυφά άλλες εφαρμογές. Αυτά τα Trojans ήταν επίσης σε θέση να αγοράσουν εφαρμογές στο Google Play.

Σε πολλές περιπτώσεις, τα Trojans ήταν σε θέση να εκμεταλλευτούν τα μέχρι πρότινος διορθωμένα τρωτά σημεία, επειδή οι χρήστες δεν είχαν εγκαταστήσει τις τελευταίες ενημερώσεις.

Περαιτέρω, το συγκεκριμένο κακόβουλο λογισμικό εγκαθιστά ταυτόχρονα τις προεκτάσεις του στο ευρετήριο του συστήματος, κάτι το οποίο καθιστά τη θεραπεία της «μολυσμένης» συσκευής αρκετά δύσκολη. Μερικά διαφημιστικά Trojans έχουν τη δυνατότητα να «μολύνουν» την εικόνα αποκατάστασης (recovery image), κάνοντας αδύνατη τη λύση του προβλήματος ακόμα και με επαναφορά στις εργοστασιακές ρυθμίσεις.

Παρακλάδια αυτής της κατηγορίας κακόβουλου λογισμικού έχουν βρεθεί επανειλημμένα στο επίσημο Google Play app store, όπως για παράδειγμα ένας μεταμφιεσμένος οδηγός για το Pokémon GO. Στην περίπτωση αυτή, η συγκεκριμένη εφαρμογή «κατέβηκε» περισσότερες από 500.000 φορές και αναγνωρίζεται με το όνομα Trojan.AndroidOS.Ztorg.ad.

Mobile ransomware προγράμματα: περαιτέρω αύξηση

Μέσα στο 2016, 153.258 μοναδικοί χρήστες από 167 χώρες δέχτηκαν επίθεση από Trojan–Ransom προγράμματα. Αυτός ο αριθμός είναι 1,6 φορές μεγαλύτερος συγκριτικά με το 2015.

Το μοντέρνο ransomware επικαλύπτει τα παράθυρα που λειτουργεί ο χρήστης με απαιτητικά μηνύματα, κάνοντας αδύνατη τη χρήση της συσκευής. Αυτό το στοιχείο χρησιμοποιήθηκε από το πιο γνωστό ransomware λογισμικό το 2016 – το Trojan-Ransom.AndroidOS.Fusob.

Το Trojan αυτό επιτίθεται κυρίως σε χρήστες στη Γερμανία, τις Ηνωμένες Πολιτείες και το Ηνωμένο Βασίλειο, αλλά αποφεύγει χρήστες στη Ρωσία και κάποιες γειτονικές της χώρες. Μόλις ξεκινήσει, τρέχει έναν έλεγχο στη γλώσσα της συσκευής και έπειτα, αφού ελέγξει τα αποτελέσματα, μπορεί να σταματήσει την εκτέλεση της διαδικασίας. Οι ψηφιακοί εγκληματίες που βρίσκονται πίσω από τα αυτά τα Trojan ζητούν από 100 έως 200 δολάρια για να ξεκλειδώσουν μια συσκευή. Η πληρωμή μπορεί να γίνει μόνο με τη χρήση προπληρωμένων iTunes καρτών. king Trojan: μία εκτινασσόμενη απειλή

Το 2016, πάνω από 305.000 χρήστες σε 164 χώρες δέχτηκαν επίθεση από mobile banking Trojans, σε σύγκριση με πάνω από 56.000 χρήστες σε 137 χώρες το προηγούμενο έτος.
Η Ρωσία, η Αυστραλία και η Ουκρανία είναι οι 3 πρώτες σε κατάταξη χώρες που δέχτηκαν επιθέσεις, με βάση το ποσοστό των χρηστών που δέχτηκαν επίθεση από mobile banking Trojans σε σχέση με τους χρήστες που έχουν πέσει θύματα mobilemalware συνολικά.
Τα mobile banking Trojans συνέχισαν να εξελίσσονται μέσα στο χρόνο. Πολλά από

αυτά απέκτησαν εργαλεία για να παρακάμψουν τους νέους Android μηχανισμούς ασφαλείας και ήταν σε θέση να συνεχίσουν να κλέβουν πληροφορίες χρηστών από τις πιο πρόσφατες εκδόσεις του λειτουργικού συστήματος. Την ίδια στιγμή, οι προγραμματιστές των mobile banking Trojans επανειλημμένα ενίσχυαν τα δημιουργήματά τους με νέες δυνατότητες. Για παράδειγμα, η «οικογένεια» Marcher, εκτός από τη συνήθη επικάλυψη τραπεζικών εφαρμογών, ανακατευθύνει συχνά τους χρήστες από τις ιστοσελίδες χρηματοπιστωτικών ιδρυμάτων σε ιστοσελίδες phishing. Η πλάνη Dark Web

Σύμφωνα με τους ειδικούς αξιωματούχους του Interpol Global Complex for Innovation (IGCI), οι οποίοι συνέβαλαν επίσης στην έκθεση, το Dark Web παραμένει ένα ελκυστικό μέσο για τη διεξαγωγή παράνομων επιχειρήσεων και δραστηριοτήτων. Δεδομένης της ισχυρής ανωνυμίας του, των χαμηλών τιμών και της πελατοκεντρικής στρατηγικής, το Dark Web παρέχει ένα μέσο για τους εγκληματικούς φορείς να επικοινωνούν και να συμμετάσχουν σε εμπορικές συναλλαγές, στην αγορά και την πώληση διαφόρων προϊόντων και υπηρεσιών, συμπεριλαμβανομένων των mobile malware. Το mobile κακόβουλο λογισμικό προσφέρεται για πώληση ως πακέτα λογισμικού (π.χ. απομακρυσμένης πρόσβασης Trojans – RATs), ατομικές λύσεις και εξελιγμένα εργαλεία, όπως αυτά αναπτύχθηκαν από επαγγελματίες ή, σε μικρότερη κλίμακα, ως μέρος ενός μοντέλου «Bot as a Service». Το mobile malware είναι επίσης «αντικείμενο ενδιαφέροντος» για καταστήματα προμηθευτών, φόρουμ και social media.

«Το 2016, συνεχίστηκε η αύξηση του αριθμού των διαφημιστικών Trojans που είναι σε θέση να εκμεταλλευτούν τα δικαιώματα super–user. Καθ ‘όλη τη διάρκεια του έτους, ήταν η κορυφαία απειλή και δε βλέπουμε κανένα σημάδι αλλαγής της τάσης αυτής. Οι ψηφιακοί εγκληματίες εκμεταλλεύονται το γεγονός ότι οι περισσότερες συσκευές δε λαμβάνουν ενημερώσεις λειτουργικού συστήματος (ή τις λαμβάνουν όταν είναι ήδη αργά), και ως εκ τούτου είναι ευάλωτες σε παλιά, γνωστά και άμεσα διαθέσιμα expoits. Επιπλέον, βλέπουμε ότι το mobile τοπίο γίνεται «αποπνικτικό» για τους ψηφιακούς εγκληματίες και αρχίζουν να αλληλεπιδρούν περισσότερο με τον κόσμο πέρα από τα smartphones. Ίσως το 2017 θα δούμε μεγάλες επιθέσεις σε IoT συστατικά, οι οποίες θα ξεκινήσουν από φορητές συσκευές», καταλήγει ο Roman Unuchek, Senior Malware Analyst της Kaspersky Lab ΗΠΑ.

Πηγή: Secnews.gr