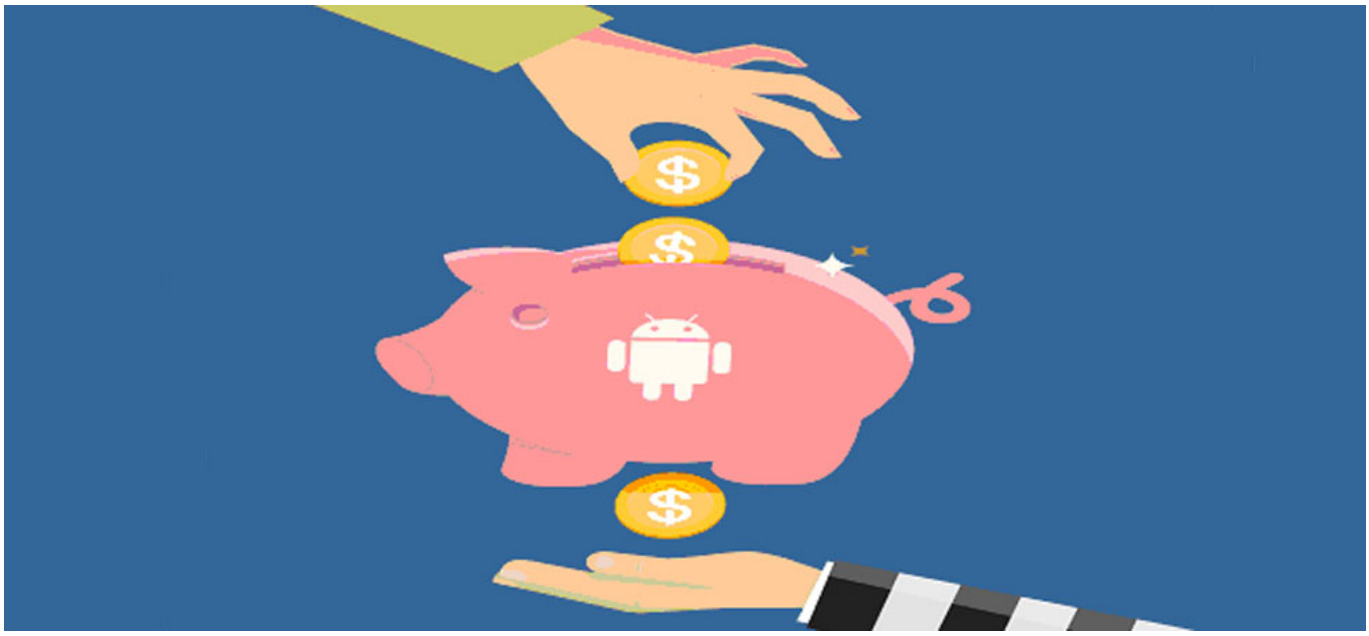
12 Οκτωβρίου 2015

Τεράστια απειλή για smartphones τα τραπεζικά trojans:

/ Πεμπτουσία

Image not found or type unknown



Τα σημερινά smartphones είναι ολοκληρωμένοι υπολογιστές, αλλά σε αντίθεση με τα οικιακά PC και τα laptops είναι συνήθως «ανοχύρωτα». Καθώς λοιπόν ο αριθμός του κινητού τηλεφώνου είναι πολύ συχνά συνδεδεμένος με κάποια πιστωτική κάρτα, μπορούμε να πούμε ότι τα τραπεζικά Trojans είναι οι πιο σημαντικές απειλές για κινητά μιας και αποτελούν πάνω από το 95% των malware σε κινητά.

Βρισκόμαστε σε μια εποχή όπου η πλειοψηφία των χρηστών smartphone εξακολουθούν να θεωρούν τη συσκευή τους «απλά ένα τηλέφωνο,» σε αντίθεση με τους χρήστες PC που ήδη χρησιμοποιούν τουλάχιστον μια βασική «υγιεινή ασφάλειας» απέναντι στα Trojans.
Σήμερα τα smartphones είναι ολοκληρωμένοι υπολογιστές. Και πιο συγκεκριμένα είναι επικίνδυνοι υπολογιστές. Εκεί που ο σκληρός δίσκος του υπολογιστή σας μπορεί να μην περιέχει τίποτα αξίας, το smartphone σας είναι πολύ πιθανό να περιέχει δεδομένα, τα οποία είναι πολύτιμα τόσο για εσάς όσο και τους κυβερνο-εγκληματίες.

Αν έχετε smartphone, είναι πολύ πιθανό έχετε και τραπεζική κάρτα. Δεδομένου ότι οι τράπεζες χρησιμοποιούν τον αριθμό κινητού τηλεφώνου σας για επιβεβαίωση των στοιχείων σας (στέλνουν one-time passwords μέσω SMS), είναι πιθανό εγκληματίες του κυβερνοχώρου να έχουν προσπαθήσει να διεισδύσουν σε αυτόν το δίαυλο επικοινωνίας και να εκτελέσουν πληρωμές και μεταφορές από τον τραπεζικό σας λογαριασμό. Γι' αυτόν και μόνο τον λόγο, μπορούμε να πούμε με σιγουριά ότι τα τραπεζικά Trojans είναι οι πιο σημαντικές απειλές για κινητά μιας και αποτελούν πάνω από το 95% των malware σε κινητά.

Αν και τα Trojans είναι λιγότερο επικίνδυνα από ιούς, δεδομένου ότι απαιτούν ενέργειες του χρήστη να διεισδύσουν στα συστήματα, υπάρχει μια σειρά αποτελεσματικών social engineering τεχνικών, που παρασύρουν τον χρήστη στην ενεργοποίησή τους μέσα από ψεύτικες ενημερώσεις.

Υπάρχουν τρεις κύριες μέθοδοι τραπεζικών Trojans που απασχολούν:
• **Η απόκρυψη του κειμένου**: Malware κινητών κρύβει τα εισερχόμενα SMS από τις τράπεζες και στη συνέχεια τα στέλνει στους εγκληματίες οι οποίοι στη συνέχεια μεταφέρουν χρήματα στους λογαριασμούς τους.
• **Μικρή διακίνηση μετρητών**: Malware actoers μεταφέρουν περιστασιακά μικρά ποσά χρημάτων σε λογαριασμούς-απάτες από το λογαριασμό ενός μολυσμένου χρήστη.
• **App Mirroring**: Malware κινητές εφαρμογές που μιμούνται τράπεζες και παίρνουν τα διαπιστευτήρια σύνδεσης του χρήστη από την πραγματική εφαρμογή

Τα μεγάλα τραπεζικά Trojans (πάνω από 50%) στοχεύουν τη Ρωσία και τις CIS countries, καθώς και την Ινδία και το Βιετνάμ. Τον τελευταίο καιρό, η νέα γενιά των καθολικών malware κινητών βρίσκεται σε άνοδο.

Ο παππούς όλων των τραπεζικών Trojans κινητού είναι ο Δίας (Zeus), γνωστός και ως Zitmo (Zeus-in-the-mobile), που δημιουργήθηκε από το 2010 (διάδοχος του Zeus για υπολογιστές του 2006). Αυτό το κομμάτι του κακόβουλου λογισμικού κατάφερε να μολύνει πάνω από 3.5 εκατομμύρια συσκευές στις ΗΠΑ και μόνο και να δημιουργήσει το μεγαλύτερο botnet της ιστορίας.
Χάρη στον Δία, οι απατεώνες κατάφεραν να ξεφύγουν με πάνω από 74.000 κωδικούς πρόσβασης FTP από διάφορες ιστοσελίδες (συμπεριλαμβανομένης της Bank of America), αλλάζοντας τον κωδικό τους, ώστε θα ήταν δυνατή η εξαγωγή δεδομένων πιστωτικών καρτών μετά από κάθε προσπάθεια πληρωμής. Ο Δίας ήταν πολύ δραστήριος μέχρι τα τέλη του 2013, όταν εκθρονίστηκε από το πιο εκσυγχρονισμένο Xtreme RAT.

Με το πέρασμα των καιρών είδαμε τραπεζικά Trojans να κάνουν την εμφάνισή τους. Το 2011 είδαμε το SpyEye που ήταν ένα από τα πιο επιτυχημένα τραπεζικά Trojans στην ιστορία. Το 2012 ένα άλλο είδος Trojan βρέθηκε – το Carberp. Αυτό το στοιχείο μιμήθηκε Android εφαρμογές των μεγάλων ρωσικών τραπεζών, των Sberbank και Alfa Bank, καθώς στόχευε τους χρήστες τους στη Ρωσία, Λευκορωσία, Καζακστάν, Μολδαβία και Ουκρανία. Περιέργως, οι δράστες ήταν σε θέση να δημοσιεύσουν ψεύτικες εφαρμογές στο Google Play.

Περνώντας στα πιο πρόσφατα περιστατικά έρχεται το 2013 το Hesperbot που αρχίζει να αναζητά τα δικά του θύματα. Επρόκειτο για ένα κακόβουλο λογισμικό προερχόμενο από την Τουρκία και εκτός από τα συνήθη προβλήματα, αυτό το Trojan δημιουργεί ένα κρυμμένο διακομιστή VNC σε ένα smartphone, ο οποίος παρείχε την πρόσβαση σε έναν εισβολέα για μια απομακρυσμένη διαχείριση της συσκευής. Επιπλέον, το Hesperbot ενήργησε όχι μόνο ως ένα τραπεζικό Trojan, αλλά και ως κλέφτης Bitcoin.

Αντίστοιχα, το 2014 αποκαλύφθηκε ο πηγαίος κώδικας του Android.iBanking. Το iBanking είναι ένα end-to-end kit για SMS hi-jacking και απομακρυσμένη διαχείριση συσκευής. Η δημοσίευση του κώδικα οδήγησε σε μια αύξηση των μολύνσεων.

Τον Ιούνιο του 2015, ένα νέο Trojan ανακαλύφθηκε στη Ρωσία. Το Android.Bankbot.65.Origin ήταν μεταμφιεσμένο ως διορθωμένη επίσημη εφαρμογή της Sberbank Online και πρόσφερε ένα «ευρύτερο φάσμα των χαρακτηριστικών m-banking», διαθέσιμων μετά την εγκατάσταση της «νεότερης έκδοσης».

Στην πραγματικότητα, η εφαρμογή παρέμεινε πράγματι ένα λειτουργικό m-banking εργαλείο, έτσι κανένας χρήστης δεν πρόσεξε την αλλαγή. Κατά συνέπεια, τον Ιούλιο 100.000 χρήστες της Sberbank ανακοίνωσαν ζημίες ύψους πάνω από 2 δισεκατομμύρια ρούβλια. Όλοι αυτοί χρησιμοποίησαν την ψεύτικη εφαρμογή “Sberbank Online”.

Είναι αυτονόητο ότι η ιστορία των τραπεζικών Trojans γράφεται ακόμα: όλο και περισσότερες νέες εφαρμογές δημιουργούνται και όλο και πιο αποδοτικές τεχνικές χρησιμοποιούν οι επιτιθέμενοι για να παρασύρουν τους χρήστες στην παγίδα τους. Έτσι, είναι καιρός να προστατεύσετε το smartphone σας σωστά!

Πηγή: secnews.gr