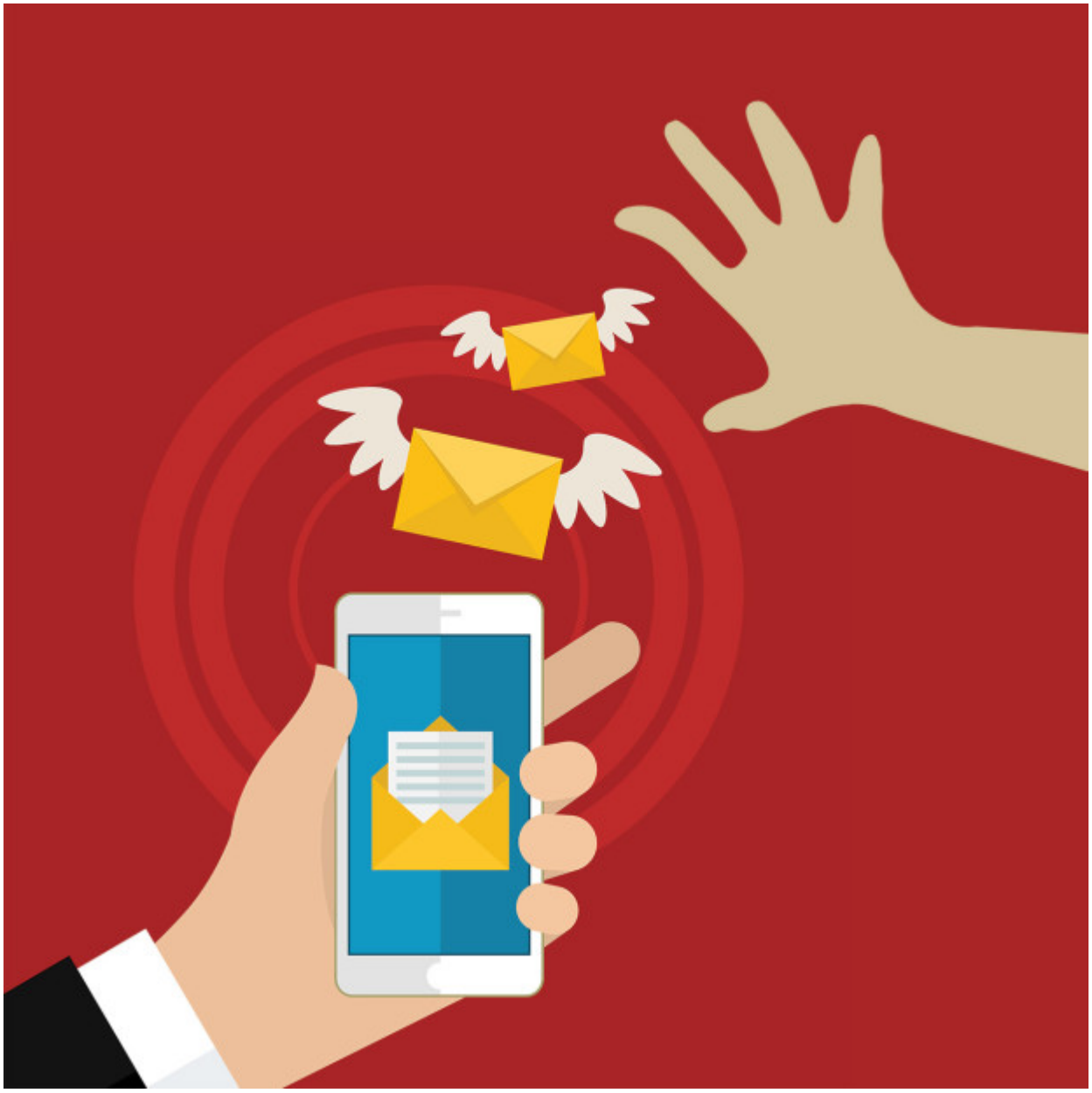
17 Μαΐου 2016

Πώς τα banking trojans παρακάμπτουν το two-factor authentication

/ Επιστήμες, Τέχνες & Πολιτισμός

Image not found or type unknown



Το two-factor authentication με SMS χρησιμοποιείται ευρέως από τα τραπεζικά ιδρύματα. Φυσικά, το μέτρο αυτό λειτουργεί καλύτερα από ό,τι ένας απλός κωδικός πρόσβασης, αλλά δεν είναι αδιαπέραστο. Ειδικοί ασφαλείας ανακάλυψαν πώς μπορούσε να ξεγελαστεί από τα λεγόμενα banking trojans πριν από 10 χρόνια, όταν αυτό το μέτρο προστασίας απλά κέρδιζε δημοτικότητα.

Όμως, την ίδια δημοτικότητα έπαιρναν παράλληλα και οι malware δημιουργοί. Επομένως, αυτός είναι και ο λόγος που οι banking Trojan προγραμματιστές παραβιάζουν τους one-time SMS passwords με τόση ευκολία. Εδώ είναι το πώς αυτό λειτουργεί:

1. Ένας χρήστης εκκινεί ένα νόμιμο τραπεζικό app σε ένα smartphone.
2. Ένα Trojan ανιχνεύει, ποια εφαρμογή χρησιμοποιείται και επικαλύπτει tointerface της με ένα ψεύτικο αντίγραφο. Η ψεύτικη οθόνη φαίνεται ακριβώς

όπως η πραγματική.
3. Το θύμα εισέρχεται με το όνομα χρήστη και τον κωδικό πρόσβασης στο ψεύτικο app.
4. Το Trojan στέλνει διαπιστευτήρια χρήστη στους εγκληματίες. Χρησιμοποιούν αυτά τα στοιχεία για να συνδεθούν στο τραπεζικό app του χρήστη.
5. Στη συνέχεια, οι ένοχοι ζητούν μια οικονομική συναλλαγή στο λογαριασμό τους.
6. Το τηλέφωνο του θύματος λαμβάνει ένα SMS με τον κωδικό μιας χρήσης.
7. Το Trojan εξάγει τον κωδικό πρόσβασης από το SMS και το στέλνει στουςcybercriminals.
8. Επίσης, κρύβει το SMS από το χρήστη. Αυτός είναι ο λόγος που το θύμα δεν γνωρίζει σχετικά με τις διεξαγόμενες εργασίες μέχρι να ελέγξει τον τραπεζικό λογαριασμό και το ιστορικό των συναλλαγών του.
9. Οι εγκληματίες χρησιμοποιούν τον κωδικό πρόσβασης που υπέκλεψαν για την επιβεβαίωση της συναλλαγής και να λαμβάνουν τα χρήματα του θύματος.

Δύσκολα θα το έλεγε κανείς υπερβολή αν σημειώσουμε ότι κάθε σύγχρονο banking Trojan ξέρει πώς να ξεγελάσει τα συστήματα ελέγχου ταυτότητας δύο παραγόντων μέσω SMS. Στην πραγματικότητα οι δημιουργοί malware δεν έχουν καμία άλλη επιλογή: καθώς όλες οι τράπεζες στρέφονται σε αυτό το μέτρο προστασίας, τα Trojans πρέπει με τη σειρά τους να προσαρμοστούν.

Υπάρχουν πολλές κακόβουλες εφαρμογές που είναι σε θέση να το κάνουν, περισσότερες από ό,τι μπορείτε να φανταστείτε. Κατά τη διάρκεια των τελευταίων δύο μηνών, ειδικοί δημοσίευσαν τρεις λεπτομερείς εκθέσεις αφιερωμένες σε τρεις διαφορετικές οικογένειες malware. Κάθε μία πιο τρομακτική ότι την άλλη:

1. ***Asacub***– ένα κατασκοπικό app που εξελίχθηκε σε Trojan και έμαθε να κλέβει χρήματα από εφαρμογές κινητού για τράπεζες.
2. ***Acecard***– ένα πολύ ισχυρό Trojan που είναι σε θέση να επικαλύψει τα interfaces των σχεδόν 30 διαφορετικών τραπεζικών εφαρμογών. Με τον τρόπο που τα mobile malware τώρα γίνονται ειδικοί πάνω σε αυτή την τάση: στην αρχή τα Trojans στόχευαν μια εφαρμογή μιας συγκεκριμένης τράπεζας ή υπηρεσίας πληρωμών, αλλά τώρα μπορούν να πλαστογραφήσουν πολλές εφαρμογές ταυτόχρονα.
3. ***Banloader***– ένα cross-platform Trojan από τη Βραζιλία, που έχει τη δυνατότητα να ξεκινήσει από μόνο του σε υπολογιστές και φορητές συσκευές ταυτόχρονα.

Έτσι, μπορείτε να καταλάβετε, ότι ο έλεγχος ταυτότητας δύο παραγόντων δεν

μπορεί να σας προστατεύσει από τα banking Trojans. Απέτυχε να το κάνει αυτό για πολλά χρόνια και τώρα η κατάσταση δεν πρόκειται να καλυτερεύσει. Γι’ αυτό θα πρέπει να έχετε πρόσθετα μέτρα ασφαλείας.

Ο βασικός κανόνας που βοηθά, αλλά όχι στο 100%, είναι να εγκαθιστάτε εφαρμογές μόνο από επίσημα καταστήματα. Το θέμα είναι ότι υπήρχαν αρκετές περιπτώσεις, όπως όταν τα Trojans κατάφεραν να μπουν στο Play Store ή ακόμα και στο App Store. Και ίσως θα ήταν καλό να σκεφτείτε και μια πιο αξιόπιστη λύση εγκαθιστώντας ένα καλό antivirus για κινητά!

Πηγή: secnews.gr