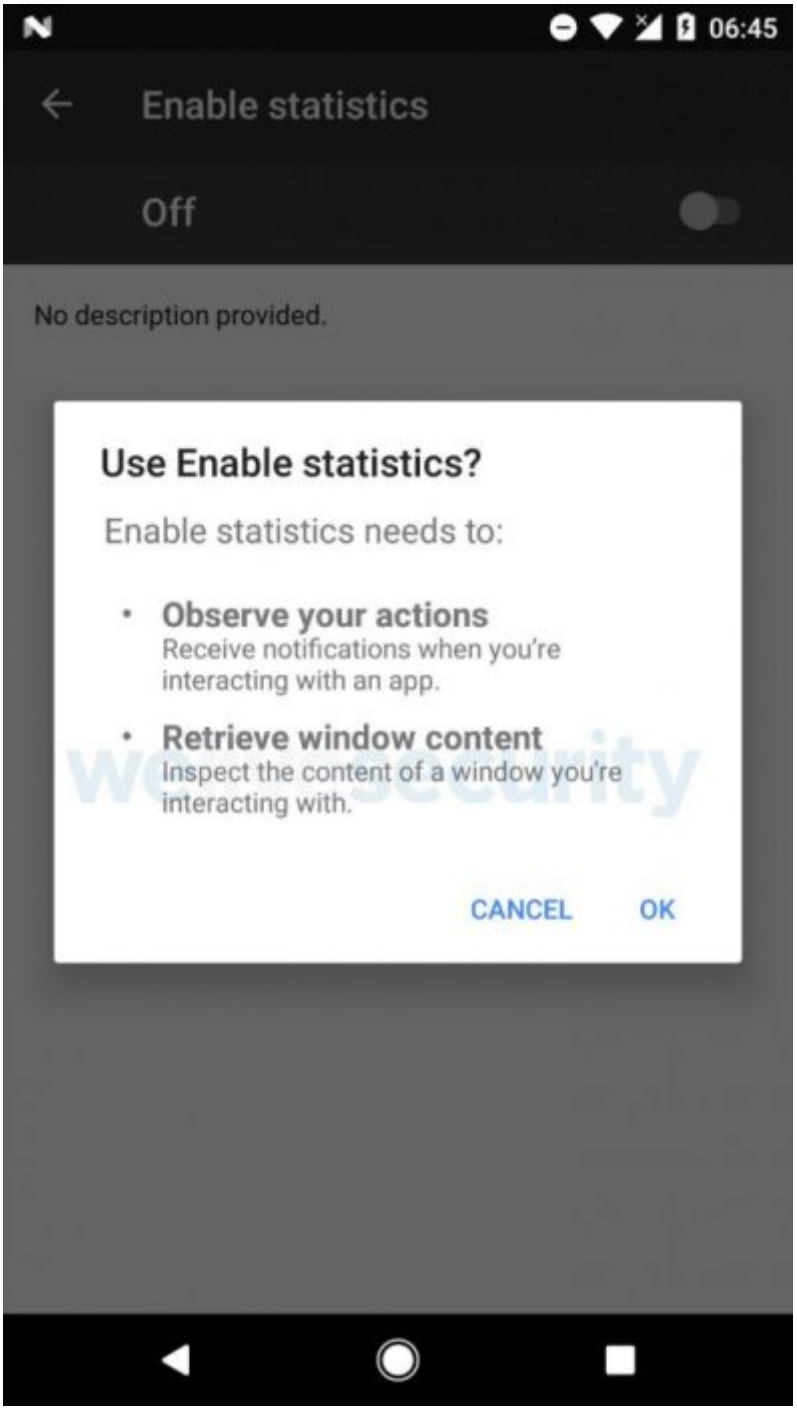
15 Δεκεμβρίου 2018

Νέο Android malware κλέβει χρήματα από την εφαρμογή PayPal, προσοχή!

/ Επιστήμες, Τέχνες & Πολιτισμός

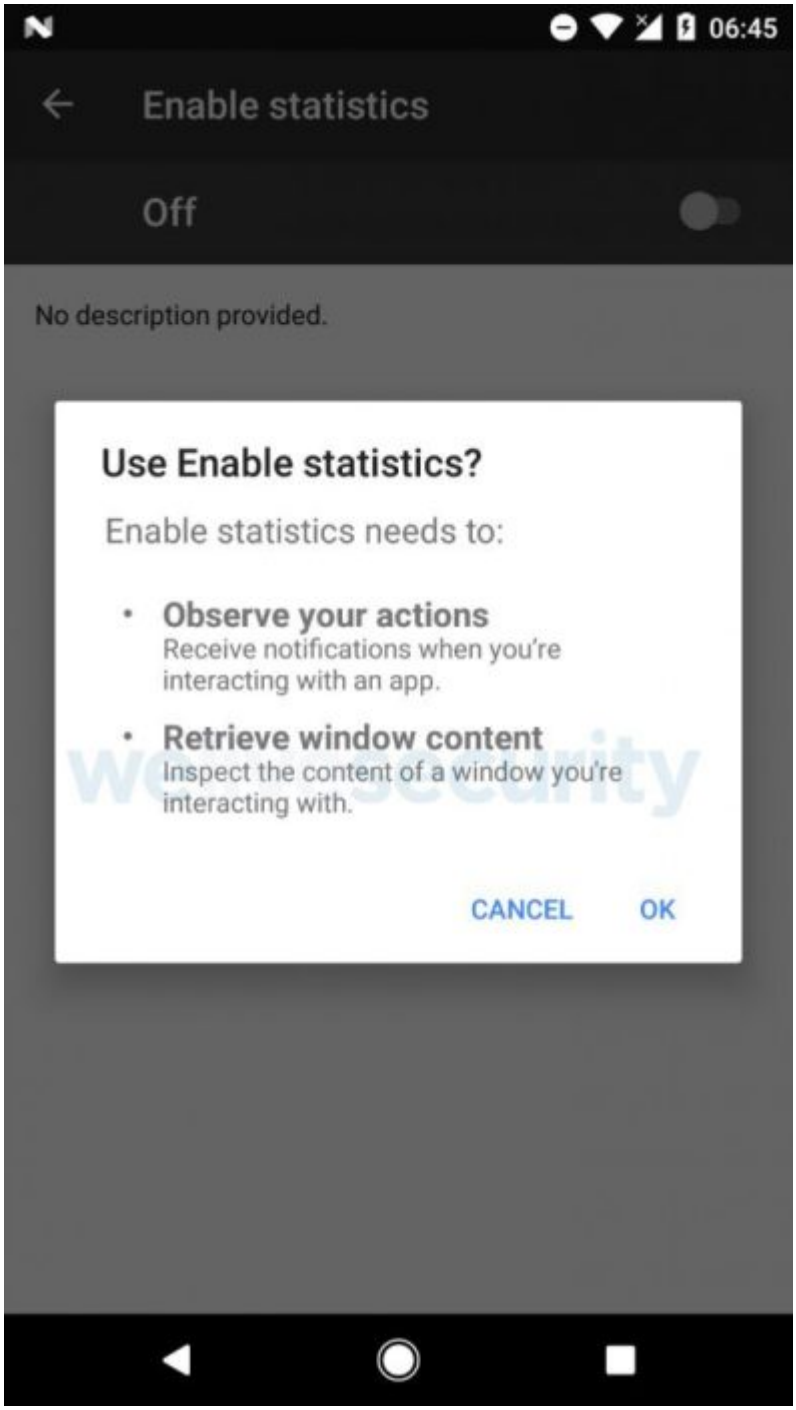


Μια νέα έκθεση από τους ερευνητές ασφάλειας της ESET παρουσίασε ένα νέο trojan που επηρεάζει τους χρήστες Android και όσους έχουν εγκατεστημένη την εφαρμογή PayPal. Το trojan αρχικά ανιχνεύτηκε από την ESET τον Νοέμβριο του

2018, καθώς συνδυάζει τις δυνατότητες ενός απομακρυσμένα ελεγχόμενου τραπεζικού Trojan με την κακή χρήση των υπηρεσιών προσβασιμότητας Android, για να στοχεύσει τους χρήστες της επίσημης εφαρμογής PayPal.

Μόλις εγκατασταθεί, η κακόβουλη εφαρμογή τερματίζεται χωρίς να δείχνει ότι λειτουργεί και κρύβει το εικονίδιο της. Η πρώτη λειτουργία του κακόβουλου λογισμικού είναι η κλοπή χρημάτων από τα θύματά του – τους κατόχους λογαριασμών PayPal. Ωστόσο, απαιτεί την ενεργοποίηση μιας κακόβουλης υπηρεσίας προσβασιμότητας. Το αίτημα αυτό παρουσιάζεται στο χρήστη ως υπηρεσία με όνομα «Enable Statistics», χωρίς περιγραφή από κάτω που δεν προϊδεάζει για την επικινδυνότητα του.

*Σημείωση: Δεν το έχουμε δει στα ελληνικά, αλλά αν το έχουν προβλέψει προφανώς θα γράφει «Ενεργοποίηση στατιστικών».



Εάν η επίσημη εφαρμογή PayPal είναι εγκατεστημένη στη προσβεβλημένη συσκευή, το κακόβουλο πρόγραμμα ειδοποιεί τον χρήστη να την εκκινήσει. Μόλις ο χρήστης ανοίξει την εφαρμογή PayPal και συνδεθεί, η κακόβουλη υπηρεσία καθίσταται ενεργή και μιμείται τα κλικ του χρήστη για να στείλει χρήματα στη διεύθυνση PayPal του εισβολέα. Η όλη διαδικασία διαρκεί περίπου 5 δευτερόλεπτα, και για έναν ανυποψίαστο χρήστη, δεν υπάρχει αρκετός χρόνος για να παρέμβει έγκαιρα.

Σημειώστε οτι το κακόβουλο λογισμικό δεν βασίζεται στην κλοπή των διαπιστευτηρίων σύνδεσης (username και κωδικός πρόσβασης) του PayPal, αντίθετα περιμένει τους χρήστες να συνδεθούν στην επίσημη εφαρμογή

PayPal,παρακάμπτοντας ταυτόχρονα τον έλεγχο ταυτότητας δύο παραγόντων του PayPal (2FA). Οι επιτιθέμενοι αποτυγχάνουν μόνο εάν ο χρήστης έχει ανεπαρκές υπόλοιπο στο PayPal και δεν έχει συνδέσει με το λογαριασμό του την κάποια κάρτα πληρωμών. Η κακόβουλη υπηρεσία ενεργοποιείται κάθε φορά που ανοίγει η εφαρμογή PayPal, που σημαίνει ότι η επίθεση μπορεί να πραγματοποιηθεί πολλές φορές.

Η δεύτερη λειτουργία του κακόβουλου λογισμικού αξιοποιεί τις οθόνες «ηλεκτρονικού ψαρέματος» (phising) που εμφανίζονται κρυφά σε συγκεκριμένες, νόμιμες εφαρμογές. Από προεπιλογή, οι κακόβουλες εφαρμογές προβάλλουν οθόνες επικάλυψης βασισμένες σε HTML για πέντε εφαρμογές (Google Play, WhatsApp, Skype, Viber και Gmail), αλλά αυτή η αρχική λίστα μπορεί και ενημερώνεται δυναμικά ανά πάσα στιγμή. Σε αντίθεση με τις επικαλύψεις (overlays) που χρησιμοποιούνται από malware κλοπής τραπεζικών λογαριασμών σε Android, αυτές εμφανίζονται στην οθόνη κλειδώματος προσκηνίου.

Αυτό εμποδίζει τα θύματα να σβήσουν το κουμπί αγγίζοντας το «Back» ή το κουμπί «Home». Ο κώδικας του malware περιέχει εκφράσεις που υποστηρίζουν ότι το τηλέφωνο του θύματος έχει κλειδωθεί και μπορεί να ξεκλειδωθεί στέλνοντας ένα μήνυμα ηλεκτρονικού ταχυδρομείου σε μια συγκεκριμένη διεύθυνση. Επιπλέον, το κακόβουλο λογισμικό μπορεί επίσης να παρακολουθεί και να στέλνει μηνύματα SMS, να διαγράφει SMS, να αλλάξει την προεπιλεγμένη εφαρμογή SMS, να

αποκτήσει λίστα επαφών, να πραγματοποιήσει και να προωθήσει κλήσεις, να αποκτήσει τη λίστα με τις εγκατεστημένες εφαρμογές, να εγκαταστήσει εφαρμογές, να εκτελέσει συγκεκριμένες εφαρμογές.

Είναι ενδιαφέρον ότι αυτά τα Trojans χρησιμοποιούν επίσης την Προσβασιμότητα Android για να αποτρέψουν τις προσπάθειες κατάργησης εγκατάστασης (Uninstall) της κακόβουλης εφαρμογής.

Πηγή: **gr.gizchina.com**