7 Ιουνίου 2022

Κακόβουλο λογισμικό στα Android κλέβει κωδικούς πρόσβασης -Πώς λειτουργεί

/ Επιστήμες, Τέχνες & Πολιτισμός



Κακόβουλο λογισμικό Android που κλέβει κωδικούς πρόσβασης θέτει σε κίνδυνο δισεκατομμύρια χρήστες / Φωτογραφία: Shutterstock

Ένα νέο επικίνδυνο κακόβουλο λογισμικό που στοχεύει συσκευές Android αποκαλύφθηκε από ειδικούς σε θέματα κυβερνοασφάλειας.



Κακόβουλο λογισμικό Android που κλέβει κωδικούς πρόσβασης θέτει σε κίνδυνο δισεκατομμύρια χρήστες / Φωτογραφία: Shutterstock

Το 2021, οι ερευνητές ανακάλυψαν ένα κακόβουλο λογισμικό με την ονομασία ERMAC που επιτίθεται σε συσκευές Android.

Τώρα, οι ειδικοί κυβερνοασφάλειας της εταιρείας ESET διαπίστωσαν ότι μια νέα έκδοση του τραπεζικού trojan – με την ονομασία ERMAC 2.0 – είναι ενεργή.

Το κακόβουλο λογισμικό στοχεύει συσκευές Android μέσω 467 εφαρμογών που κλέβουν τα διαπιστευτήρια των χρηστών και τις τραπεζικές πληροφορίες.

Το ERMAC 2.0 το κάνει αυτό υποδυόμενο δημοφιλείς και γνήσιες εφαρμογές, σύμφωνα με τους ειδικούς σε θέματα κυβερνοασφάλειας.

Η Cyble Research Labs διαπίστωσε επίσης ότι οι απειλητικοί φορείς μπορούν να νοικιάσουν το κακόβουλο λογισμικό έναντι μιας βαριάς μηνιαίας αμοιβής ύψους 5.000 δολαρίων.

Το ERMAC 1.0, το οποίο ανακαλύφθηκε επίσημα τον Αύγουστο του 2021, χρησιμοποιούσε 378 εφαρμογές και ενοικιαζόταν για 3.000 δολάρια το μήνα.

«Παρατηρήσαμε ότι το ERMAC 2.0 παραδίδεται μέσω ψεύτικων ιστότοπων», σημειώνει η Cyble Labs σε ανάρτηση στο blog της.

Οι ειδικοί πρόσθεσαν ότι το EMRAC 2.0 εξαπλώνεται επίσης μέσω ψεύτικων τοποθεσιών ενημέρωσης του προγράμματος περιήγησης.

Πώς λειτουργεί το κακόβουλο λογισμικό που κλέβει κωδικούς στα Android

Μόλις κάποιος εγκαταστήσει το ERMAC 2.0 μέσω μιας απατηλής εφαρμογής, το κακόβουλο λογισμικό ζητάει έως και 43 άδειες από τη συσκευή του.

Αυτές οι άδειες, αν χορηγηθούν, μπορεί να επιτρέψουν στους κακούς παράγοντες να πάρουν τον πλήρη έλεγχο της συσκευής του θύματος.

Μπορούν επίσης, να δώσουν στους χάκερ πρόσβαση σε SMS, πρόσβαση σε επαφές, δημιουργία παραθύρου ειδοποίησης συστήματος, ηχογράφηση ή πλήρη πρόσβαση ανάγνωσης και εγγραφής στον αποθηκευτικό χώρο.

Ακόμα, μπορούν να δημιουργήσουν μια λίστα με τις εφαρμογές που είναι εγκατεστημένες στη συσκευή του θύματος και να μοιραστούν αυτά τα δεδομένα με τον διακομιστή C2 του χάκερ, σύμφωνα με το Tech Radar.

Αυτό μπορεί να οδηγήσει σε ένα σύνθετο σχέδιο ηλεκτρονικού ψαρέματος που συλλέγει τα δεδομένα του χρήστη κάθε φορά που προσπαθεί να συνδεθεί στην προσβεβλημένη εφαρμογή.

Ορισμένες σελίδες ηλεκτρονικού ψαρέματος (phishing) που χρησιμοποιούνται για την εξαπάτηση των θυμάτων, περιλαμβάνουν τραπεζικές εφαρμογές όπως η bitbank της Ιαπωνίας, η IDBI Bank της Ινδίας, η Greater Bank της Αυστραλίας και η Santander Bank με έδρα τη Βοστώνη, σύμφωνα με το Phone Arena.

Πώς να προστατευτείτε
Διάφοροι περιορισμοί που τίθενται μέσω της Υπηρεσίας Προσβασιμότητας προστατεύουν τις συσκευές με Android 11 και 12, σύμφωνα με το BleepingComputer.

Ωστόσο, συνιστάται στους χρήστες να αποφεύγουν τη λήψη εφαρμογών εκτός του Play Store της Google.

Ακόμη και αν μια εφαρμογή βρίσκεται στο Play Store της Google, οι χρήστες θα πρέπει να βρίσκονται σε εγρήγορση σχετικά με τη νομιμότητά της.

Πηγή: iefimerida.gr