Dvmap: Κακόβουλο λογισμικό για συσκευές Android με μια νέα τεχνική για τον έλεγχο συσκευών εμφανίστηκε στο Google Play

Οι ειδικοί της Kaspersky Lab έχουν ανακαλύψει ένα ασυνήθιστο νέο Trojan που διανέμεται μέσω του Google Play Store. Το Trojan Dvmap είναι σε θέση όχι μόνο να αποκτά δικαιώματα πλήρους πρόσβασης (root access) σε Android smartphones, αλλά μπορεί επίσης να πάρει τον έλεγχο της συσκευής εισάγοντας κακόβουλο κώδικα στη βιβλιοθήκη του συστήματος. Εάν είναι επιτυχής, μπορεί στη συνέχεια να διαγράψει την πλήρη πρόσβαση, πράγμα που βοηθά στην αποφυγή της ανίχνευσής του. Το Trojan έχει «κατέβει» από το Google Play περισσότερες από 50.000 φορές από τον Μάρτιο του 2017. Η Kaspersky Lab ανέφερε το Trojan στην Google και έχει αφαιρεθεί πλέον από το κατάστημα.

Η απόκτηση της δυνατότητας έγχυσης κώδικα είναι μια επικίνδυνη νέα εξέλιξη στο κακόβουλο λογισμικό για φορητές συσκευές. Δεδομένου ότι η προσέγγιση μπορεί να χρησιμοποιηθεί για την εκτέλεση κακόβουλων λειτουργιών, ακόμη και με τη διαγραφή της πλήρους πρόσβασης, οποιεσδήποτε λύσεις ασφάλειας και εφαρμογές τραπεζών με δυνατότητες πλήρους ανίχνευσης που έχουν εγκατασταθεί μετά τη «μόλυνση» δεν θα εντοπίσουν την παρουσία του κακόβουλου λογισμικού.

Ωστόσο, η τροποποίηση των βιβλιοθηκών του συστήματος είναι μια επικίνδυνη διαδικασία που μπορεί να αποτύχει. Οι ερευνητές παρατήρησαν ότι το κακόβουλο λογισμικό Dvmap παρακολουθεί και

αναφέρει κάθε κίνηση του στον command and control server – παρόλο που ο command server δεν ανταποκρίθηκε με οδηγίες. Αυτό υποδηλώνει ότι το κακόβουλο λογισμικό δεν είναι ακόμη πλήρως έτοιμο ή εφαρμοσμένο.

Το Dvmap διανέμεται ως παιχνίδι μέσω του Google Play Store. Για να παρακάμψουν τους ελέγχους ασφαλείας του καταστήματος, οι δημιουργοί του κακόβουλου λογισμικού «ανέβασαν» μια «καθαρή» εφαρμογή στο κατάστημα στα τέλη Μαρτίου του 2017. Στη συνέχεια, την ενημέρωσαν με μια κακόβουλη έκδοση για σύντομο χρονικό διάστημα, προτού «ανεβάσουν» μια άλλη καθαρή έκδοση. Σε διάστημα τεσσάρων εβδομάδων πραγματοποίησαν τη διαδικασία αυτή τουλάχιστον πέντε φορές.

Το Trojan Dvmap εγκαθίσταται στη συσκευή του θύματος σε δύο στάδια. Κατά τη διάρκεια της αρχικής φάσης, το κακόβουλο λογισμικό προσπαθεί να αποκτήσει πλήρη δικαιώματα (root) στη συσκευή. Αν η προσπάθειά του αυτή στεφθεί με επιτυχία, θα εγκαταστήσει μια σειρά εργαλείων, μερικά από τα οποία περιέχουν σχόλια στην κινεζική γλώσσα. Μία από τις μονάδες αυτές είναι μια εφαρμογή, “com.qualcmm.timeservices”, η οποία συνδέει το Trojan με τον command and control server. Ωστόσο, κατά την περίοδο της έρευνας το κακόβουλο λογισμικό δεν έλαβε πίσω καμία εντολή.

Στην κύρια φάση της «μόλυνσης», το Trojan ξεκινά ένα αρχείο “εκκίνησης”, ελέγχει την έκδοση του Android που βρίσκεται εγκατεστημένη και αποφασίζει σε ποια βιβλιοθήκη να εγχύσει τον κώδικά του. Το επόμενο βήμα: η αντικατάσταση του υφιστάμενου κώδικα με κακόβουλο κώδικα, η οποία μπορεί να προκαλέσει κρασάρισμα της «μολυσμένης» συσκευής.

Οι βιβλιοθήκες συστήματος που έχουν ενημερωθεί εκ νέου εκτελούν μια κακόβουλη λειτουργική ενότητα, η οποία μπορεί να απενεργοποιήσει τη λειτουργία “Πιστοποίηση Εφαρμογών”. Στη συνέχεια, ενεργοποιεί τη ρύθμιση “Άγνωστες πηγές”, η οποία της επιτρέπει να εγκαθιστά εφαρμογές από οπουδήποτε και όχι μόνο από το Google Play Store. Αυτές θα μπορούσαν να είναι

κακόβουλες ή ανεπιθύμητες διαφημιστικές εφαρμογές.

«*Το Trojan Dvmap σηματοδοτεί μια επικίνδυνη νέα εξέλιξη στο Android κακόβουλο λογισμικό, με τον κακόβουλο κώδικα να εισάγεται σε βιβλιοθήκες συστημάτων όπου είναι πιο δύσκολο να εντοπιστεί και να αφαιρεθεί. Οι χρήστες που δεν διαθέτουν την απαραίτητη ασφάλεια για να εντοπίσουν και να μπλοκάρουν την απειλή προτού αυτή εξαπλωθεί, θα δυσκολευτούν αρκετά. Πιστεύουμε ότι έχουμε αποκαλύψει το κακόβουλο λογισμικό σε πολύ πρώιμο στάδιο. Η ανάλυσή μας δείχνει ότι οι κακόβουλες ενότητες αναφέρουν κάθε κίνηση τους στους εισβολείς και ορισμένες τεχνικές μπορούν να σπάσουν τις «μολυσμένες» συσκευές. Ο χρόνος είναι ουσιαστικός όταν πρόκειται να αποτρέψουμε μια μαζική και επικίνδυνη επίθεση*», δήλωσε ο Roman Unuchek, Senior Malware Analyst της Kaspersky Lab.

Στους ενδιαφερόμενους χρήστες που μπορεί να έχουν «μολυνθεί» από το Dvmap συνιστάται να δημιουργούν αντίγραφα ασφαλείας όλων των δεδομένων τους και να πραγματοποιούν επαναφορά εργοστασιακών δεδομένων. Επιπλέον, η Kaspersky Lab συμβουλεύει όλους τους χρήστες να εγκαταστήσουν στη συσκευή τους μια αξιόπιστη λύση ασφαλείας, όπως το Kaspersky Internet Security for Android, να ελέγχουν πάντοτε ότι οι εφαρμογές έχουν δημιουργηθεί από αξιόπιστο προγραμματιστή, να διατηρούν ενημερωμένα το λειτουργικό τους σύστημα και το λογισμικό εφαρμογών και να μην «κατεβάζουν» οτιδήποτε μοιάζει ύποπτο ή είναι αδύνατη η επαλήθευση της πηγής του.

Για περισσότερες πληροφορίες για το Trojan Dvmap μπορείτε να διαβάσετε το blogpost στον ειδικό ιστότοπο Securelist.com.

Όλα τα προϊόντα της Kaspersky Lab ανιχνεύουν το Trojan ως Trojan.AndroidOS.Dvmap.a.