25 Ιουλίου 2015

Όταν ο λύκος φυλάει πρόβατα: λογισμικό παραβίασης android

/ Πεμπτουσία

Image not found or type unknown

Image not found or type unknown **Για την ανάπτυξη και διανομή του εξελιγμένου malware για Android, Dendroid RAT, κατηγορείται ένας πρώην ερευνητής της εταιρείας διαδικτυακής ασφάλειας, FireEye. Το Dendroid είναι ένα εργαλείο απομακρυσμένης διαχείρισης που είναι εντελώς αόρατο στο περιβάλλον χρήστη και στο περιβάλλον του firmware, διαθέτει APK binder (εργαλείο που επιτρέπει στους χρήστες να ενσωματώνουν malware σε γνήσιες εφαρμογές android), καθώς και ένα εξελιγμένο PHP Panel.**

Ο άνθρωπος με το διπλό πρόσωπο, ο 20χρονος Morgan Culbertson, εργαζόταν για το γίγαντα της ασφάλειας, FireEye, ενώ παράλληλα είχε αναπτύξει, εξέλισσε και πωλούσε το διαβόητο Dendroid Rat. Σύμφωνα με έγγραφα του δικαστηρίου στο οποίο έχει ανατεθεί η εκδίκαση της υπόθεσης, ο νεαρός φέρεται να δίεθετε επίσης προς πώληση τον πηγαίο κώδικα του malware, έναντι του ποσού των 65.000 δολαρίων.

Το εξελιγμένο εργαλείο απομακρυσμένης διαχείρισης Android συσκευών διατίθεται μέσω υπόγειων forums και μαύρων αγορών, στην τιμή των 300 δολαρίων, ενώ ανακαλύφθηκε για πρώτη φορά από εμπειρογνώμονες ασφάλειας της Symantec, τον Μάρτιο του 2014. Το Dendroid είναι ένα HTTP based RAT, με αρκετές δυνατότητες και χαρακτηριστικά, που επιτρέπει στον οποιονδήποτε με περιορισμένη εμπειρία και γνώση να μετατρέψει σε trojan οποιαδήποτε νόμιμη εφαρμογή android.

Μεταξύ των δυνατοτήτων του Dendroid περιλαμβάνονται:

· Διαγραφή των αρχείων καταγραφής κλήσεων

· Πραγματοποίηση κλήσεων

· Άνοιγμα ιστοσελίδων

- Καταγραφή ήχου και κλήσεων
- Αποστολή μηνυμάτων
- Λήψη και μεταφόρτωση φωτογραφιών και βίντεο
- Πραγματοποίηση επιθέσεων DoS

Ο 20χρονος Morgan Culbertson εντοπίστηκε από τις αρχές επιβολής του νόμου στα πλαίσια συντονισμένης επιχείρησης με την κωδική ονομασία Shrouded Horizon, η οποία οδήγησε στη σύλληψη 70 διαχειριστών & μελών της μαύρης αγοράς, Darkode.

“Η Εισαγγελία των ΗΠΑ επιβεβαίωσε στο Forbes την ταυτότητα του κατηγορούμενου Morgan Culbertson, ο οποίος εμφανίζεται στο LinkedIn εδώ: https://www.linkedin.com/pub/morgan-culbertson/5b/225/471. Σύμφωνα με τη δικογραφία, ο 20χρονος πωλούσε το κακόβουλο λογισμικό, την ίδια στιγμή που εργαζόταν για την FireEye”, αναφέρει το Forbes.

Ο Culbertson είχε εργαστεί στην FireEye για 12 εβδομάδες, υπηρετώντας την ομάδα Advanced Persistent Threat, ως ερευνητής στον τομέα των mobile απειλών. Όπως τονίζεται από τα μέσα μαζικής ενημέρωσης, ο Culbertson θα μπορούσε να έχει χρησιμοποιήσει πληροφορίες από απόρρητες έρευνες της FireEye για να βελτιώσει το λογισμικό του. Οι πληροφορίες στις οποίες ο νεαρός χάκερ είχε αποκτήσει πρόσβαση κατά τη διάρκεια της απασχόλησής του στην FireEye θα μπορούσαν να του έχουν επιτρέψει να αναπτύξει πολύπλοκο μηχανισμό αντι-ανίχνευσης.

Η FireEye επιβεβαίωσε ότι ο Culbertson έχει τεθεί σε διαθεσιμότητα: “Η πρακτική άσκηση του Culbertson έχει ανασταλεί εν αναμονή της εσωτερική επανεξέτασης των δραστηριοτήτων του”, ανέφερε στο CNN.

Οι κατηγορίες είναι σοβαρές καθώς σύμφωνα με το FBI ο νεαρός κατηγορείται πως συνωμότησε για τη διανομή κακόβουλου κώδικα: “Ο Culbertson κατηγορείται για τον σχεδιασμό του Dendroid, ενός κωδικοποιημένου malware που προορίζεται για απομακρυσμένη πρόσβαση, έλεγχο, και υποκλοπή δεδομένων από κινητά τηλέφωνα με λογισμικό Android. Το κακόβουλο λογισμικό φέρεται πως διατίθεται προς πώληση στην Darkode”.

Πηγή: SecNews.gr