19 Μαρτίου 2015

Προσοχή! Επικίνδυνο worm διαδίδεται μέσω Facebook

/ Πεμπτουσία

Image not found or type unknown

Ερευνητές ασφάλειας της Malwarebytes έχουν εντοπίσει ένα νέο worm στο Facebook, το οποίο εξαπλώνεται εκμεταλλευόμενο τις δημοφιλείς υπηρεσίες cloud, Amazon Web Services και Box.

Τα μέσα κοινωνικής δικτύωσης είναι ο κύριος φορέας της επίθεσης, σύμφωνα με πρόσφατες εκθέσεις που δημοσιεύθηκαν από ερευνητές και επιβεβαιώνουν ότι οι εγκληματίες του κυβερνοχώρου εκμεταλλεύονται τις πλατφόρμες αυτές, για τις παράνομες δραστηριότητές τους.

Το Facebook δεν θα μπορούσε φυσικά να αποτελεί εξαίρεση, και όπως διαπιστώθηκε, το δημοφιλές κοινωνικό δίκτυο χρησιμοποιείται για την εξάπλωση του επικίνδυνου worm, το οποίο ανήκει στην οικογένεια malware Kilim, και μπορεί να μετατρέψει οποιονδήποτε υπολογιστή σε “ζόμπι”, ή αλλιώς σε μέλος του botnet.

Σύμφωνα με έκθεση που δημοσιεύθηκε από την Malwarebytes, η αλυσίδα της επίθεσης ξεκινά με ένα δελεαστικό μήνυμα στο Facebook, που υπόσχεται στους χρήστες αποκαλυπτικές φωτογραφίες εφήβων, πορνογραφικού περιεχομένου.

Το μήνυμα περιλαμβάνει έναν σύνδεσμο ow.ly, που ανακατευθύνει τα θύματα σε

μια διεύθυνση URL, η οποία οδηγεί με τη σειρά της σε μια σελίδα του Amazon Web Services (AWS). Οι ανακατευθύνσεις όμως δεν τελειώνουν εκεί, καθώς η σελίδα του Amazon Web Services (AWS) στην πραγματικότητα οδηγεί τα θύματα σε μια κακόβουλη ιστοσελίδα (videomasars.healthcare), που χρησιμοποιείται από τους απατεώνες για να προσδιορίσουν ποια πλατφόρμα χρησιμοποιείται από τους χρήστες (desktop ή κινητή συσκευή), ώστε να τους ανακατευθύνουν σε διαφορετικές ιστοσελίδες, ανάλογα με τη συσκευή που χρησιμοποιούν.

Οι χρήστες κινητών τηλεφώνων ανακατευθύνονται σε ιστοσελίδες που παράγουν έσοδα μέσω affiliate marketing και περιέχουν διάφορες προσφορές, ενώ οι χρήστες που χρησιμοποιούν desktop υπολογιστές, καλούνται να κατεβάσουν ένα αρχείο από την cloud υπηρεσία Box, που περιέχει κακόβουλο λογισμικό.

Το αρχείο φαίνεται να περιέχει μια συλλογή από βίντεο (Videos_New.mp4_2942281629029.exe), όμως μέσω της σάρωσής του με λογισμικό ασφάλειας, είναι δυνατό να εξακριβωθεί ο κακόβουλος χαρακτήρας του. Το κακόβουλο αρχείο είναι ένα downloader για το Facebook worm, το οποίο έρχεται με μορφή επέκτασης του Chrome, και περιλαμβάνει και κάποια επιπλέον εκτελέσιμα.

Οι ερευνητές διαπίστωσαν ότι το worm δημιουργεί επίσης μια συντόμευση για τον Chrome, που ξεκινά στην πραγματικότητα ένα κακόβουλο app στο πρόγραμμα περιήγησης, απευθείας στην ιστοσελίδα του Facebook.

“Όπως αναφέρθηκε προηγουμένως, μια ψεύτικη επέκταση του Chrome εγκαθίσταται, όμως η υπόθεση δεν τελειώνει εδώ. Το κακόβουλο λογισμικό δημιουργεί και μια συντόμευση για τον Chrome, που ξεκινά στην πραγματικότητα ένα κακόβουλο app στο πρόγραμμα περιήγησης, απευθείας στην ιστοσελίδα του Facebook”, αναφέρεται στο blog post που δημοσιεύθηκε από την Malwarebytes. “Σε αυτή την τροποποιημένη έκδοση του προγράμματος περιήγησης, οι επιτιθέμενοι έχουν τον πλήρη έλεγχο, και μπορούν να παρακολουθούν όλες τις δραστηριότητες των χρηστών, αλλά και να περιορίζουν ορισμένα χαρακτηριστικά”.

Για παράδειγμα οι επιτιθέμενοι απενεργοποιούν την σελίδα των επεκτάσεων – στην οποία οι χρήστες, υπό κανονικές συνθήκες, μπορούν να αποκτήσουν πρόσβαση πληκτρολογώντας chrome: // extentions/ – σε μια προσπάθεια να μην επιτρέψουν στους χρήστες να απενεργοποιήσουν ή να αφαιρέσουν την κακόβουλη επέκταση.

Το τελευταίο στάδιο της επίθεσης περιλαμβάνει την αποστολή κακόβουλων μηνυμάτων σε όλους τους φίλους των θυμάτων, που υπόσχονται επίσης πρόσβαση

σε πορνογραφικό περιεχόμενο, με σκοπό την μόλυνση όλο και περισσότερων χρηστών και την εξάπλωση του worm στο κοινωνικό δίκτυο.

Πηγή: Secnews.gr