19 Μαΐου 2015

Χρήστες Dropbox και Yahoo: προσοχή στο phishing

/ Πεμπτουσία

Image not found or type unknown

Οι ειδικοί ασφάλειας προειδοποιούν για δύο νέες σημαντικές phishing εκστρατείες που στοχεύουν τους χρήστες του Dropbox και του Yahoo, σχεδιασμένες να εκθέσουν τα email accounts και να επιτρέψουν τα follow-up scams.

Οι επιθέσεις στο Yahoo Mail ανακαλύφθηκαν πριν από έναν μήνα και γίνονται με τη μορφή ενός απλού phishing email που απαιτεί από το θύμα πρέπει να κλικάρει ένα λινκ για να αποκαταστήσει την πρόσφατα ληγμένη πρόσβασή του στο ηλεκτρονικό ταχυδρομείο.

Το 'Update Now' link συνδέει τον χρήστη σε μια απατηλή Yahoo log-in page, σχεδιασμένη να συλλέγει τα credentials των χρηστών, σύμφωνα με την δήλωση της Symantec.

Εντούτοις, τα πράγματα γίνονται έπειτα περισσότερο ενδιαφέροντα, ο AV giant εξήγησε:
«Αμέσως μετά την έκθεση αυτών των Yahoo accounts, τα scammers συνδέθηκαν στα επηρεασθέντα accounts και πρόσθεσαν ένα εναλλακτικό email address. Αυτό το εναλλακτικό email address ήταν αρκετά «πανούργο», καθώς έκανε τα

scammers να φαίνονται ότι προέρχονται από ένα email address της Outlook.com email υπηρεσίας της Microsoft χρησιμοποιώντας ακριβώς το ίδιο όνομα χρήστη με το @yahoo.com account.

Για να μην υποψιαστούν τα θύματα ότι το account τους έχει εκτεθεί, τα scammers είχαν έναν κανόνα να προωθούν όλα τα μηνύματα στο copycat εναλλακτικό email address εξετάζει και να διαγραφούν αυτά τα μηνύματα, μην αφήνοντας κανένα ίχνος των μηνυμάτων μέσα στο Yahoo Mail inbox.»

Οι phishers χρησιμοποίησαν έπειτα τα κλεμμένα Yahoo mailbox credentials για να στείλουν τα μηνύματα στις επαφές των θυμάτων, με την μορφή του κλασικού “pretexting” scam.

Συγκεκριμένα, προσποιούμενοι ότι ήταν μέλος της οικογένειας των θυμάτων, και υποστηρίζοντας πως ήταν μεγάλη ανάγκη, ζητούσαν να τους αποσταλούν χρήματα.

Η Symantec συμβουλεύει τους χρήστες του Yahoo να ενεργοποιήσουν το two-step verification προκειμένου να μετριαστεί ο κίνδυνος από το phishing scam.

Επίσης σύμφωνα με δημοσιεύματα έχουν αποκαλυφθεί και πλαστά Dropbox emails τα οποία προτρέπουν τον παραλήπτη να κλικάρουν βλέποντας συνημμένα ‘επείγοντα και άκρως απόρρητα’ έγγραφα.
Ζητάται από το θύμα να κλικάρει σε ένα εικονίδιο του email, και μετά θα οδηγηθεί σε μια fake log-in σελίδα.

Πηγή: SecNews.gr