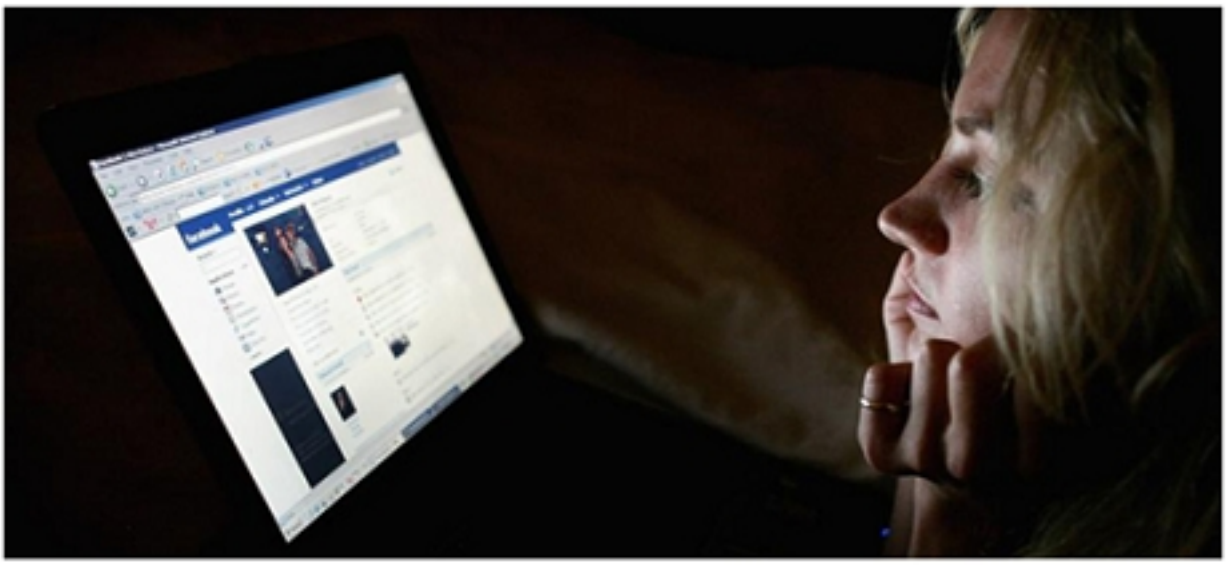

Ένα νέο και άκρως επικίνδυνο malware έκανε την εμφάνιση του στο διαδίκτυο. Εμφανίζεται στους χρήστες με την μορφή μηνυμάτων σχετικά με ένα υποτιθέμενο «ενδιαφέρον αρχείο».

Δεν είναι η πρώτη φορά βέβαια που εμφανίζεται τέτοιου είδους malware, το συγκεκριμένο όμως είναι μοναδικό, αφού μπορεί να διαδοθεί μέσω αρκετών instant messengers, ανάμεσά τους το Facebook Chat, Google Talk, Skype, Windows Live Messenger, Yahoo Messenger, ακόμα και το ICQ.

Η πρώτη επαφή με το malware γίνεται κυρίως μέσω του Facebook και συγκεκριμένα μέσω ενός link που παραπέμπει σε αρχείο του τύπου «Picturexx.JPG_www.facebook.com». Διαδίδεται μέσω του κοινωνικού δικτύου μέσω μιας εντολής στην γλώσσα προγραμματισμού Ajax που το κάνει να φαίνεται σαν να προέρχεται από έναν από τους φίλους σας στο Facebook.

Μόλις το malware αποκτήσει πρόσβαση στο μηχάνημα του χρήστη, μπορεί να λάβει εντολές από απομακρυσμένη τοποθεσία. Έτσι αυτόματα ξεκινά να στέλνει μηνύματα σε άλλους χρήστες, στην προσπάθειά του να μολύνει ακόμα περισσότερους υπολογιστές. Σύμφωνα με την McAfee, το malware παρακάμπτει το Firewall των Windows χρησιμοποιώντας την εντολή «netsh firewall allower program» ή τροποποιώντας το policy του firewall ώστε να προστεθεί στην λίστα των επιτρεπόμενων προγραμμάτων.

Στη συνέχεια προσθέτει τον εαυτό του στην λίστα εκκίνησης των Windows ενώ προσθέτει αντίγραφο «ασφαλείας» σε κρυφό φάκελο στον υπολογιστή του χρήστη ώστε να μπορεί να ξαναλειτουργήσει ακόμα και αν διαγραφεί. Ταυτόχρονα απενεργοποιεί όποιο σύστημα προστασίας βρει εγκατεστημένο, ακόμα και third-party antivirus και firewall, το Windows Update και το Yahoo Update.

Η McAfee τονίζει πως θα πρέπει να είμαστε πολύ προσεκτικοί με τα links που ανοίγουμε στο Facebook, ακόμα και αν αυτά προέρχονται από φίλους μας.

defencenet.gr