14 Νοεμβρίου 2015

Microsoft Office: απενεργοποιήστε τα macros από τα apps!

/ Πεμπτουσία

Image not found or type unknown

Απενεργοποιήστε τα macros από τα apps του Microsoft Office για να προστατευθείτε από malware spam campaign

Σκεφθείτε το καλά προτού ανοίξετε ένα συνημμένο αρχείο που περιέχεται σε ένα email που μόλις λάβατε από παραλήπτες άγνωστους για εσάς. Σκεφθείτε το δύο φορές εάν βρίσκεστε στην Ιαπωνία, καθώς υπάρχει μεγάλη πιθανότητα να είσθε θύμα ενός malware-ridden spam attack. Δεν χρειάζεται, ωστόσο, να ανησυχήσετε πολύ, αφού για να προστατεύσετε τον εαυτό σας, το μόνο που έχετε να κάνετε είναι να απενεργοποιήσετε τις μακροεντολές [macros] στα applications του Microsoft Office. Αυτό θα αποτρέψει την εκτέλεση των απειλών που βασίζονται στις μακροεντολές.

Το ζήτημα ήρθε στο φως στις 8 Οκτωβρίου, όταν εργαζόμενοι διαφόρων εταιρειών στην Ιαπωνία άρχισαν να λαμβάνουν ύποπτα emails, τα οποία, όπως αποδείχθηκε,

περιείχαν κακόβουλα συνημμένα αρχεία.

Ερευνητές από την Symantec, οι οποίοι βρήκαν το malware, επιβεβαίωσαν πως αυτά τα emails ήταν μέρος ενός ‘κύματος’ μαζικών malware-ridden spam attacks τα οποία διεξάγονται στην παρούσα φάση στην Ιαπωνία. Σε αυτά τα emails βρίσκονται συνημμένα έγγραφα Microsoft Word, που περιλαμβάνουν κακόβουλες μακροεντολές. Οι ερευνητές δήλωσαν πως το κακόβουλο λογισμικό προσπαθεί να κατεβάσει το ίδιο εκτελέσιμο αρχείο (65g3f4.exe) από πολλαπλά remote locations.

“Παρατηρήσαμε πως οι προσπάθειες για download γίνονται από τα ακόλουθα domains: **Leelazarow[.]com, Rockron[.]com, www[.]profes-decin[.]kvalitne[.]cz**,” αναφέρουν στο blog post.

“Υπάρχουν δύο είδη αυτών των emails: το ένα εμφανίζεται ως επιβεβαίωση παραγγελίας από μια Ιαπωνική εταιρεία- πάροχο εξοπλισμού, και το δεύτερο μοιάζει να είναι από μια τοπική εταιρεία εκτυπώσεων,” αναφέρουν οι ερευνητές.

Εντόπισαν ένα κακόβουλο έγγραφο Word με την ονομασία **W97M.Downloader,** ένα γνωστό εργαλείο για τέτοιου είδους απειλές όπως είναι τα **Trojan.Cryptodefense** και **Trojan.Cridex**.

Πηγή: secnews.gr