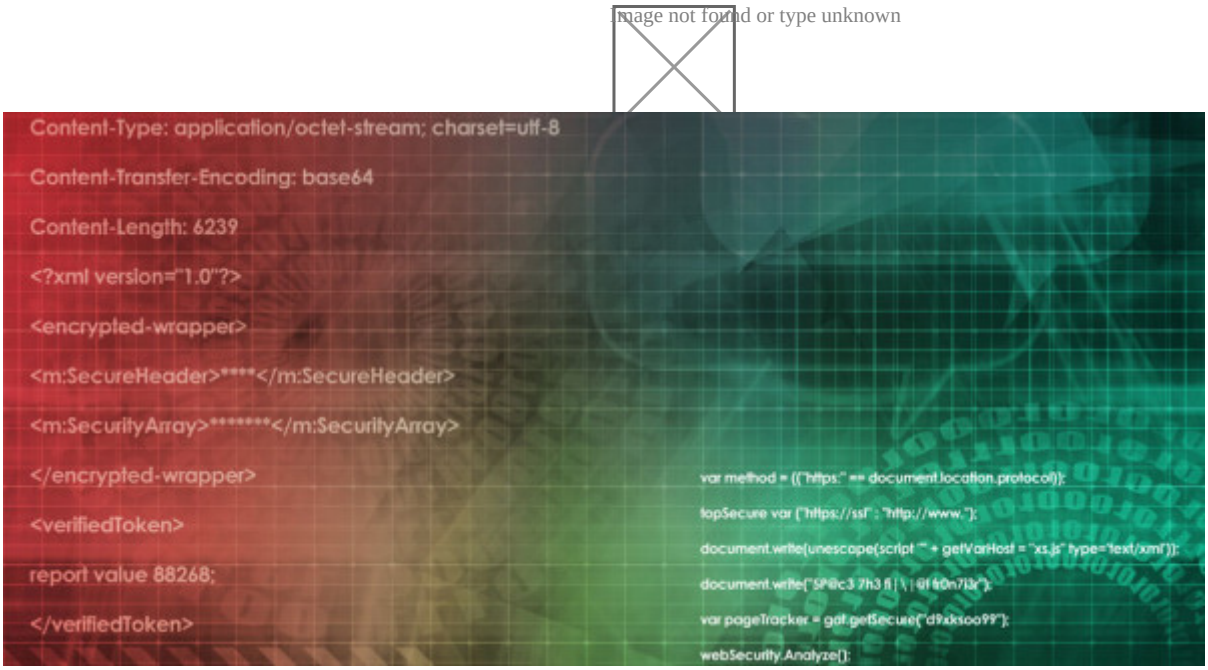
12 Μαρτίου 2015

Κίνδυνος κρυμμένος σε αρχεία PDF

/ Πεμπτουσία



Κακόβουλος script κώδικας μπορεί να κρυφτεί μέσα σε ασπρόμαυρες, JPEG εικόνες, που βρίσκονται μέσα σε αρχεία ***PDF*** και να τρέξει σε έναν υπολογιστή, αναφέρει ένας ερευνητής ασφαλείας.

Παρά το γεγονός ότι προϊόντα antivirus περιλαμβάνουν ανίχνευση για ακατάλληλα PDF, δε μπορούν να επικυρώνουν δεδομένα που συμπιέζονται με «lossy» software, όπως το DCTDecode, που χρησιμοποιείται για συμπίεση multimedia.

Για λόγους απόδοσης, και επειδή θεωρήθηκε ότι οι πληροφορίες χάνονται κατά τη διαδικασία αποσυμπίεσης με αποτέλεσμα τα κακόβουλα script να χάνονται και αυτά κατά τη διαδικασία, το αρχείο που προκύπτει με τον τρόπο αυτό είναι απλά μια προσέγγιση του αρχικού.

Όταν χρησιμοποιείται το DCTDecode, μια εικόνα JPEG στα χρώματα RGB έχει μειωμένη ποιότητα, απορρίπτοντας κάποιες πληροφορίες, που δε θα επηρεάσουν το συνολικό αποτέλεσμα σε ένα αρχείο PDF.

Σε μαύρες και άσπρες εικόνες, το pixel φέρει μόνο πληροφορίες έντασης, με το μαύρο να είναι το ισχυρότερο και το λευκό να είναι το πιο αδύναμο.

Ο ερευνητής Dénes Óvári, κωδικοποίησε ένα script ως εικόνα JPEG σε αποχρώσεις του γκρι και χρησιμοποίησε την υψηλότερη ποιότητα των ρυθμίσεων. Ο κακόβουλος κώδικας ήταν σε 0x00 bytes μέχρι το επόμενο μπλοκ των pixel (MCU), με τη διαδικασία να επαναλαμβάνεται πολλές φορές.

Κρύβοντας το κακόβουλο κώδικα με τον τρόπο αυτό, το καθιστά αόρατο σε κάποια τυποποιημένα εργαλεία που χρησιμοποιούνται στην ανίχνευση ακατάλληλων αρχείων PDF.

Πηγή: Secnews.gr