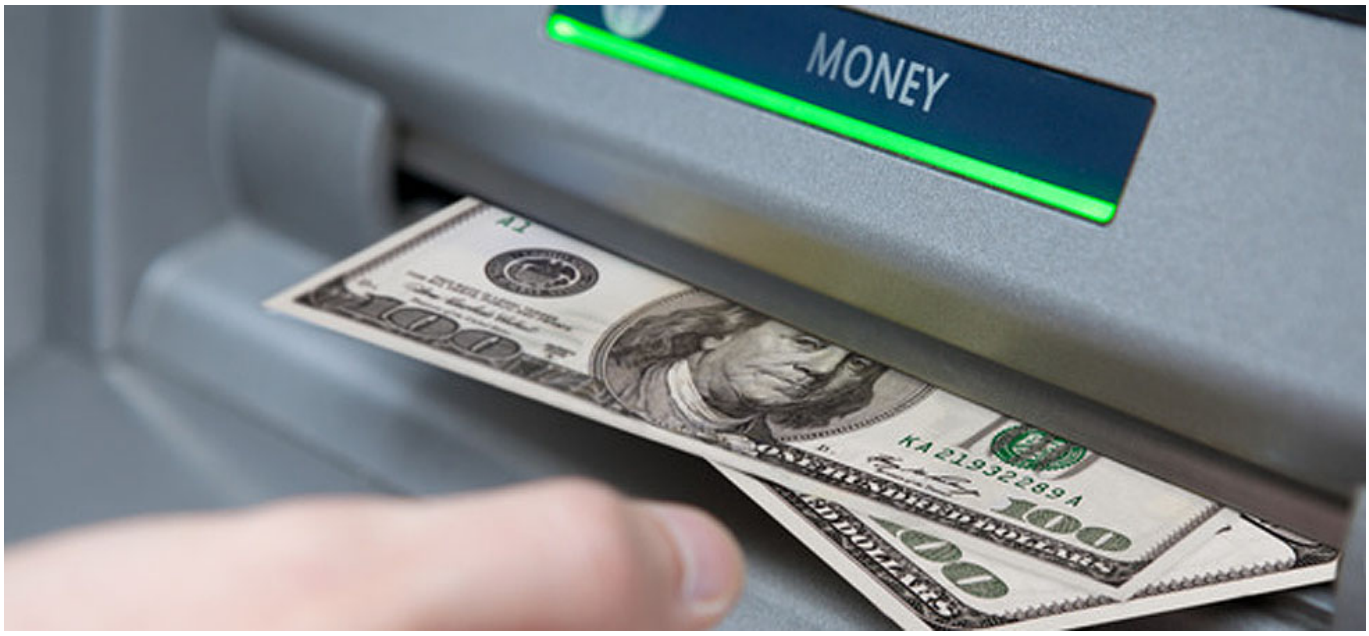
16 Οκτωβρίου 2015

GreenDispenser: malware-κίνδυνος για ATM

/ Πεμπτουσία

Image not found or type unknown



Ένα νέο malware, με το όνομα GreenDispenser, το οποίο δίνει την δυνατότητα σε hackers να επιτεθούν σε εκτεθειμένα ATMs και να αρπάξουν όλα τα μετρητά του, μια ομάδα ερευνητών ασφαλείας από την PointProof . Το GreenDispenser σηκώνει όλα τα λεφτά από τα ATMs – Τα ATM malwares δεν είναι μύθος στον κυβερνοκόσμο, είναι μια πραγματικότητα, και αυτή η περίπτωση δεν είναι διαφορετική από τις υπόλοιπες.

Το malware δρα με την βασική μεθοδολογία μιας DDoS επίθεσης, κατά την οποία το μηχάνημα εμφανίζει το μήνυμα ‘out of service’ στην οθόνη του. Εντωμεταξύ, ο κωδικός PIN μπορεί να ‘σπάσει’ κι έτσι να ανοίξει η ΄πόρτα’ του μηχανήματος δίνοντας έτσι την ευκαιρία στους κακόβουλους χάκερς να αρπάξουν από μέσα του όλα τα μετρητά.

Τέτοιου είδους δραστηριότητες αναφέρθηκαν πρωτίστως στο Μεξικό, ενώ παρόμοιες παραβιάσεις αναφέρθηκαν μετέπειτα και σε άλλες χώρες ανά τον κόσμο. Το GreenDispenser, σε αντίθεση με τους προκατόχους του, Ploutus και Tyupkin, δεν απαιτεί καμία φυσική παρουσία για την εγκατάστασή του, γεγονός

που το καθιστά πολύ πιο εύκολο για τον hacker να εισβάλλει στο μηχάνημα και φυσικά στην συνέχεια στον server.

Υπήρχαν αμφιβολίες για το αν τα “cyber criminal bosses” έχουν στα χέρια τους ένα mobile app που τους παρέχει με two-step κρυπτογράφηση και δημιουργεί ένα firewall authorisation για malwares, όπως το ίδιο το GreenDispenser. Η ProofPoint, ωστόσο, σε ένα άλλο post της, εξηγεί αυτή την κρυπτογράφηση, – απόσπασμα από αυτό το post παρατίθεται στη συνέχεια: –

Το GreenDispenser χρησιμοποιεί authentication με τη βοήθεια ενός static hardcoded PIN, ακολουθούμενο από ένα δεύτερο layer πιστοποίησης με τη βοήθεια ενός dynamic PIN, το οποίο είναι μοναδικό για κάθε εκτέλεση του malware. Ο επιτιθέμενος παίρνει αυτό το δεύτερο PIN από έναν κωδικό QR που εμφανίζεται στην οθόνη του μολυσμένου ATM. Υποψιαζόμαστε ότι ο επιτιθέμενος έχει μια εφαρμογή στο κινητό τηλέφωνο και αποκομίζει με τη σάρωση του barcode το δεύτερο PIN – δηλαδή ένα είδος two-factor authentication.

Αυτά τα malwares εξελίσσονται με το πέρασμα του χρόνου, καθιστώντας έτσι τα ATM περισσότερο ευάλωτα. Τα ATM είναι ο πρωτεύων στόχος στην αλυσίδα των χρηματοπιστωτικών ιδρυμάτων. Έτσι, η ασφάλεια των credentials των πιστωτικών και χρεωστικών καρτών θα πρέπει επίσης να ενισχυθεί αναλόγως.

Το ερώτημα που προκύπτει από όλο αυτό ποιό είναι; Πόσο καιρό θα μας πάρει για να εξασφαλίσουμε πλήρως όλες τις παραμέτρους;

Πηγή: secnews.gr