Η Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος της Ελληνικής Αστυνομίας, ενημερώνει τους πολίτες για την εμφάνιση και στην χώρα μας, του κακόβουλου λογισμικού, που ονομάζεται «Locky». Το συγκεκριμένο κακόβουλο λογισμικό αποτελεί εξέλιξη του γνωστού κακόβουλου λογισμικού «Cryptolocker» ή «Ransomware», συγκαταλέγεται στις ψηφιακές απειλές τύπου Crypto-Malware και δύναται να επηρεάσει όλα τα λειτουργικά συστήματα.

Ειδικότερα, το συγκεκριμένο κακόβουλο λογισμικό, εξαπλώνεται – μεταδίδεται κυρίως, μέσω μηνυμάτων ηλεκτρονικού ταχυδρομείου, που φέρουν μολυσμένο επισυναπτόμενο αρχείο, καθώς και όταν επισκεπτόμαστε επισφαλείς ή μολυσμένες ιστοσελίδες.

Μετά την εγκατάστασή του στο λειτουργικό σύστημα, το κακόβουλο αυτό λογισμικό, χρησιμοποιώντας ένα εξελιγμένο σύστημα κρυπτογράφησης, κρυπτογραφεί – κλειδώνει διαφόρους τύπους ψηφιακών αρχείων, (ενδεικτικά: *.doc, *.docx, *.xls, *.ppt, *.psd, *.pdf, *.eps, *.ai, *.cdr, *.jpg, etc.), που είναι αποθηκευμένα στον ηλεκτρονικό υπολογιστή του χρήστη που έχει μολυνθεί από τον ιό, δίνοντας τους την κατάληξη ‘’locky’’, ενώ για να ξεκλειδωθούν τα αρχεία, οι δράστες ζητούν από τον χρήστη να καταβάλει χρηματικό ποσό.

Η καταβολή του χρηματικού ποσού προτείνεται να γίνει, μέσω ανώνυμου προγράμματος περιήγησης, με τη χρήση του ψηφιακού νομίσματος bitcoin (BTC), κατόπιν μηνύματος που εμφανίζεται στον χρήστη, με υποδείξεις και οδηγίες για την πληρωμή.

Καλούνται οι χρήστες του διαδικτύου να μην πληρώνουν τα χρήματα που ζητούνται, προκειμένου να αποθαρρύνονται τέτοιες παράνομες πρακτικές καθώς και για να μην εξαπλωθεί το φαινόμενο, ενώ θα πρέπει να είναι ιδιαίτερα προσεκτικοί και να λαμβάνουν μέτρα ψηφιακής προστασίας και ασφάλειας για την αποφυγή προσβολής από το προαναφερόμενο κακόβουλο λογισμικό.

Συγκεκριμένα:

• Οι πολίτες που λαμβάνουν μηνύματα ηλεκτρονικού ταχυδρομείου από άγνωστους αποστολείς ή άγνωστη προέλευση, καλούνται να μην ανοίγουν τους συνδέσμους (links) και να μην κατεβάζουν τα συνημμένα αρχεία, που περιέχονται σε αυτά, για τα οποία δεν γνωρίζουν με βεβαιότητα τον αποστολέα και το περιεχόμενο του συνημμένου αρχείου.

• Επιπλέον οι χρήστες πρέπει να είναι εξαιρετικά καχύποπτοι στα μηνύματα ηλεκτρονικού ταχυδρομείου που ως αποστολέας φαίνεται να είναι κάποια υπηρεσία ή εταιρεία.

• Συστήνεται να πληκτρολογούνται οι διευθύνσεις των ιστοσελίδων (URL) στον περιηγητή (browser), αντί να χρησιμοποιούνται υπερσυνδέσμοι (links).

• Να χρησιμοποιούνται γνήσια λογισμικά προγράμματα και να ενημερώνονται τακτικά (updates), ενώ θα πρέπει να υπάρχει πάντα ενημερωμένο πρόγραμμα προστασίας (antivirus) του ηλεκτρονικού υπολογιστή.

• Να ελέγχουν και να έχουν πάντοτε ενημερωμένη την έκδοση του λειτουργικού τους συστήματος.

• Να δημιουργούν αντίγραφα ασφαλείας των αρχείων της συσκευής τους (backup) σε τακτά χρονικά διαστήματα, σε εξωτερικό μέσο αποθήκευσης, έτσι ώστε σε περίπτωση «προσβολής» από το κακόβουλο λογισμικό, να είναι δυνατή η αποκατάσταση των αρχείων τους.

Υπενθυμίζεται ότι για ανάλογα περιστατικά, οι πολίτες μπορούν να επικοινωνούν με την Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος στα ακόλουθα στοιχεία επικοινωνίας:

• Τηλεφωνικά: 11188

• Στέλνοντας e-mail στο: ccu@cybercrimeunit.gov.gr

• Μέσω της εφαρμογής (application) για έξυπνα τηλέφωνα (smart phones): CYBERKID

• Μέσω twitter: @CyberAlertGR

Πηγή: newsbeast.gr