Η Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος του Αρ-χηγείου Ελληνικής Αστυνομίας, ενημερώ νει τους πολίτες για την εμφάνιση -σε διεθνές επίπεδο- μιας νέας...

έκδοσης κακόβουλου λυτρισμικού λογισμικού «Ransomware–Cryptoware» υπό την ονομασία «JNEC», που παρουσιάζει αυξημένο ενδιαφέρον, αφενός ως προς τη μέθοδο παραπλάνησης των υποψήφιων θυμάτων και αφετέρου ως προς τον τρόπο λήψης του κλειδιού αποκρυπτογράφησης.
Το συγκεκριμένο κακόβουλο λογισμικό JNEC εκμεταλλεύεται κενό ασφάλειας παλαιότερων εκδόσεων ευρέως χρησιμοποιούμενου λογισμικού συμπίεσης/αποσυμπίεσης αρχείων μολύνοντας πληροφοριακά συστήματα με την αποστολή μηνυμάτων ηλεκτρονικού ταχυδρομείου που εμπεριέχουν κακόβουλα επισυναπτόμενα αρχεία, κυρίως δε «παραποιημένες – αλλοιωμένες» φωτογραφίες γυναικώ ν.
Μετά την εγκατάσταση του λυτρισμικού λογισμικού στο πληροφοριακό σύστημα: κρυπτογραφείται το σύνολο των αρχείων που εντοπίζει, απαιτείται η πληρωμή «λύτρων» για την παροχή του κλειδιού αποκρυπτογράφησης σε μορφή κρυπτονομισμάτων, υποδ εικνύεται στο χρήστη η δημιουργία συγκεκριμένης διεύθυνσης ηλεκτρονικού ταχυδρομείου για να λάβει το κλειδί αποκρυπτογράφησης.
Στο πλαίσιο αυτό, καλούνται οι χρήστες του διαδικτύου και οι διαχειριστές δικτύων να είναι ιδιαίτερα προσεκτικοί, να λαμβάνουν μέτρα ψηφιακής προστασίας και ασφάλειας για την αποφυγή προσβολής τους από κακόβουλο λογισμικό, καθώ ς επίσης να μην προβαίνουν στην πληρωμή των ζητούμενων «λύτρων», προκειμένου να αποθαρρύνονται τέτοιες παράνομες πρακτικές και να αποτρέπεται η περαιτέρω εξάπλωση του φαινομένου.

Συγκεκριμένα, καλούνται οι χρήστες του διαδικτύου ή/και οι διαχειριστές δικτύων:
– Να δημιουργούν αντίγραφα ασφαλείας των αρχείων (backup) σε τακτά χρονικά διαστήματα, σε εξωτερικό μέσο αποθήκευσης, το οποίο πρέπει να διατηρούν εκτός του δικτύου, έτσι ώ στε σε περίπτωση προσβολής να είναι δυνατή η αποκατάσταση τους.
– Στις περιπτώ σεις που λαμβάνουν μηνύματα ηλεκτρονικού ταχυδρομείου από άγνωστους αποστολείς ή άγνωστη προέλευση, να μην ανοίγουν τους συνδέσμους (links) και να μην κατεβάζουν συνημμένα αρχεία, που περιέχονται στα μηνύματα αυτά, για τα οποία δεν γνωρίζουν με βεβαιότητα τον αποστολέα και το περιεχόμενο του συνημμένου αρχείου.
– Να ελέγχουν και να εγκαθιστούν πάντα την ενημερωμένη (UptoDate) έκδοση του λειτουργικού τους συστήματος.
– Να χρησιμοποιούν γνήσια λογισμικά προγράμματα, ενημερωμένα στην τελευταία τους έκδοση και να διατηρούν πάντα ενημερωμένο το πρόγραμμα προστασίας του ηλεκτρονικού τους υπολογιστή από κακόβουλο λογισμικό.
– Να φροντίζουν για την προστασία και των φορητώ ν τους συσκευώ ν (Tablet&Smartphones),Οδηγίες και συμβουλές υπάρχουν στον ιστότοπο http://www.cyberalert.gr/mobile-malware.
Σημειώ νεται ότι, για περιστατικά μολύνσεων από κακόβουλο λογισμικό τύπου Ransomware – Cryptoware, η EUROPOL και το European Cybercrime Centre (EC3) έχουν θέσει σε λειτουργία τον ιστότοπο https://www.nomoreransom.org, όπου οι πολίτες μπορούν να βρουν συμβουλές προστασίας, αλλά και κλειδιά αποκρυπτογράφησης για ορισμένες από τις μορφές κακόβουλου λογισμικού.