

Συναγερμός έχει σημάνει στη Διεύθυνση Δίωξης Ηλεκτρο-νικού Εγκλήματος της Ελληνικής Αστυνομίας, μετά την ε-μφάνιση και στην Ελλάδα, νέων εκδόσεων του...

κακόβουλου λογισμικού «Dharma», το οποίο είναι τύπου «Ransomware – Cryptoware» και μπορεί να επηρεάσει αρκετές εκδόσεις λειτουργικού συστήματος.
Σύμφωνα με την Αστυνομία, το κακόβουλο λογισμικό μολύνει τους ηλεκτρονικούς υπολογιστές με δύο, κυρίως, τρόπους:
• μέσω μηνυμάτων ηλεκτρονικού ταχυδρομείου, που εμπεριέχουν κακόβουλα επισυναπτόμενα αρχεία και
• μέσω επισφαλώ ν ή «μολυσμένων» ιστοσελίδων.
Ειδικότερα, ως προς τα κακόβουλα αρχεία, πρόκειται συνήθως για αρχεία τύπου .docx και .pdf, στα οποία έχουν ενσωματωθεί κακόβουλες μακροεντολές, που εκτελούνται κατά το άνοιγμά τους και εγκαθιστούν το κακόβουλο λογισμικό στον ηλεκτρονικό υπολογιστή.
Μετά την εγκατάστασή του στο λειτουργικό σύστημα, το ransomware κρυπτογραφεί – κλειδώ νει ψηφιακά αρχεία, που είναι αποθηκευμένα στον ηλεκτρονικό υπολογιστή του χρήστη που έχει μολυνθεί.
Για να ξεκλειδωθούν τα μολυσμένα αρχεία ενός ηλεκτρονικού υπολογιστή, ζητείται η καταβολή χρηματικού ποσού, με τη χρήση του ψηφιακού νομίσματος Bitcoin (BTC) ως «λύτρα», σε διαφορετική περίπτωση καθίστανται απροσπέλαστα για το χρήστη τους.
Σημειώ νεται ότι το συγκεκριμένο κακόβουλο λογισμικό έχει τη δυνατότητα να αυτοδιαδίδεται μέσω του τοπικού δικτύου και να κρυπτογραφεί τα αρχεία κάθε συστήματος στο οποίο αποκτά πρόσβαση. Η δυνατότητα αυτή το καθιστά εξαιρετικά επικίνδυνο σε εταιρικά δίκτυα όπου η διάδοση μπορεί να είναι ραγδαία.
Στο πλαίσιο αυτό, καλούνται οι χρήστες του διαδικτύου και οι διαχειριστές δικτύων να είναι ιδιαίτερα προσεκτικοί και να λαμβάνουν μέτρα ψηφιακής προστασίας και ασφάλειας για την αποφυγή προσβολής από το κακόβουλο λογισμικό, καθώ ς και να μην πληρώ νουν τα χρήματα που ζητούνται, 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 και να διατηρούνται εκτός δικτύου, έτσι ώ στε να είναι δυνατή η αποκατάστασή τους.
• Στις περιπτώ σεις όπου 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. Ιδιαίτερη προσοχή θα πρέπει να δίνεται σε μηνύματα ηλεκτρονικού ταχυδρομείου, όπου ως αποστολέας φαίνεται να είναι κάποια υπηρεσία ή εταιρεία άγνωστη προς αυτούς.

• Να πληκτρολογούν τις διευθύνσεις των ιστοσελίδων (URL) στον φυλλομετρητή ιστοσελίδων (browser), αντί να χρησιμοποιούν υπερσυνδέσμους (links).

• Να χρησιμοποιούν γνήσια λογισμικά προγράμματα, ενώ θα πρέπει να υπάρχει πάντα ενημερωμένο πρόγραμμα προστασίας από κακόβουλο λογισμικό του ηλεκτρονικού υπολογιστή.

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

• Να απενεργοποιήσουν την εκτέλεση μακροεντολώ ν και JavaScript στις εφαρμογές με τις οποίες ανοίγουν αρχεία τύπου .docx και .pdf.

• Να φροντίζουν για την προστασία και των φορητώ ν τους συσκευώ ν (tablet & έξυπνα κινητά τηλέφωνα). Περισσότερες 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 μορφές κακόβουλου λογισμικού.

Υπενθυμίζεται ότι οι πολίτες μπορούν να επικοινωνούν, ανώ νυμα ή επώ νυμα, με τη Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος προκειμένου να παρέχουν πληροφορίες ή να καταγγέλλουν παράνομες ή επίμεμπτες πράξεις ή δραστηριότητες που τελούνται μέσω Διαδικτύου, στα ακόλουθα στοιχεία επικοινωνίας:

• Τηλεφωνικά στον αριθμό 111 88

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

• Μέσω της εφαρμογής (application) για έξυπνα τηλέφωνα (smart phones), με λειτουργικό σύστημα iOS – Android: FEELSAFE E-COMMERCE

• Μέσω Twitter «Γραμμή SOS Cyber Alert»: https://twitter.com/CyberAlertGR