Συμβουλές προστασίας από το ιό «WannaCry»

Συμβουλές προστασίας από το ιό «WannaCry» που από χθες έχει χτυπήσει μαζικά εταιρείες, φορείς και οργανισμούς σε πάνω από 100 χώρες, δίνει η Δίωξη Ηλεκτρονικού Εγκλήματος στους χρήστες του διαδικτύου.
Σημειώνεται ότι πρόκειται για μια πρωτοφανούς κλίμακας παγκόσμια κυβερνοεπίθεση που εκδηλώθηκε παράλληλα σε πάνω από 50.000 στόχους σε όλο τον πλανήτη. Θύμα στη Μ. Βρετανία έπεσε το Εθνικό Σύστημα και στην Ελλάδα το Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης.

Πως εμφανίζεται ο ιός

Η Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος της Ελληνικής Αστυνομίας ενημερώνει τους πολίτες για την συνεχιζόμενη εμφάνιση και στη χώρα μας, του κακόβουλου λογισμικού «WannaCry», το οποίο συγκαταλέγεται στις ψηφιακές απειλές τύπου «Crypto-Malware» και μπορεί να επηρεάσει όλες τις εκδόσεις λειτουργικού συστήματος.
Το κακόβουλο λογισμικό μολύνει τους ηλεκτρονικούς υπολογιστές με δύο, κυρίως, τρόπους:

- μέσω μολυσμένων μηνυμάτων ηλεκτρονικού ταχυδρομείου, που εμπεριέχουν κακόβουλα επισυναπτόμενα αρχεία και
- μέσω επισφαλών ή μολυσμένων ιστοσελίδων.

Ειδικότερα, ως προς τα μολυσμένα 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 Η/Υ.
Μετά την εγκατάστασή του στο λειτουργικό σύστημα, κρυπτογραφεί – κλειδώνει ψηφιακά αρχεία και τα δεδομένα τύπων .lay6, .sqlite3, .sqlitedb, .accdb, .java, .class, .mpeg, .djvu, .tiff, .backup, .vmdk, .sldm, .sldx, .potm, .potx, .ppam, .ppsx, .ppsm, .pptm, .xltm, .xltx, .xlsb, .xlsm, .dotx, .dotm, .docm, .docb, .jpeg, .onetoc2, .vsdx, .pptx, .xlsx και .docx, που είναι αποθηκευμένα στον ηλεκτρονικό υπολογιστή του χρήστη που έχει μολυνθεί από τον ιό.
Για να ξεκλειδωθούν τα μολυσμένα αρχεία ενός Η/Υ, ζητείται η καταβολή χρηματικού ποσού, με τη χρήση του ψηφιακού νομίσματος Bitcoin (BTC) ως «λύτρα», σε διαφορετική περίπτωση καθίστανται απροσπέλαστα για το χρήστη τους.
Επιπλέον, 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.
Σημειώνεται ότι το κακόβουλο λογισμικό κυκλοφορεί από τις 12 - 05 - 2017 και έχει μέχρι στιγμής μολύνει περισσότερους από 125.000 ηλεκτρονικούς υπολογιστές παγκοσμίως.

Στο πλαίσιο αυτό, καλούνται οι χρήστες του διαδικτύου και οι διαχειριστές εταιρικών δικτύων να είναι ιδιαίτερα προσεκτικοί και να λαμβάνουν μέτρα ψηφιακής προστασίας και ασφάλειας για την αποφυγή προσβολής από το κακόβουλο λογισμικό, καθώς και να μην πληρώνουν τα χρήματα που ζητούνται, προκειμένου να αποθαρρύνονται τέτοιες παράνομες πρακτικές και να αποτρέπεται η περαιτέρω εξάπλωση του φαινομένου.

Τι πρέπει να κάνουν οι χρήστες

- Οι χρήστες 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 η οποία δεν είναι γνωστή σε αυτούς.
- Συστήνεται να πληκτρολογούνται οι διευθύνσεις των ιστοσελίδων (URL) στον φυλλομετρητή ιστοσελίδων (browser), αντί να χρησιμοποιούνται υπερσύνδεσμοι (links).
- Να χρησιμοποιούνται γνήσια λογισμικά προγράμματα και να ενημερώνονται τακτικά (updates), ενώ θα πρέπει να υπάρχει πάντα ενημερωμένο πρόγραμμα προστασίας από ιούς του Η/Υ.
- Να ελέγχουν και να έχουν πάντοτε ενημερωμένη την έκδοση του λειτουργικού τους συστήματος.
- Να δημιουργούνται αντίγραφα ασφαλείας των αρχείων (backup) σε τακτά χρονικά διαστήματα, σε εξωτερικό μέσο αποθήκευσης και να διατηρούνται εκτός δικτύου, έτσι ώστε σε περίπτωση «προσβολής» από το κακόβουλο λογισμικό, να είναι δυνατή η αποκατάστασή τους.
- Στους διαχειριστές εταιρικών δικτύων συστήνεται ιδιαίτερη προσοχή στην τακτική και ασφαλή τήρηση αντιγράφων ασφαλείας, καθότι τα αντίγραφα αποτελούν το μόνο τρόπο επαναφοράς των αρχείων στο σύνολό τους.
- Να απενεργοποιήσουν την εκτέλεση μακροεντολών και JavaScript στις εφαρμογές με τις οποίες ανοίγουν αρχεία τύπου .docx και .pdf.
- Σημειώνεται ότι για περιστατικά μολύνσεων από κακόβουλο λογισμικό τύπου Crypto-Malware, 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.