23-10-2020: Η Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος ενημερώνει τους πολίτες σχετικά με διασπορά κακόβουλου λογισμικού μέσω μηνυμάτων ηλεκτρονικού ταχυδρομείου (emails)

ΑΡΧΗΓΕΙΟ ΕΛΛΗΝΙΚΗΣ ΑΣΤΥΝΟΜΙΑΣ

Αθήνα, 23 Οκτωβρίου 2020

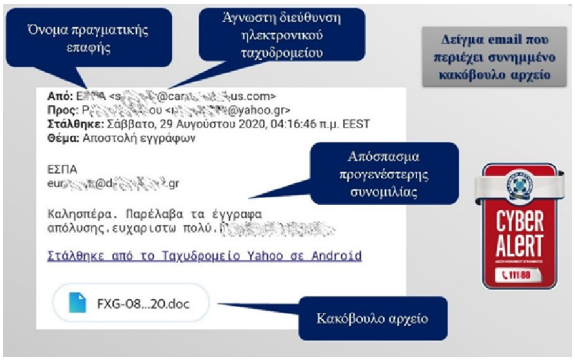
ΔΕΛΤΙΟ ΤΥΠΟΥ

Η Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος ενημερώνει τους πολίτες σχετικά με διασπορά κακόβουλου λογισμικού μέσω μηνυμάτων ηλεκτρονικού ταχυδρομείου (emails)

Στη Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος καταγγέλλονται το τελευταίο διάστημα περιστατικά λήψης μηνυμάτων ηλεκτρονικού ταχυδρομείου (emails) που εμπεριέχουν αρχεία κακόβουλου λογισμικού (malware).

Ειδικότερα, το θύμα λαμβάνει μήνυμα από άγνωστη διεύθυνση ηλεκτρονικού ταχυδρομείου, στο οποίο:

- το εμφανιζόμενο όνομα αποστολέα είναι υπαρκτό και ανήκει στη λίστα επαφών του,
- το περιεχόμενο του μηνύματος αποτελεί απόσπασμα προγενέστερης συνομιλίας μεταξύ του εμφανιζόμενου αποστολέα και άλλης επαφής (ή και του ίδιου του θύματος),
- έχει επισυναφθεί αρχείο (συνήθως τύπου Word), το οποίο εμπεριέχει (συγκεκαλυμμένο) κακόβουλο εκτελέσιμο κώδικα.



Από τις έως τώρα έρευνες, διαπιστώνεται ότι το συνημμένο κακόβουλο αρχείο ανήκει στην κατηγορία «Δούρειος Ίππος» (Trojanhorse). Το είδος αυτό του κακόβουλου λογισμικού χρησιμοποιείται, μεταξύ άλλων:

- για να ανοίξουν «κερκόπορτες» σε ένα σύστημα με σκοπό ο επιτιθέμενος να αποκτήσει τον έλεγχο της προσβληθείσας συσκευής,
- για να υποκλέψει προσωπικά δεδομένα του χρήστη και
- για να κατεβάσει και να εκτελέσει άλλο κακόβουλο λογισμικό.

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.

Συγκεκριμένα, καλούνται οι χρήστες του διαδικτύου ή/και οι διαχειριστές δικτύων:

- Να παρατηρούν τη διεύθυνση του αποστολέα ενός μηνύματος ηλεκτρονικού ταχυδρομείου και ιδιαίτερα τις διαφορές στο εμφανιζόμενο όνομα και το email του αποστολέα.
- Να δημιουργούν αντίγραφα ασφαλείας των αρχείων (backup) σε τακτά χρονικά διαστήματα, σε εξωτερικό μέσο αποθήκευσης και να τα διατηρούν εκτός δικτύου, έτσι ώστε να είναι δυνατή η αποκατάστασή τους.
- Στις περιπτώσεις 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.
- Να χρησιμοποιούν γνήσια λογισμικά προγράμματα, ενημερωμένα στην τελευταία τους έκδοση, 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 μακροεντολών και JavaScript στις εφαρμογές με τις οποίες ανοίγουν αρχεία τύπου .docx και .pdf.
- Να φροντίζουν για την προστασία και των φορητών τους συσκευών (tablet & έξυπνα κινητά τηλέφωνα). Περισσότερες οδηγίες και συμβουλές υπάρχουν στον ιστότοπο http://www.cyberalert.gr/mobile-malware/ .

Υπενθυμίζεται ότι οι πολίτες μπορούν να επικοινωνούν, ανώνυμα ή επώνυμα, 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: **11188**
- Στέλνοντας e-mail στο: ccu@cybercrimeunit.gov.gr
- Μέσω twitter: **@CyberAlertGR**
- Μέσω της διαδικτυακής πύλης (portal) της Ελληνικής Αστυνομίας (https://portal.astynomia.gr)
- Μέσω της εφαρμογής (application) για έξυπνα τηλέφωνα (smart phones): **CYBERKID**

Κλείσιμο παραθύρου