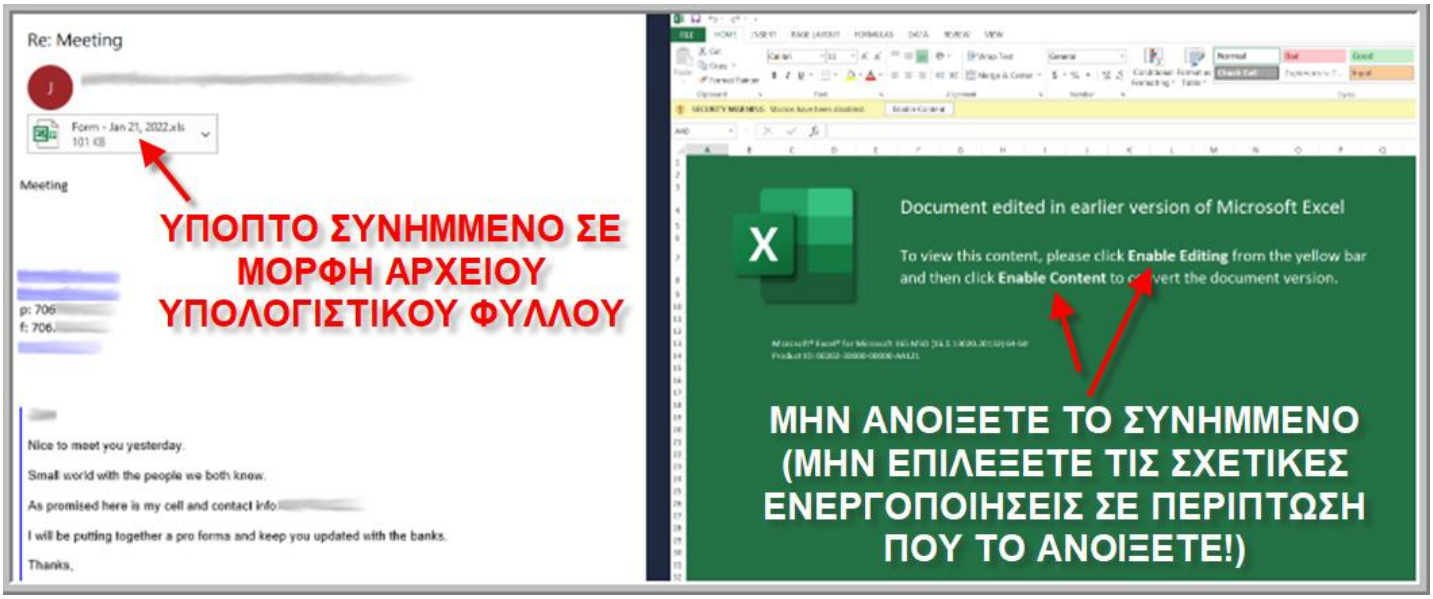
«Εχθρός... μετά των πυλών» - Κακόβουλο λογισμικό EMOTET

Αρθρογραφεί ο Παρασκευάς Γ. Παπαδόπουλος, Μηχανικός Η/Υ Συστημάτων, Η.Ι. (MSc) [email: pdesper@gmail.com]

Μία διαδεδομένη μορφή επιθέσεων τους τελευταίους μήνες, αποτελεί το EMOTET. Το Emotet ανήκει στην κατηγορία κακόβουλου (ή -εναλλακτικά όπως αναφέρεται- επιβλαβούς) λογισμικού (malicious software, malware ή badware) και διαδίδεται κυρίως μέσω μηνυμάτων email (ηλεκτρονικής αλληλογραφίας).

Ο παραλήπτης ενός τέτοιου email, πέραν του –συνήθως έκδηλα- ασαφούς περιεχομένου που θα αναφέρεται στο σώμα (body) και θέμα (subject) του μηνύματος (που μπορεί άμεσα να τον «υποψιάσει» από οπουδήποτε κι αν έχει αποσταλεί αυτό), θα παρατηρήσει πως υπάρχει και κάποιο συνημμένο αρχείο που τον προτρέπει να το ανοίξει.

Ειδικότερα, συνήθως το συνημμένο αρχείο είναι μορφής Microsoft Office (ποικίλων εκδόσεων) και πιο συγκεκριμένα είναι είτε αρχείο επεξεργασίας κειμένου (Word), είτε αρχείο υπολογιστικού φύλλου (Excel). Όταν ο παραλήπτης ΑΝΟΙΞΕΙ στη συσκευή του το συνημμένο αυτό αρχείο, θα του προταθεί να προβεί σε ΕΝΕΡΓΟΠΟΙΗΣΗ ΕΠΕΞΕΡΓΑΣΙΑΣ ή/και ΕΝΕΡΓΟΠΟΙΗΣΗ ΠΕΡΙΕΧΟΜΕΝΟΥ (βλέπετε χαρακτηριστικό παράδειγμα ληφθέντος email με σχετικό κακόβουλο συνημμένο υπολογιστικό αρχείο):



Ο παραλήπτης ΠΡΕΠΕΙ να ΜΗΝ ΑΝΟΙΞΕΙ ΤΟ ΣΥΝΗΜΜΕΝΟ ΑΡΧΕΙΟ. Ακόμα όμως κι αν το ανοίξει, έστω τότε να ΜΗΝ ΕΝΕΡΓΟΠΟΙΗΣΕΙ ΤΗΝ ΕΠΕΞΕΡΓΑΣΙΑ ΤΟΥ ΠΕΡΙΕΧΟΜΕΝΟΥ ΤΟΥ! Αν επιτρέψει την επεξεργασία/πρόσβαση στο περιεχόμενό του, ΤΟΤΕ θα εγκατασταθεί το Emotet (κακόβουλο λογισμικό) στη συσκευή του, που θα οδηγήσει σε μία ακολουθία διαφόρων –και δυσάρεστων- συμβάντων:

1. *θα διεισδύσει στις συνομιλίες του email του, αποστέλλοντας (ερήμην του) ανάλογα μηνύματα (email) σε όλους αυτούς (μέσω πρόσβασης στις «Επαφές» του) με αποστολέα εκείνον. Αποτέλεσμα, να θεωρείται έτσι από τους –μη υποψιασμένους- παραλήπτες/γνωστούς του ως «έμπιστος», άρα και δυνητικά έμπιστης αξιοπιστίας το email που θα λάβουν (μειώνοντας τους δισταγμούς τους στο να το ανοίξουν και να επεξεργαστούν κι εκείνοι το μολυσμένο συνημμένο, οπότε εν δυνάμει να «μολυνθούν» κι εκείνοι κοκ…),*
2. *στο παρασκήνιο, «παρακολούθηση/σάρωση» της συσκευής του παραλήπτη για εντοπισμό και υποκλοπή διαπιστευτηρίων (credentials), απόσπαση χρημάτων, παραχώρηση πρόσβασης στη τρέχουσα συσκευή του από άλλους εγκληματίες του κυβερνοχώρου…*

Τι θα πρέπει να προσέχουμε:

1. *πρώτα και πάνω από όλα θα πρέπει, ούτως ή άλλως, να φροντίζουμε ώστε το λειτουργικό σύστημα (operating system) και οι Εφαρμογές της συσκευής μας -σε θέματα ΑΣΦΑΛΕΙΑΣ- να είναι (όσο γίνεται) ενημερωμένα (updated),*
2. *παρομοίως, να είναι ΕΝΕΡΓΟΠΟΙΗΜΕΝΟ και ΕΝΗΜΕΡΩΜΕΝΟ το λογισμικό αντιϊκής προστασίας (antivirus) της συσκευής μας (λογικά –αναλόγως της αξιοπιστίας του- τότε θα αποκλειστεί αυτόματα η πρόσβαση σε τέτοιο περιεχόμενο και θα προστατευτούμε από βεβιασμένο «λάθος» μας να ανοίξουμε το συνημμένο του)*
3. *από εκεί και πέρα, αν λάβουμε κάποιο τέτοιο email, ΑΚΟΜΑ ΚΑΙ ΑΠΟ ΕΜΠΙΣΤΟ ΑΠΟΣΤΟΛΕΑ (γνώριμό μας) και μας «ξενίζει» το περιεχόμενο στο θέμα/σώμα του μηνύματος, τότε ΑΜΥΝΤΙΚΑ: ΔΕΝ ΠΡΕΠΕΙ να ανοίξουμε το συνημμένο του (πολύ δε περισσότερο ΜΗΝ ΕΠΙΛΕΞΟΥΜΕ τις ΠΡΟΤΡΟΠΕΣ «ΕΝΕΡΓΟΠΟΙΗΣΗΣ ΕΠΕΞΕΡΓΑΣΙΑΣ/ΠΕΡΙΕΧΟΜΕΝΟΥ» αν ήδη έχουμε ανοίξει να δούμε το ΣΥΝΗΜΜΕΝΟ), ΧΩΡΙΣ ΝΑ ΕΧΟΥΜΕ ΕΠΙΚΟΙΝΩΝΗΣΕΙ ΠΡΟΗΓΟΥΜΕΝΩΣ (με άλλον τρόπο, π.χ. τηλεφωνικά) με τον αποστολέα του email (για να βεβαιωθούμε πως δεν συμβαίνει κάτι ύποπτο και ερήμην του)*

Κλείνοντας, στην Πληροφορική Τεχνολογία μην ξεχνούμε γενικευμένα και διαχρονικά πως… «ότι κλειδώνει, ξεκλειδώνει»… Όλα τα ζητήματα Ασφάλειας και οι μορφές «επιθέσεων» διαρκώς μετασχηματίζονται και εξελίσσονται για να μας «αιφνιδιάσουν». Κρατούμε σε υψηλό βαθμό τις όποιες άμυνες των συσκευών μας αλλά και την εγρήγορσή μας, αξιολογώντας στοιχειωδώς τι λαμβάνουμε πριν προχωρήσουμε στα περαιτέρω. Δεν πρέπει να φοβόμαστε αλλά διαρκώς να προσέχουμε!

Βοηθητικές σχετιζόμενες Αναφορές: AVAST Academy (https://www.avast.com/c-trojan)

03/2022

© Παρασκευάς Γ. Παπαδόπουλος
Μηχανικός Η/Υ Συστημάτων, Η.Ι. (MSc)
Computer Systems Engineer, Η.Ι. (MSc)
Email: pdesper@gmail.com