Ασφάλεια στο διαδίκτυο

Ελευθερία Γιαμά

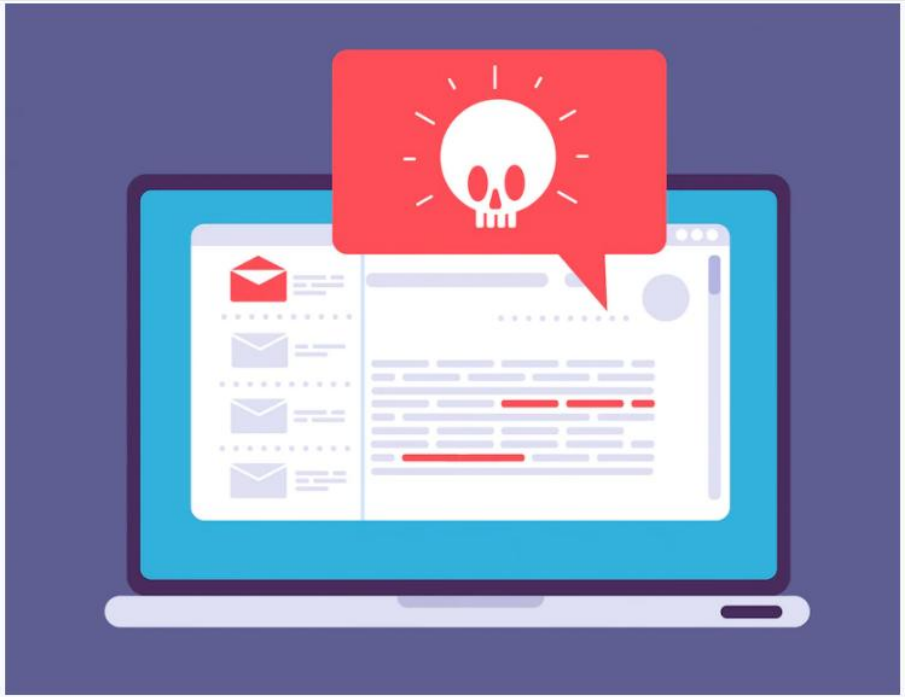
Intro

Σκοπός του παρακάτω μαθήματος είναι να σας παρουσιάσει τους διαφορετικούς τύπους κυβερνοεπιθέσεων που είναι πιθανό να στοχεύσουν τις ηλεκτρονικές σας συσκευές κατά την πλοήγηση σας στο διαδίκτυο. Μετά το τέλος του μαθήματος θα είστε σε θέση να τους εντοπίζετε με βάση τις διαφορές τους, αλλά και να λαμβάνετε τα κατάλληλα μέτρα έτσι ώστε να τους αντιμετωπίζετε

Συνήθεις κυβερνοεπιθέσεις

1. **Κακόβουλο λογισμικό**

Το κακόβουλο λογισμικό (malware) είναι δομημένο έτσι ώστε να βλάψει ένα υπολογιστικό σύστημα και να ανοίξει διόδους για την υποκλοπή και καταστροφή των δεδομένων του χρήστη.



Οι συνηθέστεροι τρόποι μετάδοσης ενός κακόβουλου λογισμικού, είναι:

- Τα συνημμένα αρχεία
- Παραβιασμένες ιστοσελίδες
- Συσκευές USB
- Πειρατικό λογισμικό

Βασικοί τύποι malware:

Ιός (virus)

Λογισμικό το οποίο μεταδίδεται μεταξύ των πληροφοριακών συστημάτων και εκτελείται μέσω της ανθρώπινης παρέμβασης μέσα από πειρατικά λογισμικά και γενικά εκτελέσιμα αρχεία. Μπορεί να αλλοιώσει, να κλέψει ή να διαγράψει τα δεδομένα του χρήστη.

Πώς καταλαβαίνουμε ότι έχουμε μολυνθεί:

- Ο υπολογιστής μας καθυστερεί αφύσικα να φορτώσει εφαρμογές
- Οι εφαρμογές καθυστερούν να εκτελεστούν
- Διακόπτεται η λειτουργία εφαρμογών ξαφνικά η οθόνη παγώνει και το λειτουργικό σύστημα μας ενημερώνει ότι ο υπολογιστής μας εμφανίζει το παρακάτω μήνυμα “Your computer has been recovered from a shutdown”
- Ο υπολογιστής μας ενημερώνει ότι ο χώρος στο δίσκο :C λιγοστεύει
- Μας εμφανίζονται ασυνήθιστα “warning” του συστήματος και ο υπολογιστής κλείνει απροσδόκητα
- Χάνουμε την πρόσβαση στον σκληρό δίσκο.
- Παρατηρούμε πολλά pop up windows να εμφανίζονται στην οθόνη μας

Worm

Κακόβουλο λογισμικό το οποίο αντιγράφει τον εαυτό του από τον έναν υπολογιστή στον άλλον χωρίς την ανθρώπινη παρέμβαση. Μεταδίδεται μέσα από επισυναπτόμενα αρχεία mail και μηνύματα σε social media

Πώς καταλαβαίνουμε ότι έχουμε μολυνθεί:

- Στέλνουμε ανεπιθύμητα μήνυματα μέσω κοινωνικής δικτύωσης ή mail σε άλλους χρήστες
- Ο browser μας ανακατευθύνει σε άλλες ιστοσελίδες μετά την εκκίνηση του

Rootkits

Κακόβουλο λογισμικό το οποίο επιτρέπει την πρόσβαση σε ένα υπολογιστικό σύστημα με δικαιώματα υπερχρήστη ενώ κρύβει την παρουσία του καθώς ενσωματώνεται σε βασικά αρχεία του λειτουργικού συστήματος ή άλλων εφαρμογών. Αποτελεί πόρτα εισόδου στην ουσία για υποκλοπή δεδομένων ή την καταστροφή του συστήματος.

Πώς καταλαβαίνουμε ότι έχουμε μολυνθεί:

- Είναι δύσκολο να εντοπιστεί από μόνο του. Συνήθως δρα συνδυαστικά με τα υπόλοιπα malware.

Δούρειος Ίππος (Trojan horse)

Κακόβουλο λογισμικό το οποίο μπορεί να αποθηκεύσει κωδικούς μέσω την καταγραφή της κίνησης του πληκτρολογίου ακόμη και να καταγράψει βίντεο μέσω της κάμερας. Συνήθως αποθηκεύεται στον υπολογιστή των θυμάτων μέσω πειρατικών λογισμικών.

Πώς καταλαβαίνουμε ότι έχουμε μολυνθεί:

- Παρατηρούμε να ανοίγει ξαφνικά η κάμερα ή άλλες εφαρμογές χωρίς να είναι αποτέλεσμα ενέργειας μας
- Παρατηρούμε φακέλους και αρχεία που δεν έχουμε δημιουργήσει εμείς
- Παρατηρούμε εφαρμογές-βοηθήματα στο toolbar τα οποία δεν έχουμε εγκαταστήσει εμείς
- Έχει αλλοιωθεί η αρχική σελίδα του browser μας με διαφημίσεις ή με ιστορικό το οποίο δεν έχουμε επισκεφθεί εμείς.
- Χάνουμε την πρόσβαση σε προσωπικούς μας λογαριασμούς γιατί έχει αλλαχθεί ο κωδικός.

Ransomware

Το ransomware είναι κακόβουλο λογισμικό που εγκαθίσταται κρυφά στο πληροφοριακό σύστημα, κρυπτογραφεί τα δεδομένα του θύματος και απαιτεί την καταβολή λύτρων για να τα αποκρυπτογραφήσει. Η καταβολή των λύτρων γίνεται κυρίως μέσω κρυπτονομισμάτων και η μετάδοση του συνήθως μέσω e-mail.

Παράδειγμα
https://articulateusercontent.com/rise/courses/IFXrL_8oQnNt_vDayJZbu83uB67WnaAQ/pEROtbhjqhiLGQs2/story.html

2. Επιθέσεις phising

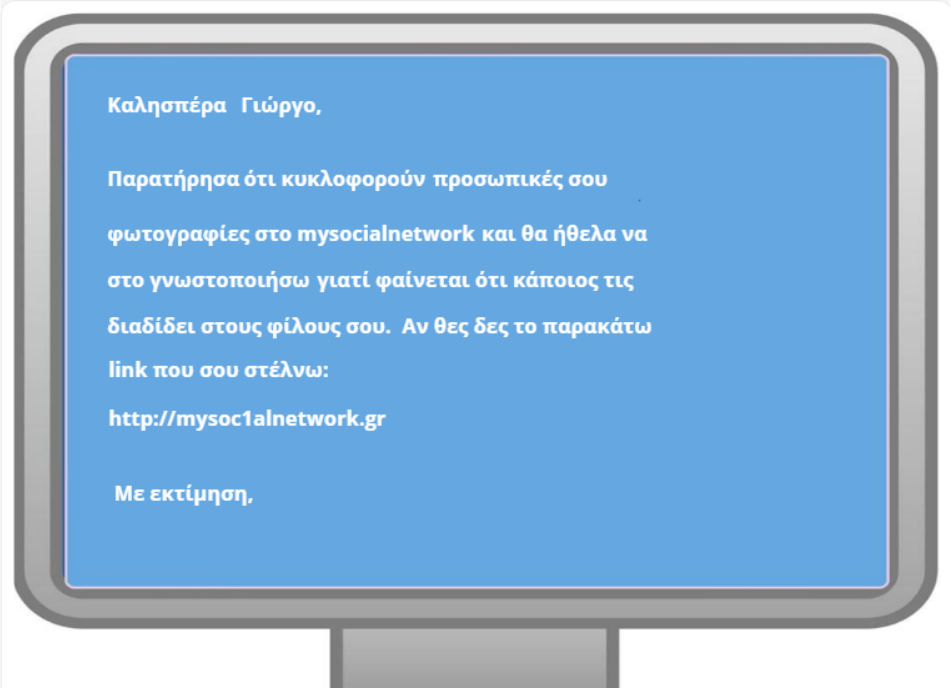
Δεν αποτελεί κακόβουλο λογισμικό αλλά τύπου κυβερνοεπίθεσης

Οι επιθέσεις phising στηρίζονται κυρίως στην:

- Έλλειψη προσοχής
- Έλλειψη γνώσεων
- Όπτικη εξαπάτηση

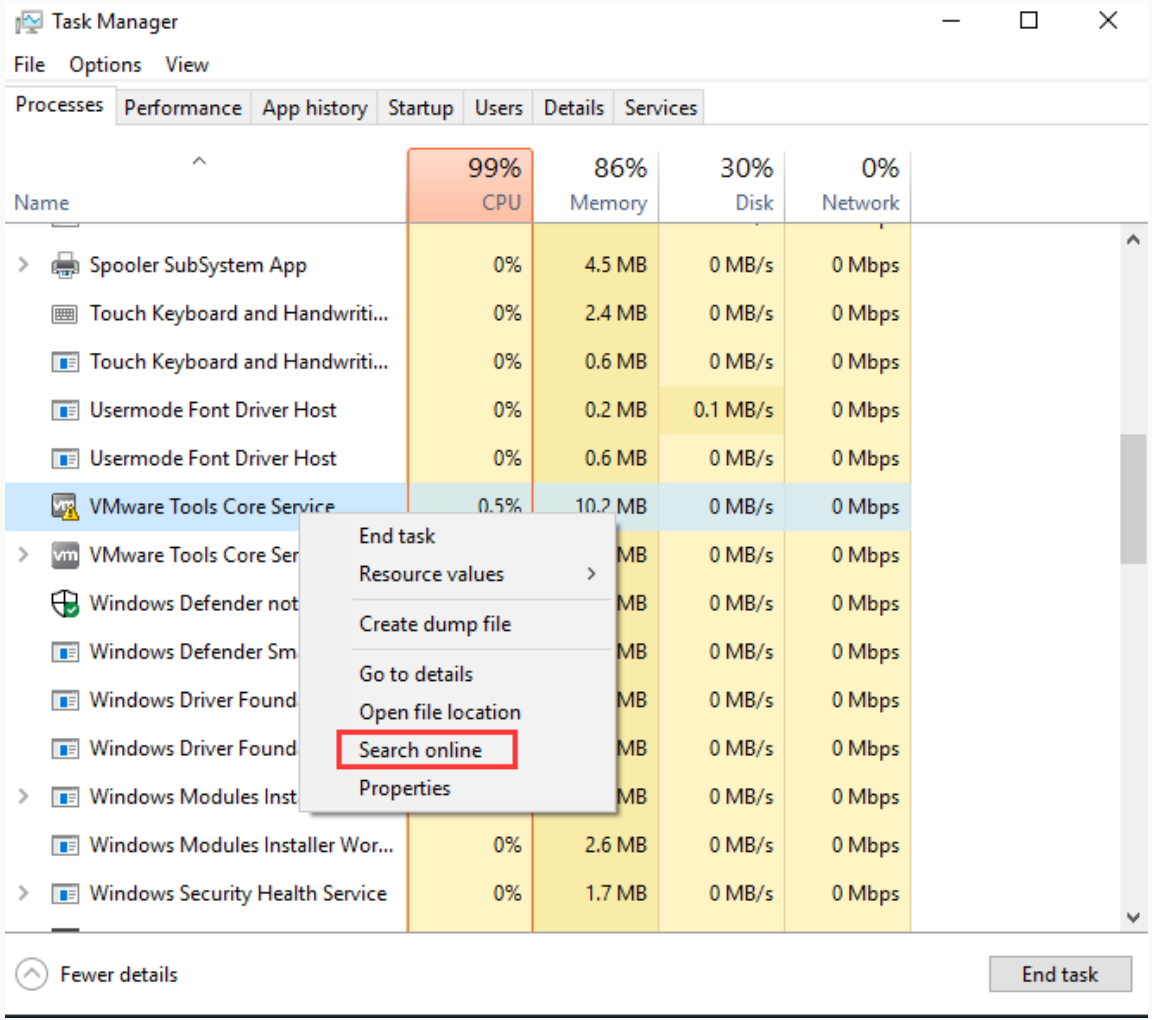
Παράδειγμα

Ένα ρεαλιστικό παράδειγμα είναι η αποστολή e-mail όπου ο κακόβουλος χρήστης έχει δημιουργήσει πανομοιότυπη ιστοσελίδα με το κοινωνικό δίκτυο mysocialnetwork.gr, έχει στην κατοχή του το όνομα ιστού mysoc1alnetwork.gr και αποστέλλει το εξής μήνυμα στο υποκείμενο με τυχαίο όνομα για την εξυπηρέτηση του παραδείγματος:



Έλεγχος της προστασίας των Windows

Έλεγχος του task manager για την εκτέλεση ύποπτων προγραμμάτων



Επαναχρησιμοποίη ση κωδικών

Ο επιτιθέμενος δημιουργεί ένα μοτίβο πληροφοριών για τα θύματα του, συλλέγοντας πληροφορίες από κοινωνικά δίκτυα όπως είναι:

- Ονοματεπώνυμο
- αγαπημένες ασχολίες
- αγαπημένο είδος μουσικής
- όνομα φίλων κ.τ.λ.

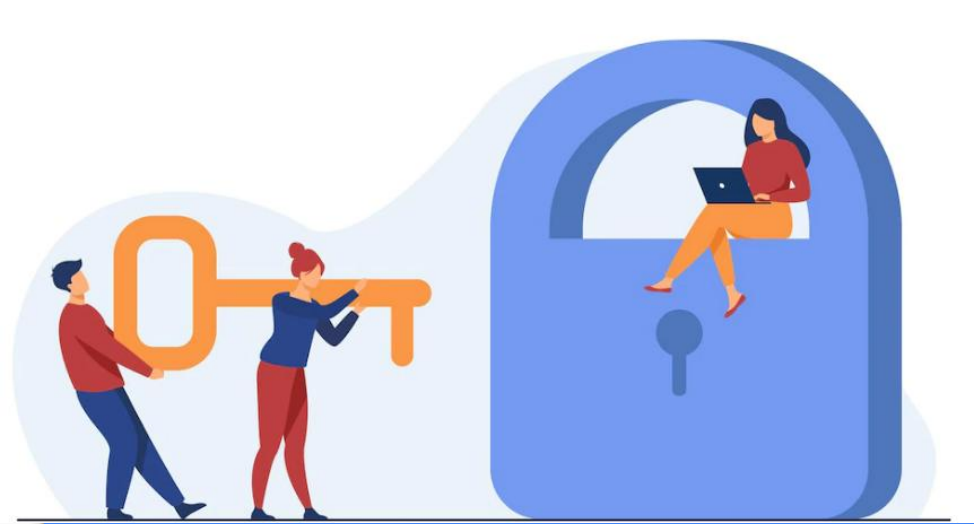
Πως προστατευόμαστε

Ισχυροί και διαφορετικοί κωδικοί

Οι κωδικοί αποτελούν το συνηθέστερο τρόπο αυθεντικοποίησης υποκειμένων στα πληροφοριακά συστήματα. Είναι ένα μέσο διατήρησης της ακεραιότητας και εμπιστευτικότητας των δεδομένων με αποτέλεσμα να χρήζει ιδιαίτερης σημασίας η πολυπλοκότητα και η συχνότητα αλλαγής του. Προτείνεται η αλλαγή κωδικών ανά τακτά χρονικά διαστήματα πχ. ανά δύο μήνες και η αποθήκευση των κωδικών σε λογισμικά διαχείρισης κωδικών (password managers).

Ενας ισχυρός κωδικός αποτελείται από τουλάχιστον 8 χαρακτήρες και συνθέτεται από οποιονδήποτε συνδυασμό χαρακτήρων, αριθμών και συμβόλων. Ενας ισχυρός κωδικός απαρτίζεται από:

- Κεφαλαία γράμματα όπως π.χ. A, D, K
- Μικρά γράμματα όπως π.χ. s,l,t
- Νούμερα όπως π.χ. 1,5,9
- Σύμβολα και ειδικοί χαρακτήρες όπως π.χ. $,(%?



Αλλοι τρόποι προστασίας

Εγκατάσταση αντιικού προγράμματος (anti - virus)

Ενημερώσεις προγραμμάτων

Αποφυγή εκτέλεσης συνημμένων μέσω μηνυμάτων ηλεκτρονικής αλληλογραφίας (E-mail attachments)/Σάρωση των αρχείων σε διαδικτυακές εφαρμογές όπως είναι το VirusTotal[1].

Εγκατάσταση τοίχους προστασίας (Firewall)

Εγκατάσταση συστήματος εισβολών (IDS) και αποτροπής εισβολών (IPS)

Κρυπτογράφηση δεδομένων με εφαρμογές του λειτουργικού συστήματος ή μέσω VPN

Ευχαριστώ πολύ

Ελευθερία Γιαμά

Ενδεικτική βιβλιογραφία:

“Τεχνικοοργανωτική έκθεση-Σύγχρονες απειλές στον Κυβερνοχώρο”, GDPR Greece, 2018

“Malware”, wikipedia (https://en.wikipedia.org/wiki/Malware)

“8 most common types of malware attack”, arcticwolf.com

“Token based authentication”, SafeNet.com

“Computer Security and Mobile Security Challenges”, researchgate.net

“Windows Security”, Microsoft.com