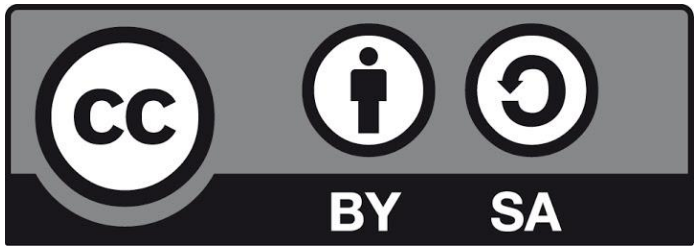
Κακόβουλο λογισμικό και αντιμετώπιση

Εισηγητής: Χρήστος Δαλαμάγκας
cdalamagkas@gmail.com

Άδεια χρήσης



Κακόβουλο λογισμικό (malware)

- **Ορισμός**: πρόγραμμα ή σύνολο προγραμμάτων που σκοπό έχει να προκαλέσει κακόβουλες βλάβες σε ένα σύστημα
- Το malware εκμεταλλεύεται αδυναμίες των υπολογιστικών συστημάτων
  - Hardware
  - Software
- Χωρίζεται σε δυο κατηγορίες:
  - «Φιλοξενείται» σε άλλο πρόγραμμα
  - Ανεξάρτητο

Είδη κακόβουλων λογισμικών

- **Ιός** (Virus): Προσαρτάται σε ένα πρόγραμμα και μεταδίδεται/αντιγράφεται αυτόματα σε άλλα προγράμματα ή αρχεία.
  - Ενσωματώνεται στην αρχή ή το τέλος ενός προγράμματος.
  - Αν εντοπίσει ένα αμόλυντο σύστημα, τότε αντιγράφεται και μεταδίδεται σε αυτό.
  - Μεταδίδεται και μέσω ηλεκτρονικού ταχυδρομείου.
  - Μπορεί να διαγράψει αρχεία ή να κατασπαταλήσει τους υπολογιστικούς πόρους.
- **Σκουλήκι** (worm): Μεταδίδεται δικτυακά σε άλλους υπολογιστές
  - Αυτόνομο, σε αντίθεση με τον ιό και δε χρειάζεται τη παρέμβαση του χρήστη για να εκτελεστεί.
  - Προκαλεί παρόμοιες βλάβες με τον ιό.
- **Δούρειος ίππος** (trojan horse): Πρόγραμμα που φαίνεται νόμιμο άλλα περιέχει μη αναμενόμενη και κακόβουλη λειτουργικότητα.

Είδη κακόβουλων λογισμικών

- **Λογική βόμβα** (logic bomb): Λογισμικό ενσωματωμένο σε πρόγραμμα που ενεργοποιείται υπό συνθήκες.
- **Κερκόπορτα** (backdoor): Πρόγραμμα που δίνει πρόσβαση σε άλλο κακόβουλο λογισμικό ή χρήστη.
- **Exploit**: Προγράμματα που εκμεταλλεύονται συγκεκριμένες αδυναμίες λογισμικού ή υλικού.
- **Spammer**: Λογισμικό που στέλνει αυτόματα μεγάλο όγκο μηνυμάτων ηλεκτρονικού ταχυδρομείου.

Είδη κακόβουλων λογισμικών

- **Flooder**: Λογισμικό που πλημυρίζει ένα δίκτυο ή υπολογιστή με πακέτα, με σκοπό να καταρρεύσει.
  - Συνήθως διεξάγουν επιθέσεις DoS (Denial of Service)
- **Keylogger**: Συσκευή ή πρόγραμμα που καταγράφει τη χρήση του πληκτρολογίου.
- **Rootkit**: Λογισμικό που στοχεύει στην απόκτηση δικαιωμάτων root.
- **Zombie**: Πρόγραμμα-ζόμπι που ελέγχεται από άλλους υπολογιστές και διεξάγει επιθέσεις.

Μέτρα αντιμετώπισης

- **Αποτροπή εισόδου**
  - Μπλοκάρισμα όλων των θυρών στο firewall που δε χρησιμοποιούνται.
  - Ισχυροί και μη κοινοί κωδικοί πρόσβασης, ώστε να μην παραβιαστούν από λεξικογραφική επίθεση
- **Αντιβιοτικά** (antivirus/antimalware): Προγράμματα που ανιχνεύουν, απομονώνουν και καταστρέφουν προγράμματα που έχουν ή ενδέχεται να έχουν κακόβουλη δραστηριότητα
  - Πρώτη γενιά: Αναζήτηση με βάση την υπογραφή (hash) του ιού
  - Δεύτερη γενιά: Ευρετικοί κανόνες (αναζήτηση βρόχων κρυπτογράφησης, έλεγχος ακεραιότητας, έλεγχος αθροίσματος ελέγχου κ.α.)
  - Τρίτη γενιά: Αναγνώριση από τις ενέργειες και όχι από τη δομή τους
  - Προσομοίωση εκτέλεσης του υπό εξέταση προγράμματος στη CPU

Γνωστά αντιβιοτικά

- Για Windows
  - **Immunet** (open-source)
  - Bitdefender
  - Malwarebytes
  - Windows Defender (free)
  - Norton
- Για Linux
  - **Clam AntiVirus** (open-source)
  - Kaspersky Lab
  - ESET