Μορφές Κακόβουλου Κώδικα (Malicious Code)

Υποπλοίαρχος Ν. Πετράκος ΠΝ

Ατζέντα

- Δούρειοι Ίπποι (Trojan Horses)
- Ιοί (Viruses)
- Worms
- Root-kit

Δούρειος Ίππος (Trojan Horse)

- Ορισμός: Πρόγραμμα το οποίο είναι χρήσιμο , αλλά περιέχει επιπλέον κρυφές κακόβουλες δυνατότητες οι οποίες του επιτρέπουν να αποκαλύπτει τις αδυναμίες ενός υπολογιστικού συστήματος ή ακόμα και να επιτυγχάνει μη εξουσιοδοτημένη πρόσβαση σε ένα σύστημα

Δούρειος Ίππος (Trojan Horse)

- Εγκαθίσταται κατά την δημιουργία ενός προγράμματος
- Δύναται να εγκατασταθεί μετά τη δημιουργία ενός προγράμματος
  - π.χ. σ' ένα αντίγραφο του AdobeReader θα μπορούσε να τοποθετηθεί Trojan Horse

Δούρειος Ίππος (Trojan Horse)

- Αποτελεί σπουδαιότερη απειλή από τον ιό καθώς δύσκολα εντοπίζεται και δεν κάνει αισθητή την παρουσία του
- Μπορεί να παραμείνει κρυφό για πάντα
- Μπορεί να είναι προγραμματισμένο να εκτελέσει συγκεκριμένη εργασία ή να είναι τηλεχειριζόμενο
- Δεν χρειάζεται να τροποποιήσει ένα πρόγραμμα ή να αναπαραχθεί ώστε να εξαπλωθεί, καθώς είναι ένα πρόγραμμα το οποίο χρησιμοποιεί το δίκτυο, ψάχνει στα υπολογιστικά συστήματα για αδυναμίες οι οποίες θα του επιτρέψουν να εξαπλωθεί ταχύτατα

Δούρειος Ίππος (Trojan Horse)

- Αντιμετώπιση του Δούρειου Ίππου
  - Εγκατάσταση μόνο έμπιστων (trustworthy) προγραμμάτων
  - Χρησιμοποίηση Λειτουργικού Συστήματος (Λ.Σ.) το οποίο να υποστηρίζει Mandatory Access Control (MAC) policy
  - Χρησιμοποίηση Antivirus

Ιοί (Viruses)

- Ορισμός: Αυτόνομο εκτελέσιμο πρόγραμμα/μικρή εφαρμογή το οποίο εγκαθίσταται χωρίς τη θέληση του χρήστη, ερευνά για άλλα προγράμματα, τα οποία «μολύνει» με την ενσωμάτωση σε αυτά αντίγραφο του εαυτού του. Όταν το μολυσμένο πρόγραμμα εκτελείται, ο ενσωματωμένος ιός ενεργοποιείται, και έτσι μεταδίδεται

Ιοί (Viruses)

- Μέθοδοι ενεργοποίησης ιού

Μέσο Διάδοσης Ιού	Ενεργοποίηση Ιού
Προγράμματα	Εκτελώντας το πρόγραμμα
Word Macros	Ανοίγοντας ένα έγγραφο
E-mail	Ανοίγοντας ένα συνημμένο

Ιοί (Viruses)

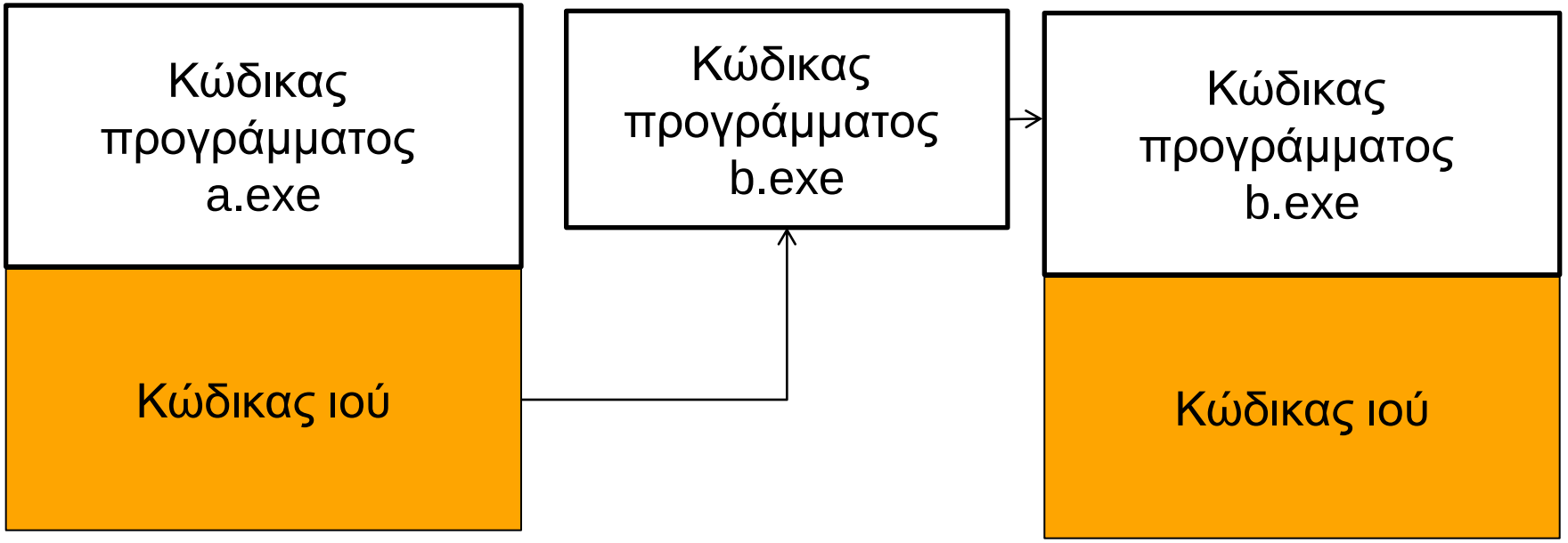
- Διάδοση προγράμματος – Ιού
  - Εκτελώντας ένα μολυσμένο πρόγραμμα (π.χ. a.exe)

  αυτό μολύνει άλλα προγράμματα ως ακολούθως:

  - ερευνώντας το σύστημα για αρχεία τα οποία δύναται να μολυνθούν (π.χ. *.exe) και
  - αντιγράφοντας το κώδικα- ιό σε αυτά

Ιοί (Viruses)

- Παράδειγμα
  - Το μολυσμένο πρόγραμμα a.exe μολύνει το πρόγραμμα b.exe



Ιοί (Viruses)

- Προφυλάξεις:
  - Προσοχή όταν ανοίγουμε αρχεία ή τρέχουμε εφαρμογές
  - Χρησιμοποίηση antivirus για το οποίο
    - φροντίζουμε να έχει επικαιροποιημένη τη βιβλιοθήκη του με αυτόματη ενημέρωση ή users update
    - Ρυθμίζουμε κατάλληλα το configuration: τι αρχεία να σκανάρουμε, πόσο συχνά να σκανάρουμε τους δίσκους

Worms

- Ορισμός: Αυτόνομο πρόγραμμα το οποίο δύναται να εξαπλωθεί μόνο του από ένα σύστημα σε ένα άλλο
- Είναι προγράμματα τα οποία :

  - Εισβάλουν σ' ένα σύστημα, αντιγράφουν τον εαυτό τους στο σύστημα και από εκεί εισβάλουν σε άλλα συστήματα
- Διαδίδονται χωρίς τη βοήθεια του χρήστη

Worms

- Είναι πιο επικίνδυνα από τους ιούς, καθώς εξαπλώνονται πιο γρήγορα

- Το worm Slammer (2003) εξαπλώθηκε σε 75000 συστήματα μέσα σε 10 λεπτά

Worms

- Προφυλάξεις:
  - Εγκαθιστώντας όλα τα patches
  - Απενεργοποιώντας όλες τις μη απαιτούμενες εφαρμογές
  - Χρησιμοποίηση Antivirus (worm detectors)

Rootkit

- Τα rootkits είναι εργαλεία τα οποία ο επιτιθέμενος εγκαθιστά σε ένα σύστημα-θύμα και εκτελούν διάφορες λειτουργίες προς όφελός του
- Ο επιτιθέμενος πρέπει προηγουμένως να έχει αποκτήσει πρόσβαση στο σύστημα-θύμα έτσι ώστε να μπορέσει να εγκαταστήσει ένα **rootkit**
- Ένα **rootkit** είναι ένα σύνολο προγραμμάτων τα οποία επιτρέπουν στον επιτιθέμενο π.χ. να συλλέγει κωδικούς από το θύμα, να βλέπει τα πακέτα που κινούνται από και προς το θύμα , να αφήσει ένα backdoor το οποίο θα του επιτρέψει μελλοντική πρόσβαση στο σύστημα-θύμα, διατηρώντας έτσι τα δικαιώματα που είχε προηγουμένως αποκτήσει
- Παράλληλα διατηρεί κρυφή την παρουσία του
- Βρίσκονται χαμηλά και εγγύς στον πυρήνα του Λ.Σ. και είναι δύσκολο να εντοπιστούν και να αντιμετωπισθούν