ΕΥΑΓΓΕΛΟΣ Χ. ΖΙΟΥΛΑΣ
Καθηγητής Πληροφορικής

VCZ

ΚΕΦΑΛΑΙΟ 7

ΠΡΟΣΤΑΣΙΑ ΛΟΓΙΣΜΙΚΟΥ

http://www.zioulas.gr vczioulas@yahoo.com

ΓΕΝΙΚΑ

- Σε ένα υπολογιστικό σύστημα, η αποθήκευση των αρχείων σε μία μονάδα αποθήκευσης (π.χ. σκληρός δίσκος) δεν είναι πάντα ασφαλής.
- Υπάρχει πάντα η **πιθανότητα απώλειας ή καταστροφής** των αρχείων και φακέλων μας για λόγους που οφείλονται στον ίδιο τον χρήστη ή και σε εξωγενείς παράγοντες.

ΠΙΘΑΝΕΣ ΑΙΤΙΕΣ ΚΑΤΑΣΤΡΟΦΩΝ

(Α) ΒΛΑΒΕΣ ΑΠΟΘΗΚΕΥΤΙΚΩΝ ΜΕΣΩΝ

- Πιθανή βλάβη σε κάποια περιφερειακή συσκευή (π.χ. δίσκος καμμένος, απομαγνητισμένος κλπ) καθιστά πλέον αδύνατη την προσπέλαση των αρχείων και των φακέλων του.

(Β) ΙΟΙ ΥΠΟΛΟΓΙΣΤΩΝ (Computer Viruses)

- Είναι προγράμματα που φτιάχνονται από κακόβουλους προγραμματιστές, τα οποία δημιουργούν προβλήματα στην ομαλή λειτουργία του υπολογιστή.
- **Ιός είναι ένα πρόγραμμα που προσκολλάται σε ένα άλλο πρόγραμμα και** όταν αυτό ενεργοποιείται, ο ιός αρχίζει και **δρα αθόρυβα.**
- **Κάθε χρόνο εμφανίζεται ένας μεγάλος αριθμός καινούργιων ιών.**

Πρώτος Ιος εμφανίστηκε το **1986**, ενώ εως σήμερα έχουν κατασκευαστεί περίπου **150.000** κακόβουλα προγράμματα.

- **Πιθανά προβλήματα** που προκαλεί ένας ιός είναι τα εξής
  - **Διαγραφή δεδομένων** του σκληρού δίσκου
  - **Επιβράδυνση ταχύτητας** επεξεργασίας του υπολογιστή
  - **Εμφάνιση** ενοχλητικών **μηνυμάτων** στην οθόνη
  - **Αδικαιολόγητη επανεκκίνηση** του συστήματος
  - **Προβληματική λειτουργία** του Λειτουργικού Συστήματος

- Ο Ιος μπορεί να μεταδοθεί στον Η/Υ με δύο κυρίως τρόπους:
  - **Εξωτερικά μέσα αποθήκευσης** (δισκέτες, cd, dvd, flash memory, εξωτερικοί δίσκοι, κάρτες μνήμης).
  - **Δίκτυα Υπολογιστών** και **Ιντερνετ** (Ιστοσελίδες, Instant Messenger, Emails)
- Υπάρχουν σήμερα πολλές κατηγορίες κακόβουλων προγραμμάτων (**malware**).

Computer Worms	Είναι προγράμματα που **πολλαπλασιάζονται** από μόνα τους, δηλαδή **δημιουργούν πολλά αντίγραφα** του εαυτού τους που μεταδίδονται μέσω του δικτύου από σταθμό σε σταθμό προκαλώντας σημαντικές καθυστερήσεις. Σε αντίθεση με τους ιούς, **τα Worms δεν προσκωλλόνται σε άλλα προγράμματα.**
Trojan Horses	Είναι κακόβουλα προγράμματα που ξεγελάνε τον χρήστη. Εξωτερικά **δείχνουν ακίνδυνα** κάνοντάς τον να πιστεύει ότι εκτελεί κάποια χρήσιμη λειτουργία (π.χ. pc-game) ενώ στα κρυφά εγκαθίσταται στον υπολογιστή **κώδικας επιβλαβής** που μολύνει τον υπολογιστή. Η μόλυνση από Trojan μπορεί να επιτρέψει σε **μη εξουσιοδοτημένους χρήστες** να έχουν πρόσβαση στον μολυσμένο υπολογιστή, ή ακόμα και να οδηγήσει στην ολική διαγραφή του σκληρού δίσκου. Σε αντίθεση με τους ιούς, **οι Trojans δεν μεταδίδονται μολύνοντας αρχεία**.

Ευάγγελος Χρ. Ζιούλας *(Καθηγητής Πληροφορικής)*

Malware	Ονομάζεται το κακόβουλο λογισμικό που είναι **επιβλαβές** για την ασφάλεια κάθε πληροφοριακού συστήματος (viruses, worms, trojans).
Adware	Κακόβουλα προγράμματα, που ενώ είναι ακίνδυνα, γεμίζουν με **διαφημίσεις** και ενοχλητικά μηνύματα την οθόνη του υπολογιστή.
Spyware	Προγράμματα που δρουν στο παρασκήνιο και συλλέγουν προσωπικές πληροφορίες που πληκτρολογεί ο χρήστης π.χ. passwords, κωδικούς καρτών.
Crimeware	Λογισμικό που επιτρέπει σε μη εξουσιοδοτημένους χρήστες να έχουν **πρόσβαση** σε λογαριασμούς για **ηλεκτρονικές αγορές** και **οικονομικές συναλλαγές**, με σκοπό να κλέβουν χρήματα ή να κάνουν παράνομες συναλλαγές.
Dialer	Κακόβουλο λογισμικό που δημιουργεί στο Ιντερνετ τηλεφωνικές συνδέσεις χωρίς να το γνωρίζει ο χρήστης. Ο πάροχος (provider) του συγκεκριμένου προγράμματος αναγκάζει τον χρήστη να κάνει **τηλεφωνήματα** μέσω ειδικών **αριθμών υψηλής χρέωσης** με σκοπό να κερδίσει χρήματα.
Dropper	Πρόγραμμα σχεδιασμένο να εγκαθιστά κακόβουλο λογισμικό είτε περιέχοντας επιβλαβή κώδικα ικανό να μην ανιχνεύεται από τα αντιϊικά προγράμματα, είτε **κατεβάζοντας** (download) **κακόβουλο λογισμικό** στον υπολογιστή του χρήστη όταν ενεργοποιηθεί.
Rootkits	Τεχνικές που επιτρέπουν σε κακόβουλο λογισμικό που εγκαθίσταται στον υπολογιστή, να **παραμένει κρυφό** και να **αποφεύγει την ανίχνευσή του** από τα αντιϊικά προγράμματα. Στην ουσία ρυθμίζουν το λειτουργικό σύστημα ώστε το κακόβουλο λογισμικό να παραμένει κρυφό από τον χρήστη και να μην μπορεί να διαβαστεί.
Backdoors	Μέθοδοι με τις οποίες οι μη εξουσιοδοτημένοι χρήστες **παρακάμπτουν** τις συνήθεις **διαδικασίες ελέγχου ταυτότητας**. Όταν το σύστημα παραβιάζεται, μια ή περισσότερες backdoors εγκαθίστανται στον υπολογιστή ώστε να επιτρέψουν την εύκολη είσοδο των κακόβουλων χρηστών στο μέλλον.
Hijackers	Λογισμικό που **αποκτά τον έλεγχο** ενός φυλλομετρητή (**web browser**), π.χ. της αρχικής σελίδας, των γραμμής αναζήτησης, των μηχανών αναζήτησης κλπ. Μπορεί επίσης να κατευθύνει την αναζήτηση του χρήστη σε συγκεκριμένες ιστοσελίδες ή να του απαγορεύει την επίσκεψη σε άλλες ιστοσελίδες όπως αυτές με περιεχόμενα εφαρμογών καταπολέμησης ιών.

(Γ) <u>ΚΑΚΟΣ ΧΕΙΡΙΣΜΟΣ ΤΟΥ ΧΡΗΣΤΗ</u>

- Συχνά ο ίδιος ο χρήστης μπορεί να **διαγράψει** ή να **απεγκαταστήσει κατά λάθος** κάποια προγράμματα του Η/Υ.
- Ένας σημαντικός παράγοντας κινδύνου είναι και η **κακή συντήρηση** του Η/Υ από τον χρήστη όπως:
  - Έκθεση σε υγρασία, ζέστη ή σκόνη
  - Ατυχείς ενέργειες (ρίψη νερού – αναψυκτικών στο πληκτρολόγιο)
  - Κακός χειρισμός (νευρικές ενέργειες και απότομες κινήσεις όταν ο Η/Υ είναι ανοικτός)
- Ο υπολογιστής όπως και όλες οι μηχανές χρειάζεται καλή συντήρηση. Χωρίς συντήρηση μπορεί εύκολα να αποτύχει. Η σκόνη ή η βρωμιά μπορούν να οδηγήσουν σε σοβαρά προβλήματα όπως χαμηλή ταχύτητα, πάγωμα οθόνης, εμφάνιση μηνυμάτων, και αδικαιολόγητες επανεκκινήσεις.

- Συχνά οι χρήστες δεν το καταλαβαίνουν αυτό και προστρέχουν σε τεχνικούς. Ωστόσο το πρόβλημα παραμένει στη φτωχή συστήρηση του προσωπικού τους υπολογιστή.
- Ο χρήστης πρέπει να κάνει συχνά έλεγχο στον υπολογιστή του και να γνωρίζει τα βασικά του χαρακτηριστικά (π.χ. τύπο επεξεργαστή, κύρια μνήμη, χωρητικότητα σκληρού δίσκου, έκδοση λειτουργικού συστήματος κλπ) διότι έτσι θα είναι ικανός να λύνει άμεσα προβλήματα.

(Δ) ΕΙΣΒΟΛΗ ΑΝΕΠΙΘΥΜΗΤΩΝ ΣΤΟΝ Η/Υ

- Με την σύνδεση των υπολογιστών στο Ιντερνετ, τα δεδομένα τους γίνονται ευάλωτα στις **επιθέσεις μη εξουσιοδοτημάνων προγραμματιστών** που ονομάζονται **Hackers** (ή **Crackers** αν είναι κακόβουλοι).
- Οι hackers αποκτώντας πρόσβαση στους υπολογιστές μας, μπορούν να αλλοιώσουν, να διαγράψουν ή και να υποκλέψουν τα δεδομένα μας, πράγμα που αποτελεί **ηλεκτρονικό έγκλημα** και τιμωρείται από το νόμο.

ΑΝΤΙΓΡΑΦΑ ΑΣΦΑΛΕΙΑΣ

Back-Up Files

Η **αντιγραφή των εργασιών** μας σε ένα δεύτερο αποθηκευτικό μέσο (π.χ. cd, dvd, flash memory, εξωτερικό σκληρό δίσκο) μας προφυλάσσει από την ενδεχόμενη απώλειά τους.

Σε τακτά χρονικά διαστήματα πρέπει να χρησιμοποιούμε το κατάλληλο **βοηθητικό πρόγραμμα (utility)** δημιουργίας back-up για την αποθήκευση της τελευταίας έκδοσης (versions) των αρχείων ως εξής:

Win XP *Εναρξη → Προγράμματα → Βοηθήματα → Εργαλεία Συστήματος → Αντίγραφα Ασφαλείας*
Win 7 *Έναρξη → Προγράμματα → Συντήρηση → Αντίγραφα ασφαλείας*

ΤΡΟΠΟΙ ΠΡΟΣΤΑΣΙΑΣ ΑΠΟ ΙΟΥΣ

1. **Προσοχή στα προγράμματα που τρέχουμε** στον Η/Υ (κυρίως όταν δεν προέρχονται από τον κατασκευαστή ή δεν τα έχουμε προμηθευτεί από το εμπόριο).
2. **Εγκαστάσταση Antivirus** και **Internet Security** προγραμμάτων που μας προστατεύουν από τους περισσότερους ιούς (π.χ. Norton, Panda, McAfee, Kaspersky, ZoneAlarm).
3. Ανανέωση προγραμμάτων μέσω **ενημέρωσης (Update)** σε τακτά διαστήματα με όλους τους καινούργιους ιούς που έχουν στο μεταξύ προκύψει.
4. Ενεργοποίηση **Τείχους Προστασίας (Firewall)** κάθε φορά που συνδεόμαστε στο Διαδίκτυο, ώστε να αποτρέπουμε τους ανεπιθύμητους από το να εισβάλουν στον υπολογιστή μας.

Win XP *Έναρξη → Ρυθμίσεις → Πίνακας Ελέγχου → Τοίχος Προστασίας*
Win 7 *Έναρξη → Πίνακας Ελέγχου → Σύστημα & Ασφάλεια → Τοίχος προστασίας*