χρήσιμου προγράμματος ή παιχνιδιού. Με την εκτέλεση του μολυσμένου αρχείου (του Δούρειου ίππου - trojan) το οποίο έχει μέσα του δυο προγράμματα, το χρήσιμο και το Trojan, εγκαθίστανται και τα δυο και το χρήσιμο εκτελείται κανονικά.

4. **Viruses:** ο προορισμός τους καθορίζεται από τον δημιουργό τους. Μπορεί να είναι ακίνδυνοι αλλά και επιβλαβής για συστήματα και χρήστες. Μεταδίδονται μέσω της εκτέλεσης των αρχείων στα οποία έχουν προσκολληθεί σε άλλα υγιή αρχεία.
5. **Worms:** μπορούν να στέλνουν προσωπικά δεδομένα στους δημιουργούς τους. Μεταδίδονται μέσω δικτύων και ηλεκτρονικών μηνυμάτων (emails) και επιβαρύνουν την κίνηση του δικτύου
6. **Backdoor:** με τις Κερκόπορτες ο δημιουργός τους αποκτά κανάλι επικοινωνίας με τον Η/Υ όπου εγκαταστάθηκε και μπορεί να εκτελέσει εντολές σε αυτόν όποτε θελήσει. Συνήθως εισχωρούν με την βοήθεια Trojan.
7. **Botnet:** είναι το δίκτυο από Bots, δηλαδή τους Η/Υ θύματα με το κακόβουλο λογισμικό. Η εγκατάσταση του λογισμικού γίνεται συνήθως από φυλλομετρητές, από Trojan και από συνημμένα ηλεκτρονικών μηνυμάτων (email attachments). Το δίκτυο των Η/Υ θυμάτων μπορεί και ελέγχεται κεντρικά μέσω πρωτοκόλλων όπως το IRC, HTTP και συχνά χρησιμοποιείται για επιθέσεις Άρνησης Υπηρεσιών (Denial of Services).
8. **Rootkit:** είναι ένα πολύ δύσκολα εντοπιζόμενο κακόβουλο λογισμικό που συνήθως καλύπτει άλλα κακόβουλα λογισμικά όπως τα Backdoors.

### 5.3.2 Λογισμικό Προστασίας από Κακόβουλο Λογισμικό (Antivirus).

Η χρήση των Η/Υ σε ολοένα και περισσότερες δραστηριότητες στο διαδίκτυο, η χρήση φορητών μέσων αποθήκευσης και οι συνεχώς αυξανόμενες απειλές σ' αυτό έχουν κάνει απαραίτητη τη χρήση προγραμμάτων προστασίας (antivirus) από κακόβουλα λογισμικά. Η προσβολή συστημάτων εντός ενός οργανισμού μπορεί να προκαλέσει προβλήματα στις Βασικές Αρχές ασφαλείας, τριάδα ΕΑΔ, Εμπιστευτικότητα, Ακεραιότητα και Διαθεσιμότητα.

Αν και η απόλυτη προστασία είναι σχεδόν αδύνατο να επιτευχθεί, θα πρέπει να επιδιώκεται η καλύτερη δυνατή. Υπάρχουν πολλά προγράμματα που προσφέρουν ικανοποιητική προστασία και τα οποία με μικρό αντίτιμο, ως προς αυτά που προσφέρουν, μπορούν να εγκατασταθούν στα συστήματα. Η επιλογή των προγραμμάτων αυτών δεν θα πρέπει να γίνεται βάσει φημών από φίλους και γνωστούς, αλλά με κριτήρια, όπως τις δυνατότητες προστασίας που προσφέρει αλλά και τις δυνατότητες του συστήματος που θα εγκατασταθεί. Ενδεικτικά θα πρέπει να έχει τις εξής δυνατότητες:

- Ανίχνευση όλων των ειδών κακόβουλων λογισμικών
- Ανίχνευση συμπιεσμένων αρχείων
- Αυτόματη ανίχνευση USB συσκευών
- Προστασία των ηλεκτρονικών μηνυμάτων και άμεσων μηνυμάτων

Πέρα της επιλογής του κατάλληλου προγράμματος προστασίας θα πρέπει στη συνέχεια να γίνουν και οι σωστές ρυθμίσεις του:

- Αυτόματη ενημέρωση της βάσης του και του προγράμματος
- Ενεργοποίηση των δυνατοτήτων του προγράμματος προστασίας
- Τακτικό πλήρη έλεγχο του συστήματος
- Προστασία των ρυθμίσεων με κωδικό

**5.3.3 Ενημερώσεις (Updates) Λειτουργικών Συστημάτων και Εφαρμογών.** Είναι σύνηθες να υπάρχει σ' ένα Πληροφοριακό Σύστημα και λογισμικό που αναπτύσσεται εντός του οργανισμού για τις δικές του εξειδικευμένες ανάγκες. Το λογισμικό αυτό αλλά και οι ενημερώσεις του απαιτούν εντατικούς ελέγχους σε απομονωμένο περιβάλλον από το τμήμα για το οποίο προορίζεται, προκειμένου να προστατευτεί το Πληροφοριακό Σύστημα.

Εκτός του εσωτερικά αναπτυγμένου λογισμικού υπάρχει και λογισμικό του εμπορίου. Το λογισμικό αυτό, συνήθως, υπάρχει διαθέσιμο στις ιστοσελίδες των εταιριών που το παράγουν και αυτό διευκολύνει κακόβουλες ομάδες στο να μελετήσουν και να εντοπίσουν κενά ασφαλείας του, ώστε μέσω αυτών να επιτεθούν στους χρήστες του λογισμικού.

Ένα από τα συνηθέστερα προγράμματα που γίνεται στόχος επιθέσεων είναι οι φυλλομετρητές ιστοσελίδων (web browsers) και διάφορα πρόσθετα που χρησιμοποιούν αυτοί για προβολή βίντεο, παιχνίδια αλλά και για εκτέλεση web εφαρμογών. Οι εταιρείες παραγωγής λογισμικού εκδίδουν συχνά ενημερώσεις των προγραμμάτων τους, για να επιδιορθώσουν διάφορα προβλήματα, μεταξύ των οποίων και κενά ασφαλείας. Για διευκόλυνση έχουν ενσωματωμένο έλεγχο για ενημερώσεις και εγκατάστασή τους και μπορεί να ελεγχθεί εύκολα αυτό από τις ρυθμίσεις του κάθε προγράμματος.

Στόχος επιθέσεων γίνονται και τα Λειτουργικά Συστήματα. Επιβεβλημένος για την προστασία του είναι ο αυτόματος έλεγχος για ενημερώσεις του και η εφαρμογή τους σχεδόν σε όλα στα συστήματα. Στα κρίσιμα συστήματα πρώτα θα πρέπει να γίνεται έλεγχος για το πώς θα τα επηρεάσουν οι ενημερώσεις πριν εγκατασταθούν, προκειμένου να αποφευχθούν προβλήματα διαθεσιμότητάς τους.

Σημαντικότατος είναι και ο ρόλος των χρηστών στην έκθεση συστημάτων σε απειλές. **Επιβάλλεται** οι χρήστες να συνδέονται στα συστήματα με λογαριασμούς **περιορισμένων δικαιωμάτων** (τυπικού χρήστη – typical user). Σε περιπτώσεις συνδέσεως με πλήρη δικαιώματα (διαχειριστή – Administrator για Windows ή root για Linux) είναι ιδιαίτερα επικίνδυνη η προσβολή από κακόβουλο λογισμικό γιατί αυτό θα μπορεί να επηρεάσει πολύ σοβαρότερα ένα σύστημα από ότι εάν είχε γίνει σε απλού χρήστη σύνδεση.

**5.3.4 Κρυπτογραφία (Cryptography).**

Η κρυπτογραφία μελετά τρόπους εξασφάλισης της εμπιστευτικότητας στην επικοινωνία δυο πλευρών.

Χρήσιμη ορολογία στην κρυπτογραφία είναι η παρακάτω:

- **Κρυπτογράφηση** (Encryption): Η διαδικασία μετασχηματισμού του μηνύματος από το αρχικό μήνυμα στο τελικό μη αναγνώσιμο
- **Αποκρυπτογράφηση** (Decryption): η αντίστροφη διαδικασία της κρυπτογράφησης