Κακόβουλο Λογισμικό

Project A’1

Ορισμός

ο «**κακόβουλο λογισμικό**», «**επιβλαβές λογισμικό**» (malicious software / malware) αποτελεί μείζον πρόβλημα για την ασφάλεια των Πληροφοριακών Συστημάτων. Το λογισμικό χαρακτηρίζεται ως *κακόβουλο* όταν βάσει των προθέσεων του προγραμματιστή το λογισμικό που προκύπτει διαθέτει τις απαιτούμενες εντολές προκειμένου να βλάψει ένα υπολογιστικό σύστημα. Το κακόβουλο λογισμικό μπορεί να χωριστεί σε δύο κατηγορίες. Σε αυτό που χρειάζεται ένα πρόγραμμα *«ξενιστή»* και σε αυτό που δεν χρειάζεται *«ξενιστή»* και μπορεί να εκτελεστεί από μόνο του όπως κάθε άλλο πρόγραμμα.

Επιπλέον το κακόβουλο λογισμικό μπορεί να διαχωριστεί και με διαφορετικό τρόπο σε δύο άλλες κατηγορίες. Το *ιομορφικό λογισμικό* και το *μη ιομορφικό λογισμικό*. Στο ιομορφικό λογισμικό ανήκουν τα προγράμματα που μπορούν και αναπαράγονται από μόνα τους και στο μη ιομορφικό λογισμικό τα προγράμματα που δεν αναπαράγονται χωρίς την ανάμειξη του ανθρώπινου παράγοντα

Είδη κακόβουλου λογισμικού

- Ιός (Virus): είναι κακόβουλο λογισμικό το οποίο έχει τη δυνατότητα να εξαπλώνεται εύκολα σε χρήσιμα προγράμματα ενός ξένου υπολογιστή με αποτέλεσμα να βλάψει χρήσιμα αρχεία ενός χρήστη. Η μετάδοσή του σε άλλους υπολογιστές μπορεί να γίνει πολύ εύκολα με τη βοήθεια κάποιας εξωτερικής συσκευής όπως μια φορητή μνήμη USB ή ένας εξωτερικός σκληρός δίσκος. Ένα στοιχείο που διαφοροποιεί τους ιούς από τα άλλα προγράμματα είναι ότι μπορεί να μεταδοθεί οπουδήποτε έχει τη δυνατότητα. Τέλος οι επιπτώσεις που μπορεί να έχει ένας ιός είναι από το να διαγράψει κάποια δεδομένα έως και να οδηγήσει στην κατάρρευση ολόκληρου του συστήματος.
- Δούρειος Ίππος (Trojan): είναι κακόβουλο λογισμικό που χρησιμοποιεί το στοιχείο της παραπλάνησης. Λογισμικό αυτού του είδους παριστάνει ότι είναι χρήσιμο για τον υπολογιστή αλλά στην πραγματικότητα μέσα από αυτό κάποιοι εγκληματίες καταφέρνουν να κλέψουν σημαντικά αρχεία ή να αποκτήσουν τον έλεγχο του συστήματος. Τις περισσότερες φορές το συγκεκριμένο λογισμικό δεν έχει στόχο τη μόλυνση του υπολογιστή, δηλαδή δεν αναπαράγεται, και για αυτό τα προγράμματα αυτά δεν χαρακτηρίζονται και επίσημα ως ιοί.

- Σκουλήκι (Worm): είναι κακόβουλο λογισμικό το οποίο μπορεί να μεταδοθεί άμεσα με τη χρήση κάποιας δικτυακής υποδομής όπως τα τοπικά δίκτυα ή μέσω κάποιου μηνύματος e-mail. Η ικανότητά του να πολλαπλασιάζετε αυτόματα στο σύστημα στο οποίο βρίσκεται του δίνει τη δυνατότητα να αποστέλλει προσωπικά δεδομένα ή κωδικούς πρόσβασης, ώστε αυτός που θα κάνει την επίθεση να έχει πρόσβαση στη σύνδεση δικτύου. Τέλος, ένα άλλο αρνητικό χαρακτηριστικό είναι ότι επιβαρύνουν το δίκτυο, φορτώνοντας το με άχρηστη δραστηριότητα.
- Rootkit: είναι λογισμικό το οποίο μπορεί να ανήκει πολύ εύκολα σε οποιαδήποτε από τις παραπάνω κατηγορίες. Αυτό το λογισμικό έχει την ιδιαιτερότητα να κρύβει κάποια κακόβουλα προγράμματα ώστε να μη γίνονται ορατά από το λογισμικό ασφαλείας. Αυτά τα προγράμματα κάποιες φορές λειτουργούν προστατευτικά για τους χάκερ διαγράφοντας τις πληροφορίες του εισβολέα.

Τρόπος διάδοσης των κακόβουλων προγράμματος

- Τα κακόβουλα προγράμματα μπορούν να εισέλθουν στον υπολογιστή σας με διάφορους τρόπους. Ακολουθούν ορισμένα συνηθισμένα παραδείγματα:
- Λήψη δωρεάν λογισμικού από το Διαδίκτυο το οποίο περιέχει κρυφό κακόβουλο πρόγραμμα
- Λήψη νόμιμου λογισμικού που συνοδεύεται κρυφά από κακόβουλο πρόγραμμα
- Επίσκεψη ενός ιστότοπου που έχει προσβληθεί από κακόβουλο πρόγραμμα
- Κλικ σε ένα ψεύτικο μήνυμα σφάλματος ή ένα αναδυόμενο παράθυρο που ξεκινά μια λήψη κακόβουλου προγράμματος
- Άνοιγμα ενός συνημμένου μηνύματος ηλεκτρονικού ταχυδρομείου που περιέχει κακόβουλο πρόγραμμα
- Υπάρχουν πολλοί διαφορετικοί τρόποι με τους οποίους μπορεί να διαδοθεί ένα κακόβουλο πρόγραμμα, ωστόσο αυτό δεν σημαίνει ότι δεν έχετε τη δυνατότητα να το σταματήσετε. Τώρα που γνωρίζετε τι είναι και τι κάνει ένα κακόβουλο πρόγραμμα, ας εξετάσουμε μερικά πρακτικά μέτρα που μπορείτε να πάρετε για να προστατευτείτε.

Τρόπος αποφυγής κακόβουλων προγραμμάτων

- Διατηρήστε τον υπολογιστή και το λογισμικό σας ενημερωμένα
- Χρησιμοποιήστε έναν λογαριασμό που δεν είναι λογαριασμός διαχειριστή, όπου αυτό είναι δυνατό
- Σκεφτείτε το καλά, προτού κάνετε κλικ σε συνδέσμους ή πραγματοποιήσετε λήψη οποιωνδήποτε αρχείων
- Να είστε προσεκτικοί, όταν ανοίγετε συνημμένα ηλεκτρονικού ταχυδρομείου ή εικόνες
- Μην εμπιστεύεστε αναδυόμενα παράθυρα τα οποία σας ζητούν να πραγματοποιήσετε λήψη λογισμικού
- Περιορίστε την κοινοποίηση αρχείων
- Χρήση λογισμικού προστασίας από ιούς