Κακόβουλο Λογισμικό (Malware)

Κεφάλαιο 16ο

Ασφάλεια και Προστασία στο Διδίκτυο

Τι είναι το Κακόβουλο Λογισμικό;

- Το κακόβουλο λογισμικό, ή **malware**, είναι κάθε τύπος λογισμικού που δημιουργείται με σκοπό να προκαλέσει βλάβη ή να εκμεταλλευτεί έναν υπολογιστή, δίκτυο ή συσκευή.
- Μπορεί να εκτελέσει διάφορες επιβλαβείς ενέργειες, όπως **κλοπή δεδομένων**, **καταστροφή αρχείων**, και **υποκλοπή προσωπικών πληροφοριών**.

Κύριοι Τύποι Κακόβουλου Λογισμικού

Ιοί (Viruses): Ένα κακόβουλο πρόγραμμα που «επικαλύπτει» και καταστρέφει άλλα προγράμματα στον υπολογιστή.

Τύποι Ιών

Ransomware (Λογισμικό Απαγωγής): Κρυπτογραφεί τα αρχεία του υπολογιστή και απαιτεί αμοιβή για την αποκατάστασή τους.

- **LockBit:**
  - Πρόκειται για ένα από τα πιο ενεργά και επικίνδυνα ransomware.
  - Κρυπτογραφεί τα αρχεία του θύματος και ζητά αμοιβή για την αποκρυπτογράφηση.
  - Συχνά, οι επιθέσεις του στοχεύουν μεγάλες εταιρείες και οργανισμούς, προκαλώντας τεράστιες οικονομικές απώλειες και διακοπή λειτουργίας.
- **Conti:**
  - Ένα άλλο πολύ διαδεδομένο ransomware που έχει προκαλέσει σημαντικές ζημιές παγκοσμίως.
  - Είναι γνωστό για την ταχύτητα και την αποτελεσματικότητά του στην κρυπτογράφηση αρχείων.
  - Προκαλεί τεράστιες οικονομικές απώλειες.
- **BlackCat:**
  - Είναι ένα ransomware γραμμένο στη γλώσσα Rust.
  - Είναι ένα από τα πιο επικίνδυνα ransomware, διότι κρυπτογραφεί τα αρχεία του θύματος και ζητά αμοιβή για την αποκρυπτογράφηση.
  - Προκαλεί διαρροή δεδομένων.

Trojans (Δούρειοι Ίπποι): Αυτά τα προγράμματα προσποιούνται ότι είναι χρήσιμα ή ακίνδυνα, αλλά στην πραγματικότητα ανοίγουν την πόρτα σε κακόβουλες επιθέσεις.

- **Emotet:**
- Ένα κακόβουλο λογισμικό που ξεκίνησε ως τραπεζικό **trojan** και εξελίχθηκε σε ένα από τα πιο διαδεδομένα **malware**.
- Χρησιμοποιείται για την εγκατάσταση άλλων κακόβουλων προγραμμάτων, όπως ransomware.
- Διακινεί **spam** και **Phishing emails**.
- **TrickBot:**
- Ένα άλλο **trojan** που χρησιμοποιείται για την κλοπή τραπεζικών στοιχείων και άλλων ευαίσθητων δεδομένων.
- Συνεργάζεται συχνά με άλλα malware, όπως το Emotet.
- Κλέβει τραπεζικά δεδομένα, προσωπικά δεδομένα και προκαλεί διαρροή δεδομένων.

Spyware (Κατασκοπευτικό Λογισμικό): Παρακολουθεί τις δραστηριότητες του χρήστη και συλλέγει προσωπικές πληροφορίες χωρίς τη συγκατάθεσή του.

- **Pegasus:** Πρόκειται για ένα από τα πιο εξελιγμένα spyware, αναπτυγμένο από την ισραηλινή εταιρεία NSO Group.
- Μπορεί να εγκατασταθεί σε κινητά τηλέφωνα και άλλες συσκευές χωρίς την γνώση του χρήστη.
- Μπορεί να παρακολουθεί τις κλήσεις, τα μηνύματα, τα emails, την τοποθεσία και άλλα δεδομένα του χρήστη.
- Έχει χρησιμοποιηθεί για την παρακολούθηση δημοσιογράφων, ακτιβιστών και πολιτικών.

Spyware (Κατασκοπευτικό Λογισμικό)

- **FinSpy (ή FinFisher):** Ένα άλλο ισχυρό spyware που χρησιμοποιείται από κυβερνήσεις και υπηρεσίες πληροφοριών.
- Μπορεί να παρακολουθεί την δραστηριότητα του χρήστη στο διαδίκτυο, να καταγράφει τις πληκτρολογήσεις και να παρακολουθεί την κάμερα και το μικρόφωνο της συσκευής.
- Προκαλεί διαρροή προσωπικών δεδομένων.
- **Cerberus**:Είναι ένα spyware που στοχεύει κυρίως συσκευές Android.Μπορεί να κλέψει τραπεζικά στοιχεία, κωδικούς πρόσβασης και άλλα ευαίσθητα δεδομένα.Μπορεί επίσης να παρακολουθεί την τοποθεσία του χρήστη και να καταγράφει τις κλήσεις.

Spyware (Κατασκοπευτικό Λογισμικό)

•**Mspy:**
•Εμπορικό λογισμικό spyware που επιτρέπει την παρακολούθηση συσκευών κινητής τηλεφωνίας.
•Σχεδιασμένο για γονικό έλεγχο, αλλά μπορεί να χρησιμοποιηθεί και για άλλους σκοπούς.
•Παρακολουθεί μηνύματα, κλήσεις, τοποθεσία GPS, ιστορικό περιήγησης και άλλα.
•**FlexiSPY:**
•Άλλο ένα εμπορικό spyware με δυνατότητες παρακολούθησης κινητών τηλεφώνων και υπολογιστών.
•Προσφέρει προηγμένες λειτουργίες όπως καταγραφή κλήσεων, παρακολούθηση εφαρμογών κοινωνικής δικτύωσης, και καταγραφή πληκτρολογήσεων.

Πως Λειτουργεί το Κακόβουλο Λογισμικό

- Το κακόβουλο λογισμικό συνήθως διανέμεται μέσω:
- **Μολυσμένων email (Phishing):** Μήνυμα ηλεκτρονικού ταχυδρομείου που περιέχει κακόβουλο συνημμένο ή σύνδεσμο.
- **Ελαττωματικών Ιστοσελίδων:** Ιστοσελίδες που εκμεταλλεύονται αδυναμίες στον φυλλομετρητή.
- **Μολυσμένων εφαρμογών και λογισμικού:** Λήψη λογισμικού από ανασφαλείς ή μη αξιόπιστες πηγές.

Σημάδια Εμφάνισης Κακόβουλου Λογισμικού

- **Αργή απόδοση του υπολογιστή:** Σημαντική πτώση στην απόδοση του συστήματος.
- **Αλλαγές στις ρυθμίσεις του συστήματος:** Ανεξήγητες τροποποιήσεις στις ρυθμίσεις.
- **Απώλεια αρχείων:** Κατεστραμμένα ή εξαφανισμένα αρχεία χωρίς προειδοποίηση.
- **Απρόσμενα παράθυρα ή διαφημίσεις:** Εμφάνιση διαφημίσεων ή αναδυόμενων παραθύρων χωρίς τη συγκατάθεση του χρήστη.

Συνέπειες της Επίθεσης από Κακόβουλο Λογισμικό

- **Απώλεια προσωπικών δεδομένων:** Κακόβουλο λογισμικό μπορεί να κλέψει ευαίσθητες πληροφορίες (π.χ., κωδικούς, τραπεζικά δεδομένα).

- **Οικονομικές ζημιές:** Με κακόβουλο λογισμικό, μπορεί να χαθούν χρήματα μέσω διαδικτυακών απάτων ή λύτρων.

- **Πλήγμα στην φήμη της επιχείρησης:** Ειδικά για επιχειρήσεις, μια επίθεση με κακόβουλο λογισμικό μπορεί να προκαλέσει απώλεια εμπιστοσύνης από τους πελάτες.

Πώς Να Προστατευτούμε Από το Κακόβουλο Λογισμικό

- **Χρήση Antivirus & Antimalware:** Εγκατάσταση αξιόπιστου λογισμικού προστασίας.
- **Τακτική ενημέρωση του λειτουργικού συστήματος και λογισμικού:** Οι ενημερώσεις διορθώνουν κενά ασφαλείας.
- **Αποφυγή ύποπτων συνδέσμων και συνημμένων:** Μην ανοίγετε email από άγνωστες πηγές.
- **Ενεργοποίηση του firewall:** Προστατεύει από εξωτερικές επιθέσεις.
- **Τακτικά αντίγραφα ασφαλείας (Backups):** Δημιουργία αντιγράφων ασφαλείας των δεδομένων

Συμπεράσματα

- Το κακόβουλο λογισμικό αποτελεί σοβαρό κίνδυνο για την ασφάλεια των προσωπικών δεδομένων και των συστημάτων. Η προστασία και η ενημέρωση είναι τα πιο αποτελεσματικά εργαλεία για την πρόληψη επιθέσεων και την αποτροπή καταστροφικών συνεπειών.