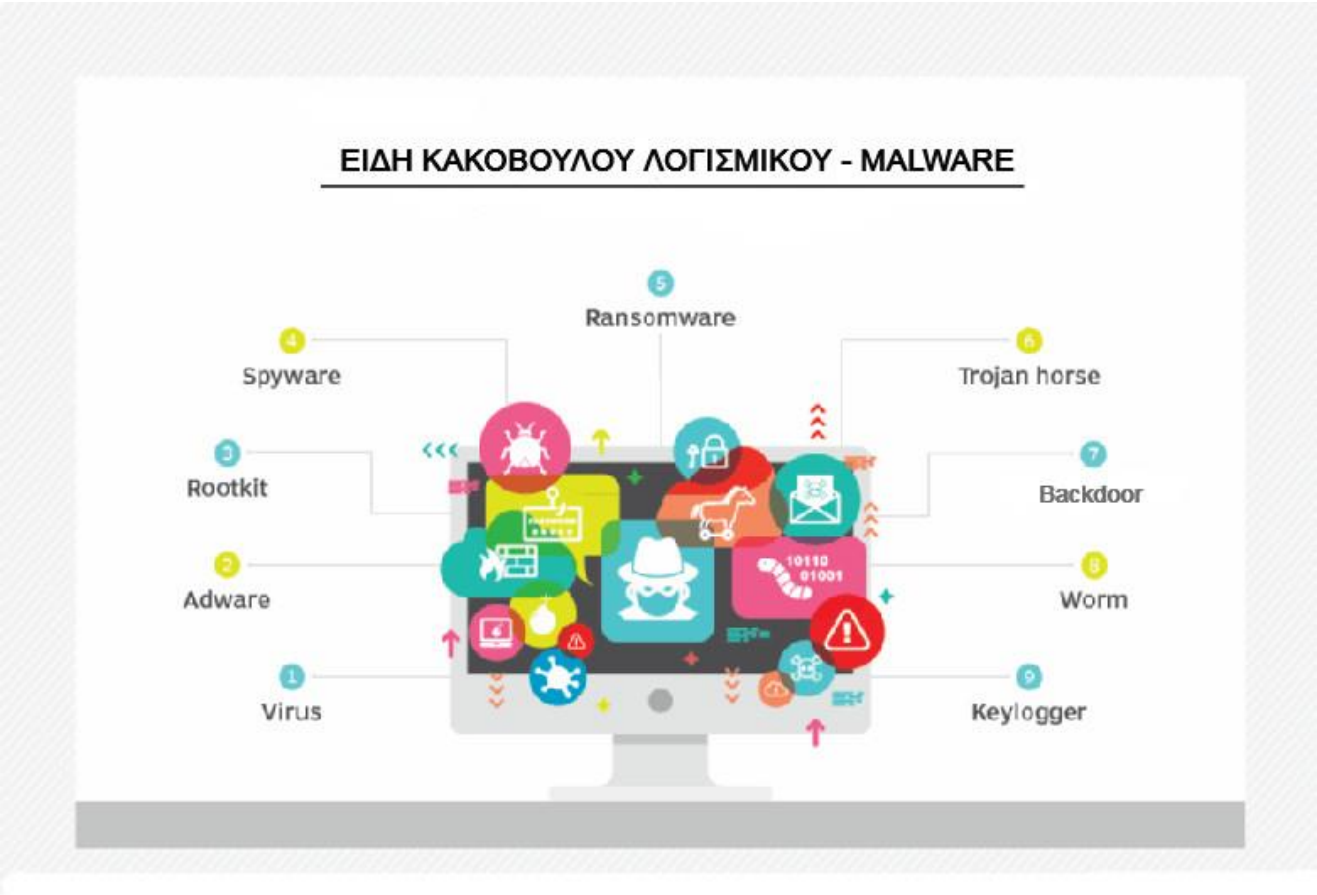
Κακόβουλο Λογισμικό - Malware



Οι διαφορετικοί τύποι του κακόβουλου λογισμικού (malware) περιέχουν ο καθένας τα δικά του χαρακτηριστικά και ιδιαιτερότητες. Σε γενικές γραμμές οι τύποι κακόβουλου λογισμικού είναι οι παρακάτω:

- Virus (ιός): είναι ο πιο συνηθισμένος τύπος κακόβουλου λογισμικού. Στη χειρότερη μορφή του, σκοπός του είναι η καταστροφή αρχείων ή προγραμμάτων (εφαρμογών) ενός υπολογιστή. Βρίσκεται ήδη σε ένα «μολυσμένο» αρχείο ή πρόγραμμα που θα κατεβάσει ο χρήστης στον υπολογιστή του. Εκτελείται αμέσως και διαδίδεται αντιγράφοντας τον εαυτό του και μολύνοντας με αυτόν τον τρόπο και άλλα αρχεία και εφαρμογές.
- Worm (σκουλήκι): είναι ένα πρόγραμμα που μολύνει όλους τους υπολογιστές που είναι συνδεμένοι σε ένα δίκτυο. Σκοπός του είναι να φορτώνει το δίκτυο με άχρηστη δραστηριότητα, επιβραδύνοντάς το. Μπορεί να αντιγράψει τον εαυτό του χωρίς να βρίσκεται ήδη σε ένα μολυσμένο αρχείο ή εφαρμογή και διαδίδεται μέσω του δικτύου, χωρίς να κάνει κάποια ενέργεια ο χρήστης.
- Spyware: η δράση του είναι εντελώς κρυφή και δεν γίνεται αντιληπτή. Έχει σχεδιαστεί για να συλλέγει πληροφορίες και δεδομένα του χρήστη και της συσκευής του, καθώς και να παρατηρεί τη δραστηριότητα του χρήστη, χωρίς ο ίδιος να το γνωρίζει.

- Trojan Horse (Δούρειος Ίππος): είναι το πιο συνηθισμένο spyware. Έχει σχεδιαστεί ώστε να έχει τη μορφή νόμιμου και καθόλου ύποπτου λογισμικού (π.χ. ενός συνημμένου αρχείου email ή μιας διαφήμισης), ώστε ο χρήστης να ξεγελαστεί και να το κατεβάσει στον υπολογιστή του. Τα trojans επιτρέπουν στον δημιουργό τους να αποκτήσει πρόσβαση σε προσωπικές πληροφορίες του χρήστη, όπως π.χ. σε λογαριασμούς τραπεζών, στοιχεία τραπεζικών καρτών και κωδικών.
- Ransomware: είναι σχεδιασμένο ώστε να κρυπτογραφεί τα αρχεία ενός χρήστη με αποτέλεσμα το σύστημα να 'κλειδώνει', εμφανίζοντας στην οθόνη ένα μήνυμα που ζητάει από το χρήστη 'λύτρα' (ransom), δηλαδή ένα χρηματικό ποσό, ώστε το σύστημα να ξεκλειδώσει και τα αρχεία να αποκρυπτογραφηθούν. Οι δημιουργοί του συνήθως ζητούν την πληρωμή τους σε κρυπτονομίσματα (π.χ. bitcoins). Το κακόβουλο λογισμικό τύπου ransomware χρησιμοποιεί τις περισσότερες φορές ένα trojan για να εγκατασταθεί στον υπολογιστή του θύματος.
- Rootkit: είναι σχεδιασμένο για να αποκτά δικαιώματα υπερ-χρήστη (superuser) ή αλλιώς διαχειριστή (administrator) στον υπολογιστή που έχει προσβάλει, εκμεταλλευόμενο πιθανά κενά ασφαλείας του λειτουργικού συστήματος. Επειδή αποκτά τέτοιου είδους δικαιώματα, μπορεί να εκτελεί λειτουργίες ίδιες με αυτές που εκτελεί ο διαχειριστής του συστήματος, χωρίς φυσικά τη συγκατάθεση του χρήστη-θύματος.
- Backdoor: είναι ένα κακόβουλο λογισμικό που χρησιμοποιείται για την απόκτηση αυθαίρετης απομακρυσμένης πρόσβασης (remote access) σε έναν υπολογιστή, χωρίς να είναι αντιληπτή από τον χρήστη του. Η απομακρυσμένη αυτή πρόσβαση επιτυγχάνεται μέσω εκμετάλλευσης 'τρωτών' σημείων στην ασφάλεια του υπολογιστή-στόχου ή λογισμικών με τα οποία έχει συνδεθεί ή κατεβάσει ο χρήστης-θύμα. Έτσι δημιουργείται μια ανοιχτή 'πίσω πόρτα' από την οποία οι δημιουργοί του backdoor μπορούν να μπαίνουν στον υπολογιστή του θύματος και να τον κατασκοπεύουν, να υποκλέπτουν προσωπικά στοιχεία του, να διαχειρίζονται όπως επιθυμούν τα αρχεία και δεδομένα του, να εγκαθιστούν κρυφά ανεπιθύμητα προγράμματα κ.α.
- Adware (ή λογισμικό διαφήμισης): χρησιμοποιείται για να περιγράψει τις διάφορες αναδυόμενες διαφημίσεις που εμφανίζονται σε έναν υπολογιστή ή μια φορητή συσκευή. Το Adware κάποιες φορές έχει τη δυνατότητα να καταστεί κακόβουλο και να βλάψει τη συσκευή, επιβραδύνοντάς τη, επεμβαίνοντας στον browser και εγκαθιστώντας ιούς και / ή spyware.
- Keyloggers: λογισμικό που καταγράφει τις καταχωρήσεις που γίνονται μέσω των πλήκτρων της συσκευής που παρακολουθείται. Μπορεί να είναι ο κωδικός ενός υπολογιστή ή ο αριθμός pin ενός κινητού τηλεφώνου. Μερικά keylogging προγράμματα, εκτός από τη δυνατότητα καταγραφής των κωδικών υπολογιστών και pin των κινητών, μπορούν να καταγράψουν στοιχεία που έχουν αντιγραφεί στο πρόχειρο (clipboard) καθώς και πλήρη στιγμιότυπα (screenshots) από την οθόνη του χρήστη. Ειδικά στην περίπτωση του smartphone, όπου όλες οι ενέργειες γίνονται από την επαφή που έχει το ανθρώπινο χέρι με την οθόνη (touchscreen), το λογισμικό keylogger μπορεί να καταγράψει όλες τις κινήσεις του χρήστη με τόσο διακριτικό τρόπο, που ο χρήστης δεν καταλαβαίνει ότι παρακολουθείται.

Δείτε τους παρακάτω συνδέσμους

- **Τι διαφορά έχει ένας ιός υπολογιστή, ένα trojan, ένα spyware και τα υπόλοιπα malware;**

- **Ransomware: γιατί ο νέος τύπος malware είναι επικίνδυνος και πως να προστατευτείτε**

- **Mobile Malware**

- **Αφαίρεση malware από κινητό χωρίς εργοστασιακή επαναφορά**