ΕΘΝΙΚΗ ΥΠΗΡΕΣΙΑ ΠΛΗΡΟΦΟΡΙΩΝ

CERT

Π. Κανελλοπούλου 4
Αθήνα - ΤΚ: 10177
210 697 3121
cert@nis.gr

Κακόβουλο Λογισμικό

Το κακόβουλο λογισμικό (malware) είναι κώδικας που έχει σχεδιαστεί για να βλάψει ένα υπολογιστικό σύστημα ή και για να καταστρέψει δεδομένα. Το κακόβουλο λογισμικό επηρεάζει τη διαθεσιμότητα κρίσιμων στοιχείων και δεδομένων, παρουσιάζοντας μια άμεση απειλή για τις καθημερινές δραστηριότητες ενός οργανισμού. Επιπλέον, το κακόβουλο λογισμικό μπορεί να διαχωριστεί σε ιομορφικό, όπου ανήκουν τα προγράμματα που έχουν τη δυνατότητα να αναπαράγονται από μόνα τους, και σε μη ιομορφικό, που ανήκουν τα προγράμματα που αναπαράγονται με την ανάμειξη του ανθρώπινου παράγοντα.

Ενδεικτικά αναφέρονται τα ακόλουθα είδη:

Backdoor (κερκόπορτα): Ένα κρυφό ελάττωμα του συστήματος γνωστό στον εισβολέα, ή ένας κρυφός μηχανισμός του συστήματος (συνήθως λογισμικό) εγκατεστημένος από τον εισβολέα, που μπορούν να ενεργοποιήσουν την «κερκόπορτα», για να αποκτήσει ο εισβολέας πρόσβαση στο σύστημα χωρίς να αποκλειστεί από μηχανισμούς ασφαλείας.

Trojan horse (δούρειος ίππος): Μεταμφιέζεται ως ακίνδυνη εφαρμογή, εξαπατώντας τους χρήστες ώστε να κάνουν λήψη και χρήση του. Όταν τεθεί σε λειτουργία, μπορεί να κλέψει προσωπικά δεδομένα, να κατασκοπεύσει δραστηριότητες, να καταστρέψει μια συσκευή ή ακόμα και να ξεκινήσει μια επίθεση π.χ. λυτρισμικού (ransomware).

Virus (ιός): Μεταδίδεται συνήθως μεταξύ υπολογιστών μέσω κάποιας εξωτερικής συσκευής αποθήκευσης (π.χ. εξωτερικό σκληρό δίσκο ή USB stick) ή μηνύματος ηλεκτρονικού ταχυδρομείου ως συνημμένο. Εξαπλώνεται γρήγορα και βλάπτει τα αρχεία του υπολογιστή, αναπαράγοντας συνεχώς τον εαυτό του.

Worm (σκουλήκι): Έχει ως στόχο να μολύνει ένα δίκτυο υπολογιστών, με τη δυνατότητα που έχει να αντιγράφεται από μηχανή σε μηχανή, εκμεταλλευόμενο κάποια αδυναμία ασφάλειας σε εγκατεστημένο λογισμικό ή το λειτουργικό σύστημα, και δεν απαιτεί την παρέμβαση του χρήστη για να εκτελείται.

Fileless κακόβουλο λογισμικό: Οι επιθέσεις κακόβουλου λογισμικού άνευ αρχείων δεν διαθέτουν αρχεία κακόβουλου λογισμικού για ανεύρεση μέσω σάρωσης ή εντοπισμό των κακόβουλων διαδικασιών τους. Δεν βασίζεται σε αποθηκευμένα αρχεία και γι' αυτό δεν αφήνει ίχνη.

Τα πιο συνηθισμένα σημάδια ότι ο υπολογιστής σας έχει παραβιαστεί από κακόβουλο λογισμικό είναι:

1. Πεσμένη απόδοση υπολογιστή (αργή λειτουργία και απόκριση).
2. Προειδοποιήσεις δήθεν μόλυνσης, που συχνά συνοδεύονται από προτάσεις να αγοράσετε κάτι για να τις διορθώσετε.
3. Το πρόγραμμα περιήγησης σας μεταφέρει σε ιστότοπους που δεν είχατε πρόθεση να επισκεφθείτε.
4. Επαναλαμβανόμενες αναδυόμενες διαφημίσεις.

Συμβουλές για να προστατευτείτε από το κακόβουλο λογισμικό:

1. Διατηρήστε ενημερωμένο το λειτουργικό σας σύστημα και τις εφαρμογές σας.
2. Να προμηθεύεστε επίσημα λογισμικά για τις συσκευές και τους υπολογιστές σας.

Π. Κανελλοπούλου 4
Αθήνα - ΤΚ: 10177
210 697 3121
cert@nis.gr

3. Όταν θέλετε να εγκαταστήσετε εφαρμογές, να τις «κατεβάζετε» από επίσημες πηγές.
4. Μην ανοίγετε άγνωστους συνδέσμους που λαμβάνετε μέσω email ή μηνυμάτων από ιστότοπους κοινωνικής δικτύωσης ή κινητής τηλεφωνίας.
5. Χρησιμοποιείτε μόνο γνωστούς και αξιόπιστους ιστότοπους. Αποφύγετε ιστότοπους που δεν χρησιμοποιούν το πρωτόκολλο HTTPS.
6. Να είστε επιφυλακτικοί όταν λαμβάνετε email που ζητούν προσωπικά σας στοιχεία ή σας ζητούν να επαναφέρετε κωδικούς πρόσβασης.
7. Μην ανοίγετε συνημμένα αρχεία σε email (εκτός αν γνωρίζετε τι είναι), από οποιονδήποτε και αν προέρχονται.
8. Χρησιμοποιήστε επίσημα προγράμματα προστασίας από ιούς (antivirus) στους υπολογιστές και στα κινητά σας.