

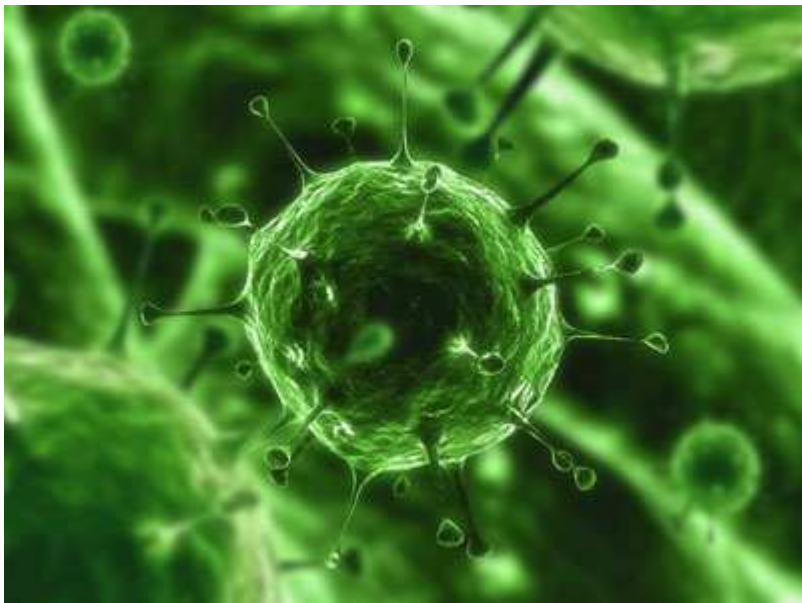
## Ιοί Ηλεκτρονικών Υπολογιστών

Ένας ιός υπολογιστών είναι ένα πρόγραμμα υπολογιστή, το οποίο μπορεί να αντιγραφεί χωρίς παρέμβαση του χρήστη και να

"μολύνει" τον υπολογιστή χωρίς τη γνώση ή την άδεια του χρήστη του. Ο αρχικός ιός μπορεί να τροποποιήσει τα αντίγραφα του ή τα ίδια τα αντίγραφα μπορούν να υποστούν από μόνα τους τροποποίηση, όπως συμβαίνει σε έναν μεταμορφικό ιό. Ένας ιός μπορεί να διαδοθεί από έναν υπολογιστή σε άλλους, παραδείγματος χάριν από ένα χρήστη που στέλνει τον ιό

μέσω δικτύου ή του Διαδικτύου, ή με τη μεταφορά του σε ένα φορητό μέσο αποθήκευσης, όπως δισκέτα, οπτικό δίσκο ή μνήμη flash USB. Οι ιοί ορισμένες φορές εσφαλμένα συγχέονται με τα "σκουλήκια" υπολογιστών (worms) και τους δούρειους ίππους (trojan horses). Ένα "σκουλήκι" μπορεί να διαδοθεί σε άλλους υπολογιστές χωρίς να πρέπει να μεταφερθεί ως τμήμα ενός υπολογιστή-οικοδεσπότη (host), ενώ ένας δούρειος ίππος είναι ένα αβλαβές πρόγραμμα μέχρι να εκτελεσθεί ή μέχρι να ικανοποιηθεί κάποια συνθήκη, την οποία έχει προκαθορίσει ο δημιουργός του. Πολλοί προσωπικοί υπολογιστές συνδέονται πλέον με το Διαδίκτυο και σε Τοπικό δίκτυο υπολογιστών τοπικά δίκτυα και διευκολύνουν έτσι τη διάδοση του κακόβουλου κώδικα. Σήμερα οι ιοί μπορούν επίσης να εκμεταλλευθούν τις υπηρεσίες του Διαδικτύου, όπως το World Wide Web, το ηλεκτρονικό ταχυδρομείο και την υπηρεσία συνομιλιών.

Μερικοί ιοί δημιουργούνται για να προξενήσουν ζημιά στον υπολογιστή, στον οποίο εγκαθίστανται, είτε με την καταστροφή των προγραμμάτων του είτε με τη διαγραφή αρχείων ή με τη



μορφοποίηση (format) του σκληρού δίσκου. Μερικές, μάλιστα, φορές, δημιουργούν σε συγκεκριμένο τομέα του σκληρού δίσκου τέτοια καταστροφή, ώστε να είναι αδύνατη η ανάκτηση ολόκληρου του περιεχομένου του. Άλλοι δεν έχουν ως σκοπό να προκαλέσουν οποιαδήποτε ζημία, αλλά απλά γνωστοποιούν την παρουσία τους με την εμφάνιση στην οθόνη κειμένου, βίντεο, ή ηχητικών μηνυμάτων, μερικές φορές αρκετά χιουμοριστικών. Όμως, ακόμη και αυτοί οι "καλοκάγαθοι" ιοί μπορούν να δημιουργήσουν προβλήματα στο χρήστη υπολογιστών: Καταλαμβάνουν τη μνήμη που χρησιμοποιείται από τα κανονικά προγράμματα και, κατά συνέπεια, προκαλούν συχνά ασταθή συμπεριφορά του συστήματος και μπορούν να οδηγήσουν σε κατάρρευσή του (system crash). Επιπλέον, πολλοί ιοί είναι, εγγενώς, γεμάτοι προγραμματιστικά σφάλματα, τα οποία πιθανόν να οδηγήσουν στην κατάρρευση των υπολογιστικών συστημάτων και στην απώλεια δεδομένων. Τέλος, ένα μεγάλο ποσοστό των ιών δεν έχει σκοπό την καταστροφή των δεδομένων του χρήστη ή την παρενόχλησή του, αλλά την κλοπή προσωπικών του δεδομένων ή την εισαγωγή του υπολογιστή-στόχου σε κάποιο παράνομο δίκτυο (botnet) χωρίς τη συγκατάθεση του χρήστη.

Ανεξάρτητα από το τι και πώς μολύνει σε ένα σύστημα, ο ιός πρέπει να εξασφαλίσει ορισμένες βασικές συνθήκες, προκειμένου να δράσει. Συγκεκριμένα, πρέπει να μπορεί να εκτελέσει τον



κώδικά του και να εξασφαλίσει πρόσβαση σε μέσα αποθήκευσης (κύρια στο σκληρό δίσκο, αλλά όχι μόνο). Γι' αυτό το λόγο, πολλοί ιοί προσκολλώνται σε εκτελέσιμα (executable) αρχεία είτε του λειτουργικού συστήματος είτε του κανονικού λογισμικού ενός

συστήματος. Εξασφαλίζουν έτσι δύο πράγματα: Πρώτον, ότι θα μπορούν να αναπαραχθούν και δεύτερον ότι θα μπορέσουν να εκτελέσουν τον κώδικά τους.

Οι ιοί διαδίδονται από τον ένα υπολογιστή στον άλλο με δύο τρόπους: Είτε μέσω φορητού μέσου αποθήκευσης είτε μέσω δικτύου. Ο δεύτερος τρόπος είναι σήμερα ο πλέον διαδεδομένος, λόγω της ευρείας διάδοσης του Διαδικτύου διεθνώς. Η βασική υπηρεσία διάδοσης ιών είναι αυτή του ηλεκτρονικού ταχυδρομείου (e-mail), μέσω του οποίου αποστέλλονται είτε ως συνημμένα είτε ως τμήμα αυτού καθαυτού του μηνύματος. Για το λόγο αυτό, πολλές υπηρεσίες e-mail προσφέρουν πρώτα σάρωση των μηνυμάτων και των συνημμένων τους με κάποιο αντιβιοτικό, πριν επιτρέψουν στο χρήστη να τα λάβει.

Οι ιοί αποτέλεσαν και αποτελούν έναν από τους πλέον διαδεδομένους τύπους κακόβουλου λογισμικού. Η ανίχνευση τους από τον απλό χρήστη είναι από δύσκολη έως αδύνατη - ορισμένοι, μάλιστα, ιοί, είναι τόσο προσεκτικά δημιουργημένοι που ακόμη και ο πλέον ειδικευμένος χρήστης αδυνατεί να τους εντοπίσει χωρίς να διαθέτει ειδικά προγραμματιστικά εργαλεία. Για την προστασία ενός συστήματος έχει δημιουργηθεί μια ειδική κατηγορία λογισμικού, γνωστή ως αντιϊκό (antivirus). Προκειμένου να εξασφαλίσουν την απρόσκοπτη και χωρίς μολύνσεις λειτουργία ενός συστήματος, τα αντιϊκά εκκινούν ταυτόχρονα με το λειτουργικό σύστημα του υπολογιστή, χωρίς εντολές από το χρήστη, και παραμένουν ως διαδικασίες στη μνήμη (memory resident), ώστε να είναι σε θέση να ανιχνεύουν τυχόν μολύνσεις σε πραγματικό χρόνο. Τα προγράμματα αυτά πρέπει να αναβαθμίζονται σε τακτική βάση, ώστε να είναι σε θέση να αντιμετωπίζουν με επιτυχία τους νεοδημιουργούμενους ιούς. Σήμερα, αρκετοί οίκοι δημιουργίας λογισμικού ασχολούνται με τη δημιουργία τέτοιων προγραμμάτων. Τα αντιϊκά είναι σε θέση τόσο να εντοπίσουν μόλυνση τη στιγμή που αποπειράται, όσο και να "καθαρίσουν" τυχόν μολυσμένα αρχεία που εντοπίζουν.



Κάθε αντιϊκό έχει το δικό του τρόπο δράσης απέναντι στους ιούς. Ωστόσο, τα περισσότερα είναι σε θέση να εργάζονται σε πραγματικό χρόνο, εντοπίζοντας τους ιούς τη στιγμή ακριβώς που αποπειρώνται να

μολύνουν το σύστημα. Ορισμένα τέτοια προγράμματα προσφέρονται δωρεάν για προσωπική χρήση (δεν καλύπτουν, ωστόσο, ούτε μικρό τοπικό δίκτυο υπολογιστών) και άλλα έναντι σχετικά χαμηλής τιμής (κανένα αντιϊκό για υπολογιστές δικτύου δεν προσφέρεται δωρεάν μέχρι σήμερα). Θα πρέπει να σημειωθεί ότι οι δημιουργοί των λαμβάνουν σοβαρά υπόψη τους τις μεθόδους εντοπισμού του "προϊόντος" τους και δημιουργούν ιούς, οι οποίοι προσπαθούν να αποφύγουν τον εντοπισμό, ακόμη και με απενεργοποίηση του αντιϊκού. Αυτό σημαίνει ότι ο χρήστης θα πρέπει να ενημερώνει τακτικά το λογισμικό του αλλά και να δημιουργεί τις ειδικές δισκέτες, που τα περισσότερα αντιβιοτικά προγράμματα προτείνουν τη δημιουργία τους, ώστε να είναι δυνατή η εκκαθάριση και η επαναφορά του συστήματος μετά από τυχόν μόλυνσή τους.