Ιοί Υπολογιστών



Εισαγωγικά 1/2

Οι ιοί των υπολογιστών αποτελούν πλέον ένα διαδεδομένο, καθημερινό φαινόμενο. Η γρήγορη εξάπλωση των ιών τα τελευταία χρόνια οφείλονται στο διαδίκτυο και ειδικότερα στο ηλεκτρονικό ταχυδρομείο, το οποίο αποτελεί μία από τις βασικότερες πηγές μόλυνσης των υπολογιστών. Το πρόβλημα των ιών των υπολογιστών είναι αρκετά παλιό.

Εισαγωγικά 2/2

Οι ιοί υπήρχαν εδώ και αρκετά χρόνια αλλά η εξάπλωσή τους δεν ήταν μεγάλη. Ο τρόπος μου μεταδίδονταν ήταν οι δισκέτες. Αυτό είχε σαν αποτέλεσμα την αργή εξάπλωσή τους. Οι χρήστες έπρεπε να εκτελέσουν ένα μολυσμένο αρχείο για να μολυνθεί ο υπολογιστής του. Τα αποτελέσματα του ιού επηρεάζουν μόνο τον υπολογιστή του συγκεκριμένου χρήστη.

Εξέλιξη των ιών

1987-1990	Εμφάνιση των πρώτων ιών που μεταδίδονταν με τη βοήθεια των δισκετών (μέσω της περιοχής εκκίνησης των δισκετών)
1990-1995	Άρχισαν να μεταδίδονται οι ιοί με τη βοήθεια των αρχείων.
1995-1998	Εμφάνιση των πρώτων ιών μακρο-εντολών που μεταδίδονταν με τα έγγραφα κειμένου.
1998-2001	Εμφάνιση των πρώτων ιών τύπου worm που μεταδίδονταν με τα μηνύματα του ηλεκτρονικού ταχυδρομείου.
2001 -	Κατακόρυφη αύξηση των ιών που μεταδίδονταν μέσω του διαδικτύου

Ορισμός

Ιός υπολογιστή είναι ένα εκτελέσιμο πρόγραμμα που έχει την ικανότητα να αναπαράγει τον εαυτό του. Αποτελείται από δύο τμήματα:

- **Τον κώδικα αναπαραγωγής**: αποτελεί απαραίτητο στοιχείο του ιού καθώς μέσω αυτού ο ιός εξαπλώνεται.
- **Τον κώδικα εκτέλεσης**: εκτελεί μία συγκεκριμένη λειτουργία ανάλογα με το τι έχει αποφασίσει ο δημιουργός του ιού.

Τύποι Ιών

Υπάρχουν πολλοί τύποι υπολογιστικών ιών, όπως ιοί αρχείων, ιοί της περιοχής εκκίνησης (boot sector), ιοί σκουλήκια και προγράμματα δούρειοι ίπποι(Trojan Horse).

Ιοί περιοχής εκκίνησης

- Αυτοί οι ιοί μολύνουν δισκέτες και σκληρούς δίσκους. Ο ιός φορτώνεται πριν από το λειτουργικό σύστημα. Ήταν οι πρώτοι ιοί που εμφανίστηκαν



File Viruses - Ιοί αρχείων

- Σ’ αυτή τη κατηγορία ανήκει η πλειοψηφία των ιών και η πιο εύκολα αντιμετωπίσιμη κατηγορία. Είναι μικρά εκτελέσιμα αρχεία. Προσκολλούνται σε ένα αρχείο, συνήθως αρχείο εφαρμογής. Το βασικό γνώρισμα των ιών είναι ότι δημιουργούν αντίγραφα του εαυτού τους μέσα σε άλλα αρχεία. Τα αρχεία αυτά είναι εκτελέσιμα ή αρχεία βιβλιοθηκών. Οι ιοί είτε αντικαθιστούν κάποιο τμήμα του κώδικα του αρχείου (χωρίς να μεταβάλλουν το μέγεθός του) είτε προσκολλώνται σε αυτό.

Ιοί σκουλήκια (Worms)1/2

- Έχουν την ικανότητα αναπαραγωγής χωρίς να χρησιμοποιούν άλλα αρχεία. Ο τρόπος διάδοσης τους είναι το διαδίκτυο με τη βοήθεια των δικτυακών πρωτοκόλλων, εκμεταλλευόμενοι τα προβλήματα ασφαλείας των λειτουργικών συστημάτων ή με τη βοήθεια των μηνυμάτων του ηλεκτρονικού ταχυδρομείου.

Ιοί σκουλήκια (Worms)2/2

- Οι ιοί σκουλήκια αποκτούν προσπέλαση στο βιβλίο διευθύνσεων του υπολογιστή (όπου κρατούνται οι διευθύνσεις ηλεκτρονικού ταχυδρομείου με τις οποίες επικοινωνεί ο χρήστης του υπολογιστή) και αποστέλλει μολυσμένα μηνύματα. Αρκετές φορές χρησιμοποιούν σαν αποστολέα ένα όνομα από το βιβλίο διευθύνσεων. Όσοι παραλήπτες ανοίξουν το ηλεκτρονικό μήνυμα μολύνονται. Η διάδοση των ιών worm με αυτή τη μέθοδο είναι αστραπιαία.

Trojan Horse
Δούρειος ίππος



- Αυτοί οι ιοί δρουν αθόρυβα. Μολύνουν τον υπολογιστή και αναμένουν κάποιο γεγονός ανάλογα με το προγραμματισμό τους. Συνήθως δεν πολλαπλασιάζοντας και δεν εξαπλώνονται σε άλλους υπολογιστές. Για να μολυνθεί ένας υπολογιστής ο χρήστης του πρέπει να κατεβάσει και να εκτελέσει τον ιό. Αυτό γίνεται συνήθως με ένα ηλεκτρονικό μήνυμα όπου ο ιός είναι συνημμένος και ο χρήστης πείθεται να τον εκτελέσει. Όταν ο ιός δούρειος ίππος εγκατασταθεί στέλνει μέσω διαδικτύου τις κατάλληλες πληροφορίες στο δημιουργό του ώστε αυτός να πάρει τον έλεγχο του υπολογιστή και να χρησιμοποιηθεί σε διάφορες παράνομες και επιβλαβείς ενέργειες

Spyware

Το spyware εγκαθίσταται συνήθως στον υπολογιστή σας χωρίς τη γνώση ή την άδειά σας. Εκτελείται στο παρασκήνιο, συλλέγοντας στοιχεία ή παρακολουθώντας τις δραστηριότητές σας. Πολλά προγράμματα spyware συγκεντρώνουν στοιχεία που σχετίζονται με τον υπολογιστή σας και τον τρόπο με τον οποίο τον χρησιμοποιείτε. Για παράδειγμα, ένα πρόγραμμα spyware μπορεί να παρακολουθεί τις συνήθειές σας όσον αφορά στην περιήγηση στο Διαδίκτυο. Ωστόσο, πιο πολύπλοκες μορφές spyware είναι γνωστό ότι συλλέγουν και μεταδίδουν πολύ ευαίσθητα προσωπικά στοιχεία στους κλέφτες ταυτότητας, από τους κωδικούς πρόσβασης σε ιστότοπους και τα ονόματα χρήστη έως τους αριθμούς πιστωτικής κάρτας ή τα αντίγραφα των άμεσων μηνυμάτων σας.

Adware

Το adware διαφέρει ελαφρώς από το spyware. Πρωταρχικός σκοπός του είναι να εμφανίσει διαφημιστικό περιεχόμενο στον υπολογιστή σας. Χρησιμοποιώντας αναδυόμενα παράθυρα, τα προγράμματα adware εμφανίζουν διαφημίσεις και συνδέσεις προς άλλους ιστότοπους. Πολλές από αυτές τις διαφημίσεις προωθούν νόμιμα προϊόντα. Ορισμένα adware παρακολουθούν την περιήγησή σας στο Διαδίκτυο και, στη συνέχεια, χρησιμοποιούν τις πληροφορίες αυτές για να παρέχουν πιο στοχευμένο διαφημιστικό περιεχόμενο. Ορισμένα άτομα δεν ενοχλούνται από αυτό, κάποια άλλα όμως θεωρούν αυτήν την πρακτική ως παραβίαση του ιδιωτικού απόρρητου.

Πώς να αποφύγετε το spyware και το adware

- Να είστε επιλεκτικοί όσον αφορά τα αρχεία που κατεβάζετε στον υπολογιστή σας.
- Διαβάστε τις συμφωνίες άδειας χρήσης.
- Προσέξτε αν υπάρχει κάποια απάτη όσον αφορά στην προστασία από spyware.
- Να προσέχετε τις διαφημίσεις στις οποίες μπορείτε να κάνετε κλικ.





Polymorphic virus
πολυμορφικός ιός

Οι ιοί αυτοί, στην προσπάθειά τους να "κρυφτούν" από τα προγράμματα antivirus, δημιουργούν πολλαπλά ενεργά αντίγραφα του εαυτού τους στο δίσκο ενός μολυσμένου υπολογιστή. Έτσι, είναι δυνατόν ο ίδιος ιός να εμφανίζεται με διαφορετικές μορφές σε διαφορετικά συστήματα ή ακόμα και σε διαφορετικά αρχεία που μολύνει. Οι πιο εξελιγμένοι ιοί του είδους χρησιμοποιούν ειδικές ρουτίνες μετάλλαξης και γεννήτριες τυχαίων αριθμών, ώστε να αλλάξουν τόσο τον κώδικά τους όσο και τον τρόπο κρυπτογράφησής τους.

Stealth Virus -Αόρατος ιός

Αυτοί οι ιοί είναι ουσιαστικά αυτό λέει και το όνομα τους. Δεν εντοπίζονται καθόλου εύκολα από τα anti-virus, καθώς κρύβονται από αυτά. Μόλις καταλάβουν ότι ένα πρόγραμμα anti-virus ξεκίνησε το scanning, αποκαθιστούν προσωρινά το αρχείο που είχαν μολύνει και μόλις τελειώσει το scanning το ξανά-μολύνουν (tunneling).

Virus Hoaxes - Ιός Απάτη

Οι περισσότερες hoax virus ειδοποιήσεις δίνουν οδηγίες στον παραλήπτη να προωθήσει την ειδοποίηση σε «όλους τους γνωστούς του» και εξαπλώνονται τόσο γρήγορα. Έχουν ως αποτέλεσμα να σπαταλάται ο χρόνος των χρηστών , ορισμένες hoax virus ειδοποιήσεις προτρέπουν τους χρήστες να σβήσουν αρχεία από τους υπολογιστές τους, π.χ. αρχεία που δεν έχουν μολυνθεί και μπορεί να είναι σημαντικότατα για τη σωστή λειτουργία του υπολογιστή.

Bootkit 1/3

- Ένα bootkit είναι ένα είδος κακόβουλου λογισμικού που μολύνει το Master Boot Record (MBR). Αυτή η μέθοδος μόλυνσης επιτρέπει το κακόβουλο πρόγραμμα που θα εκτελεστεί πριν από την εκκίνηση του λειτουργικού συστήματος. Από τη στιγμή που το BIOS (Basic Input Output System) επιλέγει την κατάλληλη συσκευή εκκίνησης (αυτό μπορεί να είναι σε ένα σκληρό δίσκο ή μια μονάδα flash), η bootkit που κατοικεί στο MBR αρχίσει την εκτέλεση του κώδικα. Μόλις το bootkit λαμβάνει τον έλεγχο, συνήθως ξεκινά την προετοιμασία η ίδια (διαβάζει και αποκρυπτογραφεί βοηθητικά αρχεία του στο δικό του σύστημα αρχείων που έχει δημιουργήσει κάπου στο αδιάθετο χώρο στο δίσκο) και επιστρέφει τον έλεγχο στο νόμιμο φορτωτή εκκίνησης επιβλέπει όλα τα στάδια της εκκίνησης διαδικασία.

Bootkit 2/3

Το κύριο χαρακτηριστικό ενός bootkit είναι ότι δεν μπορεί να ανιχνευθεί με τυπικές μέσω ενός λειτουργικού συστήματος επειδή όλα τα συστατικά του βρίσκονται έξω από τα τυποποιημένα συστήματα αρχείων. Ορισμένοι τύποι bootkits κρύβουν ακόμη και το γεγονός ότι το MBR έχει παραβιαστεί επιστρέφοντας το νόμιμο αντίγραφο του MBR, όταν έχει γίνει μια προσπάθεια για να το διαβάσετε.

Αν και τα rootkits απο μόνα τους δεν αποτελούν κάποια απειλή , υφίστανται μερικοί κίνδυνοι που προκύπτουν απο την χρήση τους όπως είναι η αδυναμία εξυγίανσης ενός συστήματος και κατά αποτέλεσμα η απώλεια του εξ ολοκλήρου ελέγχου του από τον ιδιοκτήτη ή η υποκλοπή σημαντικών πληροφοριών(π.χ. αριθμός πιστωτικής κάρτας,κωδικοί πρόσβασης, κ.α.)

Bootkit 3/3

Ένα σύστημα που έχουν μολυνθεί με bootkit μπορεί να θεραπευτεί με την **TDSSKiller** *δωρεάν πρόγραμμα* της kaspersky



Keylogger

- Λογισμικό το οποίο καταγράφει όλες τις πληροφορίες που κάποιος χρήστης πληκτρολογεί και τις αποστέλλει σε αυτόν που τον έχει μολύνει.

Μόλυνση

Τρόποι μόλυνσης

Ένας ιός εισάγεται σε έναν υπολογιστή μέσω μίας ποικιλίας ενεργειών. Για τους χρήστες του διαδικτύου αυτό μπορεί να συμβεί με το κατέβασμα αρχείων με FTP (file transfer protocol) με τη λήψη ενός ηλεκτρονικού μηνύματος ή και απλά με περιήγηση στο διαδίκτυο. Παλαιότερα οι ιοί διαδίδονταν με τις δισκέτες. Όταν ένας ιός εισαχθεί σε έναν υπολογιστή προσκολλάται ή αντικαθιστά ένα υπάρχον πρόγραμμα. Έτσι, όταν ο χρήστης εκτελεί το μολυσμένο πρόγραμμα, εκτελείται και ο ιός. Αυτό συνήθως συμβαίνει χωρίς να το αντιλαμβάνεται ο χρήστης.

Επιπτώσεις 1/2

Ένα πρόγραμμα ιός περιλαμβάνει εντολές που εκτελούν κάποια ενέργεια που επηρεάζει τον μολυσμένο υπολογιστή. Κάθε ιός περιλαμβάνει κάποια διαφορετική ενέργεια τα αποτελέσματα της οποίας μπορούν να είναι από απλά έως καταστροφικά:

- Η εμφάνιση στην οθόνη ενός εκνευριστικού μηνύματος.
- Μείωση της ελεύθερης μνήμης ή της χωρητικότητας του σκληρού δίσκου.
- Τροποποίηση δεδομένων.
- Αντικατάσταση ή καταστροφή αρχείων.
- Διαγραφή σκληρού δίσκου.

Επιπτώσεις 2/2

Σήμερα οι επιπτώσεις των ιών είναι λιγότερο καταστροφικές αλλά πολύ περισσότερο επικίνδυνες.

- Δυνατότητα παρακολούθησης των ενεργειών του χρήστη
- Δυνατότητα κατάληψης του υπολογιστή από άλλο χρήστη μέσω διαδικτύου.
- Χρήση του υπολογιστή για επιθέσεις σε άλλους υπολογιστές
- Υποκλοπή κωδικών – στοιχείων πιστωτικών καρτών.

Antivirus

Τα **Antivirus** είναι εφαρμογές που προστατεύουν τον υπολογιστή από τους ιούς. Βέβαια πρέπει το **Antivirus** να ενημερώνεται τακτικά με τις τελευταίες αναβαθμίσεις. Σε αντίθετη περίπτωση ο υπολογιστής θα μπορεί να προσβληθεί από τους καινούργιους ιούς.
Τα αντιβιοτικά προγράμματα αποτελούνται από δύο τμήματα:

- τη προστασία από τους ιούς και
- το τμήμα ανίχνευσης



Το πρόγραμμα προστασίας

Το πρόγραμμα προστασίας λειτουργεί σαν ασπίδα και ανιχνεύει τους ιούς τη στιγμή που προσπαθούν να εισχωρήσουν στον υπολογιστή και να εγκατασταθούν στη μνήμη του. Το πρόγραμμα αυτό ελέγχει τη μνήμη του υπολογιστή και τους βασικούς φακέλους με τα αρχεία του λειτουργικού συστήματος. Σε περίπτωση που ένας ιός ενεργοποιηθεί εξαιτίας της εκτέλεσης από το χρήστη μίας μολυσμένης εφαρμογής ή το άνοιγμα ενός μολυσμένου αρχείου, εμφανίζεται το μήνυμα αναφορά ύπαρξης του ιού. Οι περισσότερες εφαρμογές προστασίας από τους ιούς δίνουν την δυνατότητα στο χρήστη να διαγράψει ή να καθαρίσει (εάν αυτό είναι εφικτό) το μολυσμένο αρχείο. Επίσης τα αντιβιοτικά προγράμματα εκτός από τη μνήμη ελέγχουν και την εισερχόμενη και εξερχόμενη αλληλογραφία.

το τμήμα ανίχνευσης

Για την ανίχνευση των ιών χρησιμοποιείται μία βάση δεδομένων ή οποία περιλαμβάνει τμήματα του κώδικα των ιών. Αυτά ονομάζονται ψηφιακές υπογραφές. Με αυτό τον τρόπο αναγνωρίζονται τα μολυσμένα αρχεία καθώς και αν ένας ιός έχει φορτωθεί στη μνήμη του υπολογιστή. Το τμήμα ανίχνευσης είναι το δεύτερο σημαντικό τμήμα των αντιβιοτικών εφαρμογών. Η ενέργεια αυτή έχει σαν σκοπό αν στο σκληρό δίσκο του υπολογιστή υπάρχει κάποιος ιός (σε αναμονή). Το πρόγραμμα ελέγχει όλα τα αρχεία και του φακέλους του σκληρού δίσκου. Η διαδικασία του ελέγχου ξεκινάει με εντολή του χρήστη. Ο χρήστης μπορεί ακόμη να προγραμματίσει την εφαρμογή να προβαίνει αυτόματα σε περιοδικούς ελέγχους.

Σε περίπτωση που το πρόγραμμα ανιχνεύσει κάποιο ιό, ενημερώνει το χρήστη και προβαίνει στις προβλεπόμενες διαδικασίες. Συνήθως ολοκληρώνει τον έλεγχο και προβάλει μία λίστα με τα μολυσμένα αρχεία. Ο χρήστης μπορεί να επιλέξει να διαγράψει ή να καθαρίσει (αν αυτό γίνεται) τα αρχεία από τους ιούς.

Τι είναι το τείχος προστασίας; 1/2

- Το τείχος προστασίας (firewall) είναι λογισμικό ή υλικό το οποίο ελέγχει τις πληροφορίες που προέρχονται από το Internet ή από ένα δίκτυο και, στη συνέχεια, τις αποκλείει ή επιτρέπει να περάσουν στον υπολογιστή σας, ανάλογα με τις ρυθμίσεις του τείχους προστασίας.
- Το τείχος προστασίας εμποδίζει εισβολείς ή λογισμικό κακόβουλης λειτουργίας (όπως ιούς τύπου worm) να αποκτήσουν πρόσβαση στον υπολογιστή σας μέσω δικτύου ή του Internet. Το τείχος προστασίας εμποδίζει επίσης τον υπολογιστή σας να στείλει λογισμικό κακόβουλης λειτουργίας σε άλλους υπολογιστές.

Τι είναι το τείχος προστασίας;2/2

Η παρακάτω εικόνα παρουσιάζει τον τρόπο λειτουργίας ενός τείχους προστασίας:



Όπως ένας τοίχος με τούβλα μπορεί να δημιουργήσει ένα φυσικό εμπόδιο, το τείχος προστασίας δημιουργεί ένα εμπόδιο μεταξύ του Internet και του υπολογιστή
Το Τείχος προστασίας δεν είναι το ίδιο με το πρόγραμμα προστασίας από ιούς. Για την προστασία του υπολογιστή σας, χρειάζεστε τείχος προστασίας και πρόγραμμα προστασίας από ιούς και από λογισμικό κακόβουλης λειτουργίας.

Συμβουλές προστασίας

Ενεργοποίηση του Firewall στα Windows ή εγκατάσταση Firewall σε προηγούμενες εκδόσεις των Windows.

Τερματισμός υπηρεσιών δικτύου που δεν χρησιμοποιούνται

Χρήση antivirus προγραμμάτων με αυτόματη ενημέρωση.

Εγκατάσταση ενημερωμένων εκδόσεων του λειτουργικού συστήματος (service pack)

Αποεγκατάσταση εφαρμογών που δεν χρησιμοποιούνται

Ερωτήσεις

