Α) Ιοί ηλεκτρονικών υπολογιστών

Στο διήγημα **«When HARLIE was one»** (Όταν ο HARLIE ήταν ένας) ο Gerrold βάσισε την όλη πλοκή σε έναν ιό υπολογιστών. Ο HARLIE ήταν το ακρωνύμιο της φράσης Human Analog Robot Life Input Equivalent computer. Περιγραφόταν ως μια μορφή τεχνητής νοημοσύνης που είχε τη δυνατότητα να προσομοιώνει τις εγκεφαλικές λειτουργίες. Αυτό που έκανε ο HARLIE ήταν απίστευτα προφητικό για τη σημερινή εποχή των δικτυακών ιών: ο τεχνητός εγκέφαλος καλούσε τυχαία τηλεφωνικά νούμερα μέχρι να πάρει μια απάντηση από έναν υπολογιστή. Όταν το κατάφερνε, φόρτωνε ένα αντίγραφο του εαυτού του σε αυτόν. Ο «μολυσμένος» υπολογιστής με τη σειρά του άρχιζε την ίδια διαδικασία. Καλούσε και αυτός τυχαίους τηλεφωνικούς αριθμούς μέχρι να βρει άλλους υπολογιστές για να τους περάσει το πρόγραμμα. Σε ελάχιστο χρόνο εκατοντάδες υπολογιστές ασχολούνταν αποκλειστικά με την κλήση τυχαίων αριθμών.

Τι είναι Ιός Ηλεκτρονικού Υπολογιστή

Ο ιός υπολογιστών είναι ένα πρόγραμμα γραμμένο αποκλειστικά για *να αλλάζει τον τρόπο που λειτουργεί ο υπολογιστής σας, χωρίς την άδεια σας και χωρίς να το γνωρίζετε*.

Η πρώτη αναφορά στον όρο «Ιός υπολογιστή» έγινε το 1985, όταν ο Fred Cohen, μεταπτυχιακός φοιτητής του Πανεπιστημίου της Νότιας Καλιφόρνια, αποφάσισε να ονομάσει τα αυτοαναπαραγόμενα προγράμματα «computer viruses» (ιοί υπολογιστών). Ο Cohen είχε ακολουθήσει την υπόδειξη του καθηγητή του, που με τη σειρά του είχε επηρεαστεί από μια σειρά διηγημάτων επιστημονικής φαντασίας του David Gerrold από τη δεκαετία του '70 με τον τίτλο «When HARLIE was one».

Ο ίδιος ο Cohen όρισε αργότερα τον ιό υπολογιστών ως "***μια ακολουθία συμβόλων, τα οποία με τη μετάφρασή τους σε ένα δεδομένο περιβάλλον προκαλούν τη μεταβολή άλλων ακολουθιών συμβόλων ούτως ώστε να περιέχουν τμήμα της αρχικής ακολουθίας***".

Γενικά υποστηρίζεται σήμερα ότι ένα πρόγραμμα μπορεί να ονομαστεί ιός αν έχει τα ακόλουθα χαρακτηριστικά:

- Προκαλεί τη μεταβολή άλλου λογισμικού, εισάγοντας το δικό του κώδικα μέσα σε αυτό.
- Έχει την ιδιότητα να προκαλεί τέτοιου είδους μεταβολές σε περισσότερα του ενός προγράμματα.
- Έχει τη δυνατότητα να αναγνωρίζει τις μεταβολές που το ίδιο προξένησε σε άλλα προγράμματα.
- Έχει τη δυνατότητα να παρεμποδίζει την περαιτέρω μεταβολή (μόλυνση) αυτών των προγραμμάτων.
- Τα προγράμματα που έχουν προσβληθεί αποκτούν, με τη σειρά τους, όλα τα προαναφερθέντα χαρακτηριστικά.

Κατηγορίες ιών

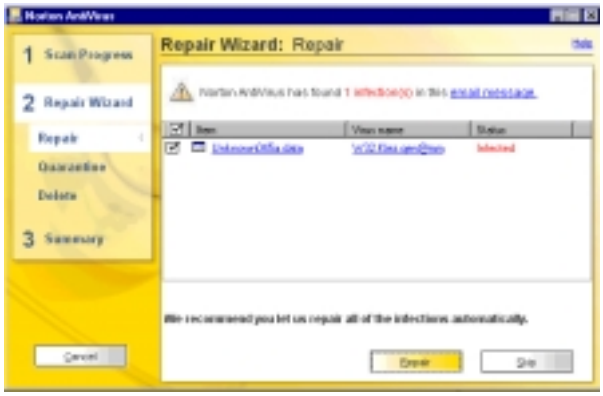
Σήμερα θα συναντήσουμε μεγάλη ποικιλία πολλών βλαπτικών προγραμμάτων στα οποία αποδίδεται γενικά ο όρος "rogue programs", είναι όμως απαραίτητη η ταξινόμησή τους σε τρεις βασικές κατηγορίες:

1. Trojan Horses ή Δούρειοι Ίπποι

Στην περίπτωση αυτή έχουμε ένα τμήμα ανεπιθύμητου κώδικα κρυμμένου μέσα σε ένα τμήμα επιθυμητού κώδικα. Προμηθεύεστε, δηλαδή, ένα πρόγραμμα το οποίο εκτελεί ή υποστηρίζει ότι εκτελεί μια επιθυμητή λειτουργία και μόλις το χρησιμοποιήσετε (είτε αμέσως είτε μόλις ικανοποιηθεί μια λογική ή χρονική συνθήκη), αυτό κάνει και κάτι άλλο, συνήθως επιτρέπει την πρόσβαση σε τρίτους στον μολυσμένο υπολογιστή ή προκαλεί καταστροφές στα αρχεία του..

2. Viruses ή Ιοί

Πρόκειται για έναν ειδικό τύπο Trojan Horse, ο οποίος έχει την ικανότητα να προσαρτά τον κώδικά του σε άλλα τμήματα κώδικα, να αναπαράγει τον εαυτό του και να πολλαπλασιάζεται, καθώς και να εκτελεί κάποια καταστροφική ή ουδέτερη λειτουργία.



Ο ιός w32Klez.gen@mm εντοπίσθηκε από το πρόγραμμα “Norton AntiVirus” και προτείνεται η επιδιόρθωση του αρχείου (Repair)

3. Worms ή Σκουλήκια

Αυτά μοιάζουν με τους ιούς, καθώς δεν επιτελούν καμία χρήσιμη ή επιθυμητή λειτουργία και επιπλέον μπορούν να παράγουν ακριβή αντίγραφα του εαυτού τους. Διαφέρουν, όμως στο ότι αποτελούν ανεξάρτητα και αυτόνομα προγράμματα και επιχειρούν ενεργά να διασπείρουν τον εαυτό τους και τα αντίγραφά τους μέσα σε ένα περιβάλλον δικτύου. Στόχος ενός Worm δεν είναι να προκαλέσει κάποια συγκεκριμένη ζημιά. Απλώς, με τον συνεχή πολλαπλασιασμό του, απασχολεί όλο και περισσότερους από τους πόρους (resources) του συστήματος, καθιστώντας το τελικά ανίκανο να λειτουργήσει κανονικά.

Πως μεταδίδονται οι ιοί

Οι τρόποι με τους οποίους μπορεί ένας ιός να μεταδοθεί είναι πολλοί. Τρεις είναι αυτοί που χρησιμοποιούνται πιο συχνά:

1. Ανταλλαγή αρχείων: Μεταφέροντας αρχεία με δισκέτα ή με CD από υπολογιστή σε υπολογιστή ο ιός μεταδίδεται, εφ' όσον ο αρχικός υπολογιστής ήταν μολυσμένος.

2. Ηλεκτρονικό Ταχυδρομείο: Μέσω των επισυναπτόμενων αρχείων του Ηλεκτρονικού ταχυδρομείου μπορεί να μεταδοθεί κάποιος ιός. Το ηλεκτρονικό ταχυδρομείο συνήθως προσβάλλεται από «Σκουλήκια» («Worms»).

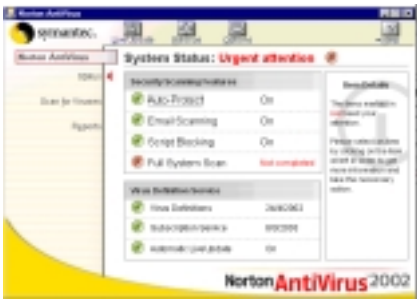
3. Παγκόσμιος Πληροφοριακός Ιστός: Όταν «κατεβάζετε» (Download) αρχεία από το Διαδίκτυο κάποιο απ' αυτά μπορεί να περιέχει ιό. Το σύνηθες εδώ είναι οι "Δούρειοι Ίπποι" ("Trojan Horses").

Τα αρχεία που περιέχουν έναν ιό, είναι είτε εκτελέσιμα αρχεία (αρχεία εφαρμογών) είτε αρχεία κειμένου και λογιστικών φύλλων τα οποία περιέχουν *μακροεντολές*.

Ο δικτυακός τόπος του McAfee VirusScan στη διεύθυνση www.mcafee.com

Αντιμετώπιση

Για την αντιμετώπιση των ιών αναπτύχθηκαν εφαρμογές **«Αντιβίωσης» (antivirus)**. Οι εφαρμογές αυτές παρακολουθούν όλες τις διαδικασίες, που πραγματοποιούνται στο υπολογιστικό σύστημα, με στόχο να ανιχνεύσουν οποιαδήποτε ενέργεια μπορεί να γίνει από κάποιον ιό. Ο έλεγχός τους ξεκινά από τη μνήμη, τις εφαρμογές που εκτελούνται στον υπολογιστή, για να καταλήξει στην πραγματοποίηση ελέγχου στα δεδομένα που μετακινούνται από και προς το υπολογιστικό σύστημα.



Το Norton Antivirus 2002

Η λειτουργία των προγραμμάτων antivirus μπορεί να περιγραφεί ως εξής : ανιχνεύουν τον ιό και δίνουν στο χρήστη μια σειρά από δυνατότητες: να καθαρίσει τα "μολυσμένα" αρχεία, να τα σβήσει, ή να τα θέσει σε καραντίνα. Ελέγχουν κάθε νέο αρχείο που προσπαθεί ο χρήστης να περάσει στον υπολογιστή του (από δισκέτα, CDROM, e-mail, τοπικό δίκτυο κλπ) και ακόμα προσφέρουν τη δυνατότητα ενημέρωσής τους (**Update**) μέσω του Διαδικτύου, ώστε έτσι να αναβαθμιστούν και να αντιμετωπίζουν τους νέους ιούς που εμφανίζονται.

Προληπτικές ενέργειες

Αν μεταφέρετε αρχεία από άλλους υπολογιστές ή χρησιμοποιείτε το διαδίκτυο υπάρχει πολύ μεγάλη πιθανότητα να προσβληθεί το υπολογιστικό σας σύστημα από κάποιον ιό. Καλό θα είναι να ακολουθήσετε τα παρακάτω «προληπτικά μέτρα»

1. **Πρόγραμμα Antivirus**: θα πρέπει το υπολογιστικό σας σύστημα να είναι εφοδιασμένο με κάποιο πρόγραμμα προστασίας από Ιούς.

2. **Συνεχής ενημέρωση**: Δεν έχει κανένα νόημα να χρησιμοποιείτε ένα πρόγραμμα antivirus, χωρίς να πραγματοποιείτε συχνές ενημερώσεις (updates) για νέους ιούς. Η συχνότητα παρουσίασης νέων ιών είναι πραγματικά τρομακτική, με αποτέλεσμα ένα "αντιβιοτικό" πρόγραμμα, το οποίο δεν έχει ανανεωθεί για πάνω από 15 μέρες να είναι ξεπερασμένο και κατ' επέκταση το σύστημα είναι ευάλωτο σε όλους τους νέους ιούς.

3. **Συχνοί έλεγχοι**: Καθώς ένας ιός μπορεί να μπει στο σύστημα σας ανά πάσα στιγμή, είτε ανοίγετε ένα αρχείο μέσω του δικτύου του σχολείου, είτε βρισκόσαστε συνδεδεμένοι στο Internet, θα πρέπει να πραγματοποιείτε συχνούς ελέγχους. Ο έλεγχος είναι απαραίτητος όταν εισαγάγετε μια δισκέτα ή ένα CD-ROM στο σύστημά σας, ή όποτε κατεβάζετε ένα αρχείο από το Internet.

4. **Μηνύματα από αγνώστους**: Δεν είναι λίγες οι φορές, που κάποιες εφαρμογές θα φτάσουν στο σύστημά σας μέσω e-mail. Θα πρέπει να είστε ιδιαίτερα προσεκτικοί στα συνημμένα αρχεία που μπορεί να σας έρθουν με μήνυμα ηλεκτρονικού ταχυδρομείου και τα οποία θα έχουν αποστολέα κάποιον άγνωστο.

5. **Αφύσικες λειτουργίες**: Υπάρχουν αρκετοί ιοί, οι οποίοι δημιουργούν κάποια προφανή προβλήματα δυσλειτουργίας στα συστήματα που προσβάλλουν. Χαρακτηριστικά παραδείγματα αυτού του προβλήματος είναι η παρουσίαση περίεργων δεικτών ποντικιού (mouse pointers), αλλά και πάγωμα (crash) του συστήματος. Σε αυτή την περίπτωση θα πρέπει να χρησιμοποιήσετε άμεσα κάποια εφαρμογή antivirus, για να μπορέσετε να δείτε, αν έχετε κάποιον ιό στο σύστημά σας.

6. **Αντίγραφα ασφαλείας**: Κρατήστε τα αρχεία δεδομένων σας σε αντίγραφα ασφαλείας (BackUp) σε δισκέτες ή CD-Rom. Μπορεί σαν διαδικασία να είναι ιδιαίτερα χρονοβόρα, ή κουραστική, αλλά μπορεί να αποβεί σωτήρια σε περίπτωση που κάποιος ιός έχει εισβάλλει στο σύστημά σας.

7. **Δισκέτα εκκίνησης**: Από τη στιγμή που θα εγκαταστήσετε ένα πρόγραμμα προστασίας από ιούς στο σύστημά σας, καλό θα ήταν να δημιουργήσετε τις δισκέτες εκκίνησης του προγράμματος, οι οποίες θα σας βοηθήσουν να ξεκινήσετε το σύστημά σας σε περίπτωση που έχει προσβληθεί από κάποιον ιό.

Για περισσότερες πληροφορίες σχετικά με την πρόληψη επισκεφθείτε τις παρακάτω διευθύνσεις :

http://www.mcafee.com
http://www.symantec.com
http://www.kaspersky.com
http://www.antivirus.com/pc-cillin
http://www.ca.com
http://www.pandasoftware.com
http://www.sophos.com
http://members.nbci.com/kbechtel/edu.htm
http://www.datafellows.com/vir-info/