Ιοί

- Τι είναι ένας ιός
  - Πρόγραμμα που γράφτηκε ειδικά για να εισέρχεται σε συστήματα χωρίς να το ξέρει ή να το επιτρέψει ο ιδιοκτήτης/χρήστης
  - Μετά την επιτυχή είσοδό του στο σύστημα, ο ιός προβαίνει σε (γενικά ανεπιθύμητες) ενέργειες όπως:
    - » Αναπαραγωγή
    - » σε υποβάθμιση της ασφάλειας του συστήματος
    - » Καταστροφή/φθορά δεδομένων

Γενικό μοντέλο ιών

Fred Cohen, "Computer Viruses - Theory and Experiments", 1984

```
program virus:= {1234567;
    subroutine infect-executable := {
        loop: file = get-random-executable-file;
        if first-line-of-file = 1234567 then goto loop;
        prepend virus to file;}
   subroutine do-damage := {whatever damage is to be done}
   subroutine trigger-pulled := {return true if some condition holds}
   main-program :=  {infect-executable;
        if trigger-pulled then do-damage;
        goto next;}
        next:}
```

Συμπεριφορά ιών (1)

- Δύο φάσεις: φάση μόλυνσης και φάση επίθεσης
- Φάση μόλυνσης
  - Οι συγγραφείς ιών αντισταθμίζουν την αμεσότητα και αποτελεσματικότητα της μόλυνσης με την ευκολία αποκάλυψης του ιού
    - » Μπορεί να μολύνει αμέσως
    - » Μπορεί να μολύνει όταν πληρείται κάποια συνθήκη (χρονική, πλήθος εκτελέσεων, εξωτερικά συμβάντα)

Συμπεριφορά ιών (2)

- Φάση μόλυνσης
  - Πολλοί ιοί προσομοιάζουν τη συμπεριφορά των *παραμενόντων προγραμμάτων*
    - » Με τον τρόπο αυτό απεξαρτώνται από τον φορέα τους
    - » Παραμονεύουν στη μνήμη μέχρι να έρθει η κατάλληλη στιγμή
    - » ... και τότε φροντίζουν να μολύνουν
  - Οι παραμένοντες ιοί φροντίζουν να προφυλάσσονται από την ανίχνευση (τεχνικές απόκρυψης –stealth– ή πολυμορφισμού)
  - Αντιθέτως, τα «σκουλήκια» διαδίδονται άμεσα

Συμπεριφορά ιών (3)

- Φάση επίθεσης
  - Οι ιοί μπορεί να επιτίθενται, μπορεί και όχι
  - Αλλά σε κάθε περίπτωση καταναλώνουν πόρους του συστήματος
  - Συχνές ενέργειες:
    - » Διαγραφή ή παραφθορά αρχείων
    - » Αναπαραγωγή μουσικής ή μηνύματα στην οθόνη
    - » Αποστολή μηνυμάτων ηλεκτρονικού ταχυδρομείου
  - Οι καταστροφές μπορεί να είναι προτιθέμενες ή όχι
    - » Ο ιός *stoned* έκρυβε τον εαυτό του με τρόπο που λειτουργούσε σε δισκέτες 360K, κατέστρεφε όμως τις 1.2M (το πρόβλημα λύθηκε σε επόμενη έκδοση)

Υπάρχουν «καλοί» ιοί;

- Πολλοί έχουν συλλάβει την ιδέα του «καλού» ιού
  - Ο «αντιβιοτικός» ιός – εντοπίζει και «σκοτώνει» τους κακούς ιούς
  - Ο ιός «συμπιεστής» – Ουσιαστικά συμπιέζει τα αρχεία πριν τα «μολύνει»
  - Ο ιός «κρυπτογράφος» – εγκαθίσταται στο σκληρό δίσκο και τον κρυπτογραφεί βάσει ενός συνθηματικού που δίνει ο χρήστης
  - Ο ιός «συντηρητής» – πραγματοποιεί κάποιες λειτουργίες συντήρησης π.χ. διαγραφή προσωρινών αρχείων

Υπάρχουν «καλοί» ιοί; - ΟΧΙ

- Τεχνικοί λόγοι
  - Αδυναμία ελέγχου
  - Είναι δύσκολο να διακρίνουμε μεταξύ ιών και κανονικών προγραμμάτων – πόσο μάλλον μεταξύ καλών και κακών ιών
  - Σπατάλη πόρων
  - Πιθανότητα ύπαρξης σφαλμάτων
  - Ζητήματα συμβατότητας με αυτοεπαληθευόμενα προγράμματα

Υπάρχουν «καλοί» ιοί; - ΟΧΙ

- Ηθικά, νομικά, ψυχολογικά ζητήματα
  - Μη εξουσιοδοτημένη τροποποίηση δεδομένων
  - Ζητήματα ιδιοκτησίας και πνευματικής ιδιοκτησίας
  - Πιθανή κακή χρήση
  - Υπευθυνότητα
  - Αντίληψη του όρου «ιός»
  - Ζήτημα εμπιστοσύνης – αίσθημα ασφάλειας

Είδη ιών

- Κατηγοριοποίηση βάσει του:
  - Τι μολύνουν
  - Πως μολύνουν

Ιοί τομέων εκκίνησης-συστήματος

- Ιοί που μολύνουν τομείς εκκίνησης/συστήματος
  - Κάθε δίσκος/δισκέτα έχει έναν τομέα εκκίνησης, ακόμη και αν δεν περιέχει λειτουργικό σύστημα
  - Οι σκληροί δίσκοι έχουν επιπλέον έναν κύριο τομέα εκκίνησης
  - Ο ιός εγκαθίσταται σε έναν από τους τομείς αυτούς, μετατοπίζοντας τον κανονικό κώδικα σε άλλο σημείο του δίσκου
  - Όταν εκκινηθεί ο υπολογιστής από μολυσμένο δίσκο/δισκέτα, ο ιός εγκαθίσταται στη μνήμη και μολύνει τον σκληρό δίσκο και τυχόν δισκέτες που θα προσπελασθούν

Ιοί αρχείων

- Η πολυπληθέστερη ποικιλία
- Στην απλούστερη μορφή τους, επικαλύπτουν το αρχικό τμήμα του προγράμματος με τον δικό τους κώδικα
  - Αλλά το πρόγραμμα έτσι παύει να λειτουργεί σωστά
- Στην πιο εξελιγμένη μορφή τους, μετατοπίζουν τον αρχικό κώδικα του αρχείου ή επισυνάπτουν τον δικό τους κώδικα στο τέλος, με τις κατάλληλες εντολές σύνδεσης

Παράδειγμα: Μόλυνση command.com

- Κανονικό command.com, μήκους 52.164 bytes

```
0100 06        PUSH    ES
0101 17        POP     SS
0102 BE1B02    MOV     SI,021B
```

- Μολυσμένο command.com

```
0100 E9C1CB    JMP     52420
0103 90        NOP
0104 90        NOP
...
CCC4 ; Κώδικας ιού
...
CDE0 06        PUSH    ES
CDE1 17        POP     SS
CDE2 BE1B02    MOV     SI,021B
CDE5 E91D33    JMP     105
```

Ιοί αρχείων

- Συνήθως μολύνουν αρχεία τύπου .COM, .EXE
- Αλλά και τα OVL, .DRV, .SYS, .BIN, .DLL είναι στους στόχους
- Μπορούν να παραμένουν στη μνήμη μετά την εκτέλεση του «ξενιστή»

Ιοί μακροεντολών

- Τα αρχεία δεδομένων δεν μπορούν να διαδώσουν ιούς
- *Ευτυχώς όμως υπάρχουν οι γλώσσες μακροεντολών, όπου κώδικας μπορεί να ενσωματωθεί σε αρχεία δεδομένων*
- Όσο πιο ισχυρή η γλώσσα μακροεντολών, τόσο πιο καταστροφικός μπορεί να είναι ο ιός
- Τα συνημμένα έγγραφα σε μηνύματα ηλεκτρονικού ταχυδρομείου μπορούν να μεταφέρουν και αυτά ιούς

Ιοί συστοιχίας

- Επικολλούνται στα αρχεία, χωρίς όμως να μεταβάλλουν το ίδιο το αρχείο, αλλά τις πληροφορίες των καταλόγων
- Ο ιός παραμένει στη μνήμη και διευθετεί τις αναγνώσεις/εγγραφές στον δίσκο
- *«Ευχάριστη παρενέργεια» ότι δημιουργούν μόνο ένα αντίγραφό τους στον δίσκο*
- *Δυσάρεστη παρενέργεια: αν ξεκινήσουμε τον υπολογιστή με «καθαρό» σύστημα και χρησιμοποιήσουμε πρόγραμμα ελέγχου δομής του δίσκου, μπορούμε να καταστρέψουμε το σύμπαν*

Ιοί «συνοδείας»

- Ιδιαίτερα δημοφιλείς σε περιβάλλον DOS
- Δεν αλλάζουν τα αρχεία, αλλά εκτελούνται πριν από αυτά
- Αξιοποιούν το χαρακτηριστικό του DOS ότι ψάχνει πρώτα για εκτελέσιμο τύπου .COM, μετά για τύπου .EXE
- Σχετικά εύκολο να ανιχνευθούν και να καθαρισθούν

Ιοί ειδικά για Windows

- Οι ιοί μπορούν να εκτελούνται ως διεργασίες εξυπηρέτησης (services) ή προγράμματα οδήγησης συσκευών, ή ακόμη και ως «κρυφές» εφαρμογές
- Μπορούν να εκτελούνται πριν από τα προγράμματα χωρίς να τα μολύνουν, αλλάζοντας το μητρώο

HKEY_CLASSES_ROOT\exefile\shell\open\command=virus.exe "%1" "%*"

- Αξιοποίηση της «εναλλακτικής ροής δεδομένων» του NTFS
  - File.exe → (File.exe file.exe:orig)

Τρόποι μόλυνσης

- Πολυμορφικοί ιοί
  - Οι ιοί μεταλλάσσονται σε κάθε μόλυνση για να αποφύγουν την ανίχνευση
  - Υπάρχουν ακόμη και εργαλειοθήκες για να βοηθούν τη μετάλλαξη ή ακόμη και τη συγγραφή νέων ιών
  - Τα προγράμματα καταπολέμησης ιών έχουν προσαρμοσθεί και μπορούν να εντοπίσουν τις μεταλλαγμένες μορφές

Τεχνικές απόκρυψης (stealth)

- Οι ιοί πραγματοποιούν τροποποιήσεις σε αρχεία/τομείς δίσκου/μνήμη και έτσι ανιχνεύονται
- Οι τεχνικές απόκρυψης αποσκοπούν στο να αποτρέψουν την ανίχνευση, συγκαλύπτοντας τις τροποποιήσεις
- Ο ιός παραμένουν στη μνήμη παγιδεύοντας τις κλήσεις συστήματος που θα απεκάλυπταν την παρουσία τους, και αναφέρουν τις πληροφορίες που θα επιστρεφόταν αν ο ιός δεν υπήρχε στο σύστημα
- Η ανίχνευση ιών πρέπει να γίνεται σε «καθαρό» σύστημα
- Η τεχνική απόκρυψης μπορεί να επηρεάσει την προσβασιμότητα στα δεδομένα – καθαρισμός μόνο με ειδικά προγράμματα

Προγράμματα εναπόθεσης ιών

- Δεν είναι τα ίδια ιοί
- ... αλλά μολύνουν το σύστημα με τον πραγματικό ιό
- Η κατηγορία περιλαμβάνει τους δούρειους ίππους που μεταφέρουν ιούς

Δυσκολεύοντας τη ζωή των προγραμμάτων ανίχνευσης

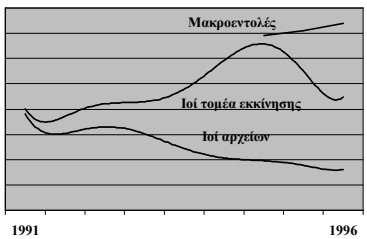
- Αργή μόλυνση έναντι ταχείας μόλυνσης
- «Αραιές» μολύνσεις (sparse infection)
- «Θωρακισμένοι» ιοί (armored viruses)
- «Πολυδραστικοί ιοί»
  - Επιτίθενται τόσο σε αρχεία όσο και σε τομείς συστήματος
- Ιοί «οπών»
  - Εγκαθίστανται σε αχρησιμοποίητους χώρους στο μέσον των αρχείων
  - Δεν είναι εύκολο να βρεθεί τέτοιος χώρος πάντα – το νέο πρότυπο PE ωστόσο τείνει να δημιουργεί κενά
- Ιοί «υπόγειας δράσης» (tunneling viruses)

Σύντομο ιστορικό - ο πρώτος ιός

- *Cloner* – Μόλυνε τις δισκέτες του Apple II

It will get on all your disks
It will infiltrate your chips
Yes it's Cloner!
It will stick to you like glue
It will modify ram too
Send in the Cloner!

Τα ποσοστά των κατηγοριών



Ιοί – Πώς τους αντιμετωπίζουμε

- Ορισμός διαδικασιών – συνεργασία χρηστών
  - Δεν ξεκινάμε ποτέ από δισκέτες – ρυθμίζουμε κατάλληλα το BIOS. Σε εταιρικά περιβάλλοντα μπορούμε να μην έχουμε συνολικά δισκέτες
  - Ρυθμίζουμε τον υπολογιστή στο μέγιστο επίπεδο ασφάλειας, κυρίως για προγράμματα πλοήγησης και ηλεκτρονικού ταχυδρομείου
  - Τα δεδομένα τα επεξεργαζόμαστε μόνο με συγκεκριμένα και ελεγμένα προγράμματα
  - Δεν κατεβάζουμε-εκτελούμε αρχεία συνημμένα σε ύποπτα μηνύματα, ή από αμφιβόλου αξιοπιστίας ιστοχώρους ή από newsgroups

Ιοί – Πώς τους αντιμετωπίζουμε

- Κρατάμε τακτικά εφεδρικά αντίγραφα και τα διατηρούμε για πολύ καιρό
- Χρησιμοποιούμε ειδικό λογισμικό αντιμετώπισης ιών

Λογισμικό αντιμετώπισης ιών

- Λειτουργικότητα
  - Εργαλεία ανίχνευσης
    - » Με στατική ανάλυση
      - Δυναμικά κατά την εκτέλεση
      - Περιοδικά
    - » Με αναχαίτιση της δράσης
      - Παρεμπόδιση των παράνομων ενεργειών
    - » Ανίχνευση αλλαγών
      - Εντοπισμός των τροποποιήσεων που έχουν επέλθει από ιούς
  - Εργαλεία προσδιορισμού ταυτότητας
  - Εργαλεία καθαρισμού

Κριτήρια επιλογής εργαλείων

- Ακρίβεια
  - Το εργαλείο πρέπει να ανιχνεύει τους ιούς, όλους τους ιούς και μόνο τους ιούς
  - Η σημασία εξαρτάται και από το επίπεδο των χρηστών
- Ευχρηστία
  - Προσπάθεια προσαρμογής του προγράμματος στο επίπεδο του χρήστη
- Διαχειριστικό φορτίο
  - Ενημερώσεις με νέες εκδόσεις/μηχανές ανάλυσης
  - Βοήθεια στους χρήστες για χειρισμό των αναφορών
- Υπολογιστικό φορτίο – κατανάλωση πόρων
  - «Βαριές» εφαρμογές συνήθως απενεργοποιούνται

Ζητήματα ακρίβειας

- Εργαλεία ανίχνευσης
  - Αναφορά ανύπαρκτων ιών (false positive)
  - Μη αναφορά υπαρκτών ιών (false negatives)
- Εργαλεία προσδιορισμού ταυτότητας
  - Αδυναμία προσδιορισμού συγκεκριμένου ιού
  - Εσφαλμένος προσδιορισμός ιού
    - » Συνολικό ζήτημα «ποιοι είναι διαφορετικοί ιοί»
- Εργαλεία καθαρισμού
  - Επιτυχία = επάνοδος στο προ της μόλυνσης αρχείο
  - *Συνολική αποτυχία*: παράγεται εκτελέσιμο που δεν λειτουργεί ή ο ιός δεν απομακρύνεται
  - *Μερική αποτυχία:* παράγεται εκτελέσιμο που λειτουργεί αλλά είναι διαφορετικό από το αρχικό

Ζητήματα ευχρηστίας

- Ευκολία χρήσης του λογισμικού
- Ευκολία να αντιληφθεί τα μηνύματα
- Δεν εισάγονται πρόσθετες δυσχέρειες στον χειρισμό του συστήματος

Διαχειριστική επιβάρυνση

- Ευκολία εγκατάστασης
- Ευκολία συντήρησης
- Υποστήριξη τελικών χρηστών

Επιβάρυνση συστήματος

- Πόροι που καταναλώνονται
- Επιβράδυνση του συστήματος
- Διαρκής παρακολούθηση έναντι περιοδικής ανίχνευσης

Εργαλεία και τεχνικές

- Εντοπισμός «υπογραφών» και αλγοριθμική ανίχνευση
  - Χρησιμοποιείται από τα εργαλεία ανίχνευσης που λειτουργούν επίσης και σαν εργαλεία προσδιορισμού ταυτότητας
  - Στόχος: εντοπισμός αν υπάρχει ιός σε αρχεία ή στη μνήμη
  - Χρήση: συνεχής ή περιοδική
  - Ο εντοπισμός «υπογραφών» επιχειρεί να βρει ακολουθίες bytes που είναι γνωστό ότι ανήκουν σε ιούς ή οικογένειες ιών
  - Οι υπογραφές συλλέγονται από μολυσμένα αρχεία
  - Μία υπογραφή μπορεί να περιέχει μεταχαρακτήρες ή να συνδυάζεται με τη θέση μέσα στο αρχείο
  - Για πολυμορφικούς ιούς απαιτείται αλγοριθμική ανίχνευση

Αξιολόγηση εντοπισμού υπογραφών

- Ακρίβεια
  - Γενικώς είναι ακριβείς ΑΝ έχουν ελεγχθεί από τον κατασκευαστή ΟΛΟΙ οι ιοί και ΟΛΑ τα «κανονικά» εκτελέσιμα
  - Αλλά και αναφέρονται ανύπαρκτοι ιοί και δεν αναφέρονται υπαρκτοί (νέοι ιοί ή ιοί με τεχνικές απόκρυψης)
  - Μερικές φορές προσδιορίζεται λάθος ιός ή λάθος παραλλαγή ιού

Αξιολόγηση εντοπισμού υπογραφών

- Ιδιαίτερα εύχρηστη – απαιτούνται λίγες γνώσεις
- Διαχειριστική επιβάρυνση
  - *Πάντα* είναι παρωχημένοι – απαιτούν ενημέρωση
  - Για μεγάλους οργανισμούς μπορεί να είναι πρόβλημα
  - Εύκολη εγκατάσταση ακόμη και για τους απλούς χρήστες
  - Στο βαθμό που οι διαγνώσεις είναι σωστές δεν απαιτείται υποστήριξη των χρηστών
  - Στις αναφορές ανύπαρκτων ιών απαιτείται συνδρομή διαχειριστών
- Ιδιαίτερα αποδοτικοί σε περιοδική εκτέλεση, αρκετά αποδοτικοί σε διαρκή παρακολούθηση

Εντοπισμός υπογραφών - Σύνοψη

✓ Τα καλά συντηρούμενα συστήματα εντοπίζουν άνω του 95% των ιών
✓ Δρουν και ως εργαλεία προσδιορισμού ταυτότητας, μειώνοντας τον χρόνο ανάκαμψης
✓ Δοκιμασμένη τεχνολογία με βελτιστοποιημένους αλγόριθμους
✓ Απαιτείται ελάχιστη γνώση

× Βρίσκουν μόνο τους ιούς που ήταν γνωστοί κατά την ανάπτυξη του «πακέτου υπογραφών»
× Πρέπει να συντηρούνται διαρκώς
× Είναι επιρρεπείς σε εσφαλμένους προσδιορισμούς ταυτότητας
× Οι χρήστες παρανοούν το *«δεν ανιχνεύθηκε ιός»* πιστεύοντας ότι σημαίνει *«δεν υπάρχει ιός»*

Ελεγκτές ακεραιότητας

- Δημιουργία αθροίσματος ελέγχου σε καθαρό σύστημα για κάθε εκτελέσιμο
  - με κυκλικούς πλεοναστικούς κώδικες (CRC)
  - με κρυπτογραφικές μεθόδους (ψηφιακές υπογραφές)
  - με συνδυασμό συναρτήσεων κερματισμού και κρυπτογραφικών μεθόδων
- Επανυπολογισμός του αθροίσματος ελέγχου και σύγκριση με το αρχικό

Αποτίμηση ελεγκτών ακεραιότητας

- Ακρίβεια
  - Όλοι οι ιοί εντοπίζονται, αρκεί ο αρχικός υπολογισμός να έχει γίνει σε καθαρό σύστημα
  - Πολλές ψευδείς αναφορές για ύπαρξη ιών
  - Αναποτελεσματικό για ιούς μακροεντολών
- Ευχρηστία
  - Τα αθροίσματα ελέγχου πρέπει να αποθηκεύονται σε μη προσβάσιμη περιοχή
  - Ο μέσος χρήστης δεν γνωρίζει αν ένα πρόγραμμα αυτοτροποποιείται
  - Οι πολλές ψευδείς αναφορές κάνουν τους χρήστες επιφυλακτικούς στις προειδοποιήσεις

Αποτίμηση ελεγκτών ακεραιότητας

- Διαχειριστική επιβάρυνση
  - Εύκολη εγκατάσταση
  - Ενημέρωση αθροισμάτων ελέγχου σε κάθε νέα εγκατάσταση ή αναβάθμιση
  - Διαρκής υποστήριξη χρηστών για χειρισμό των αναφορών
- Επιβάρυνση συστήματος
  - Δεν επηρεάζει τη συνήθη λειτουργία
  - Ο χρόνος υπολογισμού είναι σημαντικός

Ελεγκτές ακεραιότητας - Σύνοψη

- ✓ Δεν χρειάζονται ενημέρωση
- ✗ Δεν βρίσκουν τους ιούς – μόνο τις αλλαγές
- ✗ Πρέπει να υπολογίζονται αθροίσματα ελέγχου σε κάθε εγκατάσταση/αναβάθμιση προγράμματος
- ✗ Εσφαλμένες αναφορές, θετικές και αρνητικές
- ✗ Δεν είναι καθόλου αποτελεσματικοί για ιούς μακροεντολών

Επόπτες γενικού σκοπού

- Προστατεύουν το σύστημα από τη διάδοση ιών ή τη δράση των Δούρειων Ίππων αναχαιτίζοντας κακόβουλες ενέργειες
- Οι κατασκευαστές *μοντελοποιούν* τη συμπεριφορά των ιών και δημιουργούν κώδικα που προσπαθεί να ανιχνεύσει και να παρεμποδίσει τις ενέργειες αυτές
  - το πρόγραμμα ζητά μνήμη που «αυτονομείται»
  - το πρόγραμμα ανοίγει αρχεία συστήματος (π.χ. command.com)
  - το πρόγραμμα ανοίγει εκτελέσιμα σε άλλους καταλόγους
  - ένα έγγραφο Word διαγράφει αρχεία MP3

Αποτίμηση εποπτών γενικού σκοπού

- Ακρίβεια
  - Προϋποθέτει ότι οι ιοί θα συμπεριφερθούν βάσει των μοντέλων – δεν συμβαίνει πάντα
  - Οι ιοί πιθανώς να προσπαθήσουν να απενεργοποιήσουν τον επόπτη
  - Κανονικά προγράμματα μπορεί να προβαίνουν σε ενέργειες που εντάσσονται στα μοντέλα ιών
- Ευχρηστία
  - Ο μέσος χρήστης δεν έχει τις γνώσεις να τα χειριστεί
  - *Απαιτείται και διαμόρφωση-ρύθμιση*

Αποτίμηση εποπτών γενικού σκοπού

- Διαχειριστική επιβάρυνση
  - Αρκετή κατά την εγκατάσταση, ειδικά αν υπάρχουν διαφορετικές εγκαταστάσεις
  - Συνεχής για υποστήριξη χρηστών, ανάλογα με το προφίλ τους
  - Απαιτείται ενημέρωση μόνο για νέες *τεχνικές ιών*
- Επιβάρυνση συστήματος
  - Εισάγεται από την παρακολούθηση των λειτουργιών
  - Γενικώς είναι περιορισμένη

Επόπτες γενικού σκοπού - σύνοψη

✓Αρκετά γενική τεχνική
✓Κανονικά λειτουργεί και για άγνωστους ιούς
✓Μικρή συχνότητα ενημερώσεων
× Δύσχρηστο για τον μέσο χρήστη
× Αρκετές ψευδείς αναφορές ύπαρξης ιών
× Μεγάλο διαχειριστικό κόστος
× Ευάλωτο σε νέες τεχνικές ιών
× Μπορεί να απενεργοποιηθεί από τους ιούς

Κελύφη ελέγχου πρόσβασης

- Ενσωματώνονται στο Λ.Σ.
- Επιβάλλουν πολιτικές που ορίζουν ποιο πρόγραμμα μπορεί να κάνει τι σε τύπους αρχείων
- Μπορεί να περιλαμβάνονται και πληροφορίες ταυτότητας χρήστη
- Μπορεί να περιλαμβάνει εργαλεία κρυπτογράφησης
  + (*, winword, "*.doc", rw)
  + (admin, winword, "*.dot", rw)
  + (*, winword, "*.dot", r)
  + (admin, windowsUpdate, "c:\windows*", "rw")
  – (*, *, "c:\windows\system*", "w")

Αποτίμηση κελύφους ελέγχου πρόσβασης

- Ακρίβεια
  – Ιοί που δεν συμπεριφέρονται σύμφωνα με τα κωδικοποιημένα πρότυπα δεν ανιχνεύονται
  – Ο ιός μπορεί να μολύνει όλα τα αρχεία που επιτρέπεται στον ξενιστή του να τροποποιήσει
    » ιοί μακροεντολών διαδίδονται ελεύθερα
  – Απαιτείται καλή ρύθμιση για να αποφευχθούν εσφαλμένες αναφορές ύπαρξης ιών
- Ευχρηστία
  – Οι χρήστες απλά δουλεύουν όπως πριν, ζητώντας επιπλέον προνόμια όταν το σύστημα τους αρνείται λειτουργίες
  – Ακατάλληλο για «οικιακή χρήση»

Αποτίμηση κελύφους ελέγχου πρόσβασης

- Διαχειριστική επιβάρυνση
  – Μεγάλη κατά την αρχική ρύθμιση
  – Σημαντική αν αλλάζει το λογισμικό, ή οι ρόλοι στο εταιρικό περιβάλλον
  – Δεν απαιτούνται ενημερώσεις του ίδιου του λογισμικού
- Επιβάρυνση συστήματος
  – Σχετικά μικρή για την επιβολή των πολιτικών
  – Μεγαλύτερη αν χρησιμοποιούνται μηχανισμοί κρυπτογράφησης

Ευρεστική ανάλυση κώδικα

- Έλεγχος του κώδικα για εντοπισμό κώδικα που *μοιάζει* με ιό
  – π.χ. άλμα στο τέλος, αυτοτροποποίηση του κώδικα, άλμα στην αρχή
- *Πιθανώς μολυσμένα* αρχεία

✓Εύκολα στη χρήση
✓Ανίχνευση αγνώστων ή πολυμορφικών ιών
× Δεν βρίσκουν όλους τους ιούς
× Μπορεί να αναφέρουν ανύπαρκτους ιούς
× Απαιτούν πολύ επεξεργαστική ισχύ

Εργαλεία καθαρισμού ιών

- Καθαρισμός ιού → Η πραγματοποίηση των αντίστροφων των αλλαγών που επέφερε ο ιός
  – Ανάλυση του τρόπου δράσης του ιού και ανάπτυξη αλγορίθμου αναίρεσης
- Εργαλεία που απομακρύνουν έναν μόνο ιό
  – Συνήθως μετά από «επιδημίες» συγκεκριμένου ιού
- Εργαλεία καθαρισμού πλειάδας ιών

Εργαλεία καθαρισμού ιών

- Για να λειτουργήσουν πρέπει οι αλλαγές να είναι αντιστρέψιμες
  - Ιοί που επικαλύπτουν το εκτελέσιμο δεν είναι δυνατό να «καθαρισθούν»
- Σημαντικό στοιχείο είναι ο ορθός προσδιορισμός του ιού ή της συγκεκριμένης παραλλαγής
  - διαφορετική διαδικασία για τους Jerusalem-DC και Jerusalem-E2
- Δύσκολος ή αδύνατος ο καθαρισμός για πολλαπλές μολύνσεις
- Προτιμότερη η αντικατάσταση του εκτελέσιμου με «καθαρό»