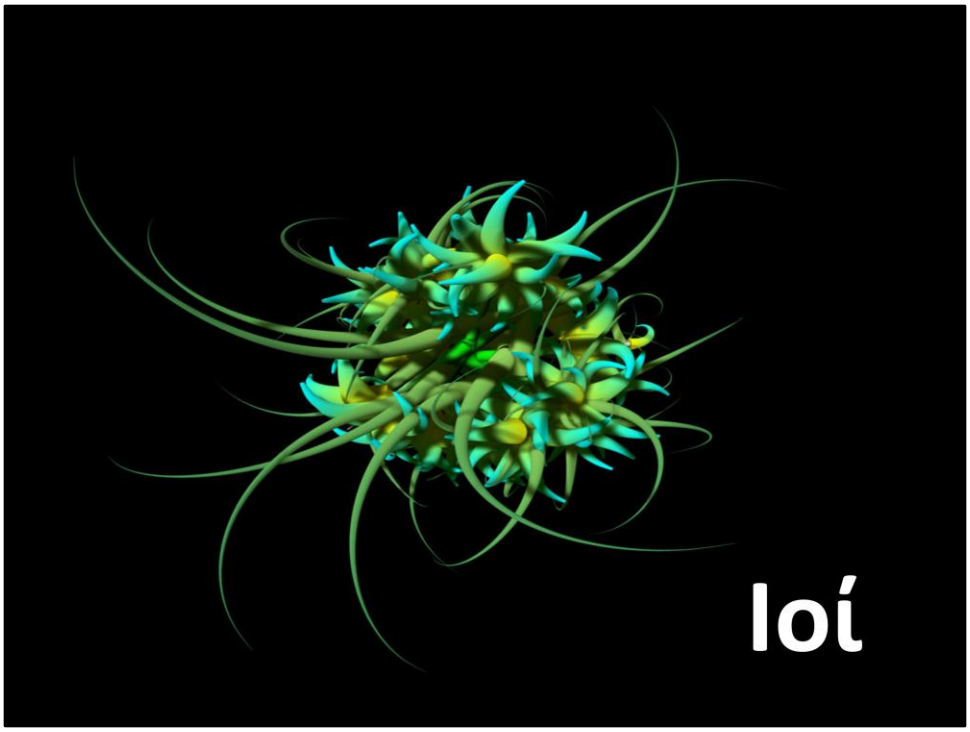

Ιομορφικό
και κακόβουλο λογισμικό
Δρ Κωνσταντίνος Παπαπαναγιώτου



Ορισμός

Τι είναι ιός;

Ένα πρόγραμμα ή κομμάτι κώδικα που προσκολλάται, γράφει από πάνω ή αντικαθιστά με άλλο τρόπο ένα άλλο πρόγραμμα με σκοπό να αναπαραχθεί χωρίς τη γνώση του χρήστη

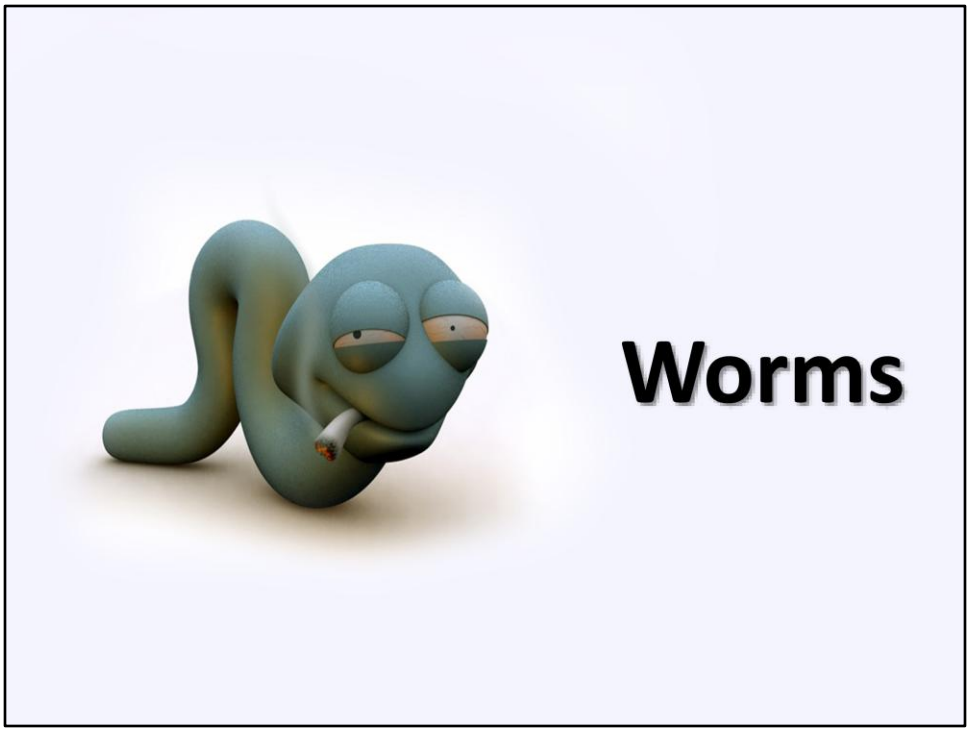
Μπορεί να μεταδοθεί μεταξύ υπολογιστών αντιγράφοντας τον εαυτό του.

Μετά την επιτυχή είσοδό του στο σύστημα, ο ιός προβαίνει σε (γενικά ανεπιθύμητες) ενέργειες όπως:

Αναπαραγωγή

σε υποβάθμιση της ασφάλειας του συστήματος

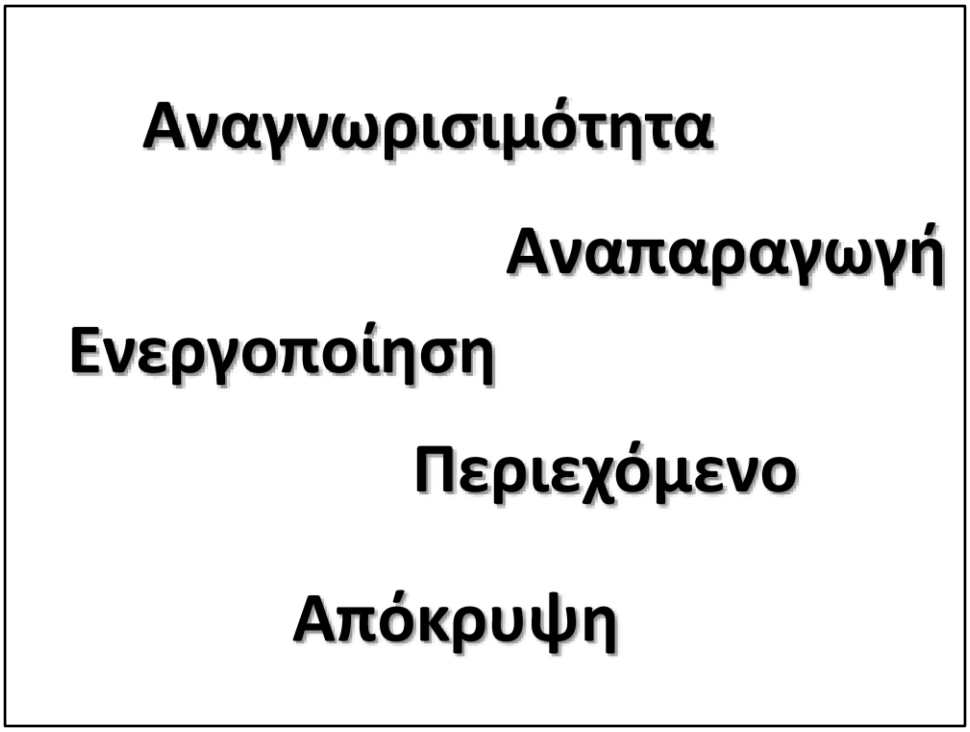
Καταστροφή/φθορά δεδομένων



Worm
Ένα πρόγραμμα που μεταδίδεται (συνήθως) μέσα από δίκτυα. Αντίθετα με έναν ιό, δεν προσκολλάται σε άλλο πρόγραμμα-ξενιστή και δεν απαιτεί ανθρώπινη παρέμβαση για να διαδοθεί.
Πρακτικά μοιάζουν με ιούς μόνο που μεταδίδονται μόνα τους. Αποτελούν ουσιαστικά ανεξάρτητα προγράμματα.

1981: *Elk Cloner*
1986: *Brain*
1987: *Christmas Tree*
1988: *Internet Worm*
1992: *Michelangelo*
1994: *Good Times* (hoax)
1998: *CIH (Chernobyl)*
1999: *Melissa*
2001: *Nimda*
2003: *Slammer*, *Blaster*
…
2009: *Conficker (Downadup)*

Ιστορικό
1981: Elk Cloner: ιός boot sector που μόλυνε Apple II συστήματα και εμφάνιζε ένα ποιήμα ανά 50 φορές εκκίνησης.
1986: Brain: ιός boot sector που γράφτηκε από δύο αδέρφια στο Πακιστάν και εμφάνιζε μήνυμα για να επικοινωνήσει μαζί τους ο χρήστης.
1987: Ζωγράφιζε ένα χριστουγεννιάτικο δέντρο
1988: Internet Worm: το πρώτο Worm, εξαπλώθηκε πολύ γρήγορα και πέρα από τις αρχικές προσδοκίες
1992: Michelangelo: Δημιούργησε μεγάλο ντόρο αλλά τελικά δεν είχε πολλές συνέπειες
1994: Good Times: Ο πρώτος ιός-φάρσα.
1998: CIH: Ο πρώτος ιός που επηρέαζε το hardware
1999: Melissa: Μακρο-ιός που επηρεάζει έγγραφα Word (για πρώτη φορά μη εκτελέσιμα αρχεία)
2001: Nimda: Τροποποιούσε δικτυακές σελίδες για να μοιράζει μολυσμένα αρχεία
2003: Εκμετάλλευση αδυναμιών στην υπηρεσία RPC των Windows
2009: Conficker: δυνατότητα «ενημέρωσης» και αλλαγής συμπεριφοράς



Βασικά στοιχεία ενός ιού:
Αναγνωρισιμότητα: μπορεί να αναγνωρίσει τον εαυτό του
Αναπαραγωγή: μπορεί να αντιγράφει τον εαυτό του
Ενεργοποίηση: κριτήρια σύμφωνα με τα οποία θα ενεργοποιθεί-επιτεθεί
Περιεχόμενο: καταστροφική ρουτίνα που θα ενεργοποιηθεί
Απόκρυψη: μέθοδοι που χρησιμοποιεί ο ιός για να αποκρύψει την παρουσία του από το χρήστη και τα αντιβιοτικά

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: ημέρα, ώρα, συγκεκριμένη ημερομηνία, πλήθος εκτελέσεων, εξωτερικά συμβάντα)

Πολλοί ιοί προσομοιάζουν τη συμπεριφορά των *παραμενόντων προγραμμάτων*

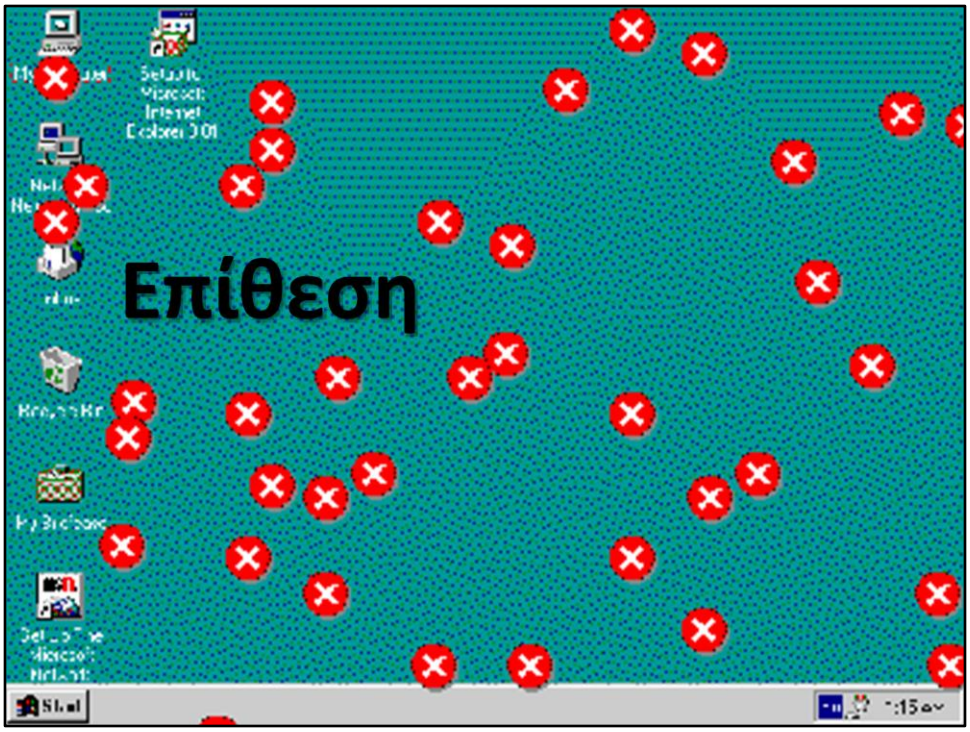
Με τον τρόπο αυτό απεξαρτώνται από τον φορέα τους

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



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)

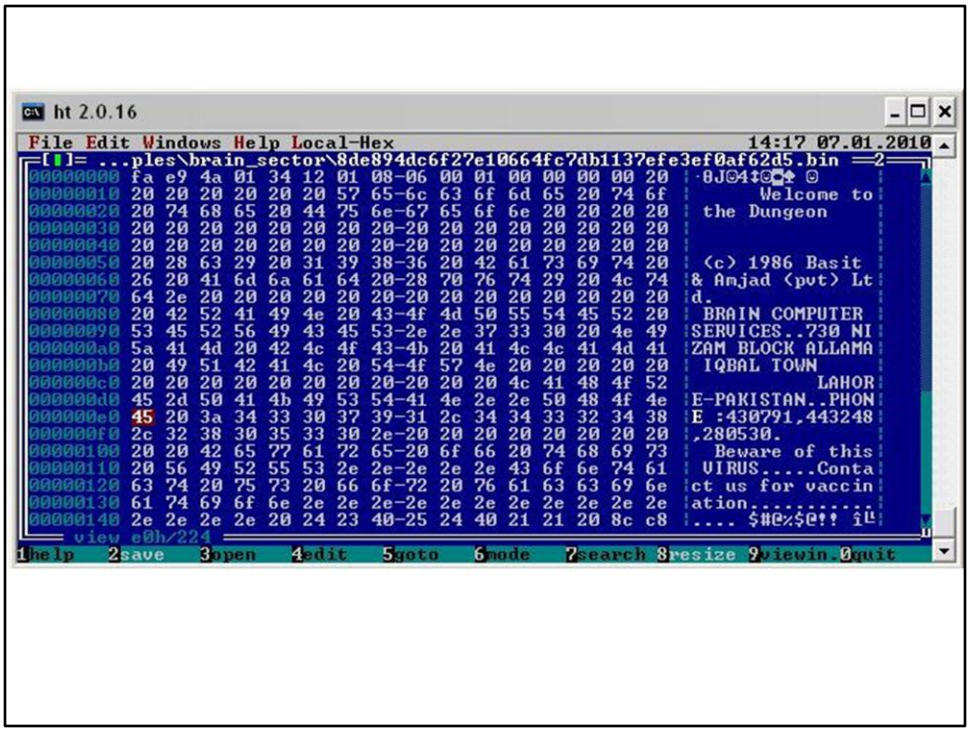
Π.χ.:
Εμφάνιση μηνυμάτων:
WM97/Jerk: I think <username> is a big stupid jerk
Yankee: εμφανίζει Yankee Doodle Dandy στις 17:00 ακριβώς

Άρνηση πρόσβασης:
WM97/NightShade: προστατεύει με password όσα αρχεία είναι ανοιχτά κάθε Παρασκευή και 13

Κλοπή δεδομένων:
Troj/LoveLet-A: στέλνει με e-mail πληροφορίες για το χρήστη και το σύστημα σε μία διεύθυνση στις Φιλιππίνες.

Καταστροφή δεδομένων:
XM/Compatable: αλλάζει δεδομένα σε αρχεία Excel
Michelangelo: σβήνει μέρη του σκληρού δίσκου

Καταστροφή hardware:
CIH: απόπειρα διαγραφής BIOS στις 26 Απριλίου



Ιοί που μολύνουν τομείς εκκίνησης/συστήματος

Κάθε δίσκος/δισκέτα έχει έναν τομέα εκκίνησης, ακόμη και αν δεν περιέχει λειτουργικό σύστημα

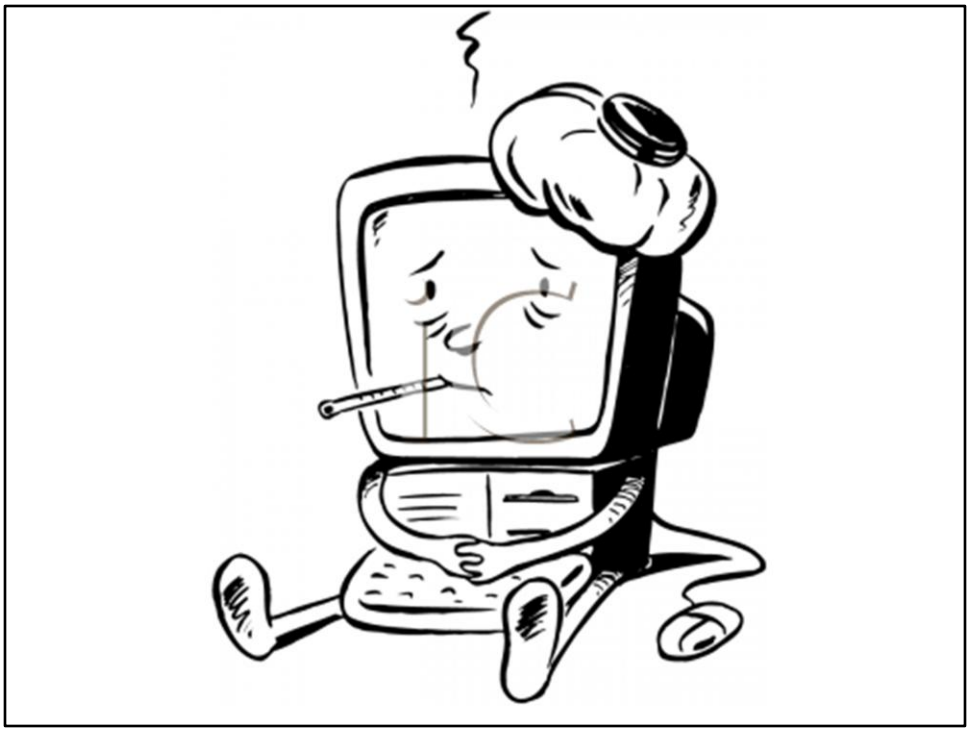
Οι σκληροί δίσκοι έχουν επιπλέον έναν κύριο τομέα εκκίνησης

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

Πρώτος τύπος ιών λόγω της διάδοσης των δισκετών.

Σημερινό ανάλογο: usb disks και autorun



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

Δούρειοι ίπποι
Στόχος ο έλεγχος του συστήματος χωρίς να το γνωρίζει ο χρήστης.
Δυνατότητα κλοπής δεδομένων

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

Οι ιοί μπορεί να εμφανίζονται και να μεταλλάσσονται κρυπτογραφημένα καθιστώντας τον εντοπισμό τους πιο δύσκολο. Ο κώδικας είναι διαφορετικός σε κάθε μετάλλαξη αλλά πρακτικά ισοδύναμος.

Τεχνικές απόκρυψης
Δυνατότητα απόκρυψης από λογισμικό προστασίας, λειτουργικό σύστημα και χρήστη (π.χ. Rootkits).
Μπορούν να ανιχνεύουν διαδικασίες συστήματος και να επιστρέφουν λανθασμένες απαντήσεις.
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

SORRY - but as you're on my address list this virus has probably forwarded itself on to you.

It is easily removed if you don't open the file (jdbgmgr.exe) It has a teddy bear icon and is not detectable by norton or mcafee.

First go to Start then the find or search option. In the files or folders option type jdbgmgr.exe. Search C drive and tick the 'include subfolders' and any other drives you may have. Click 'find now' - the virus has a grey teddy icon. DO NOT OPEN IT. Go to edit (on the menu bar) and 'select all'. Now go to file (on the menu bar) and DELETE. This will send it to the recycle bin so then go and delet or empty it there as well.

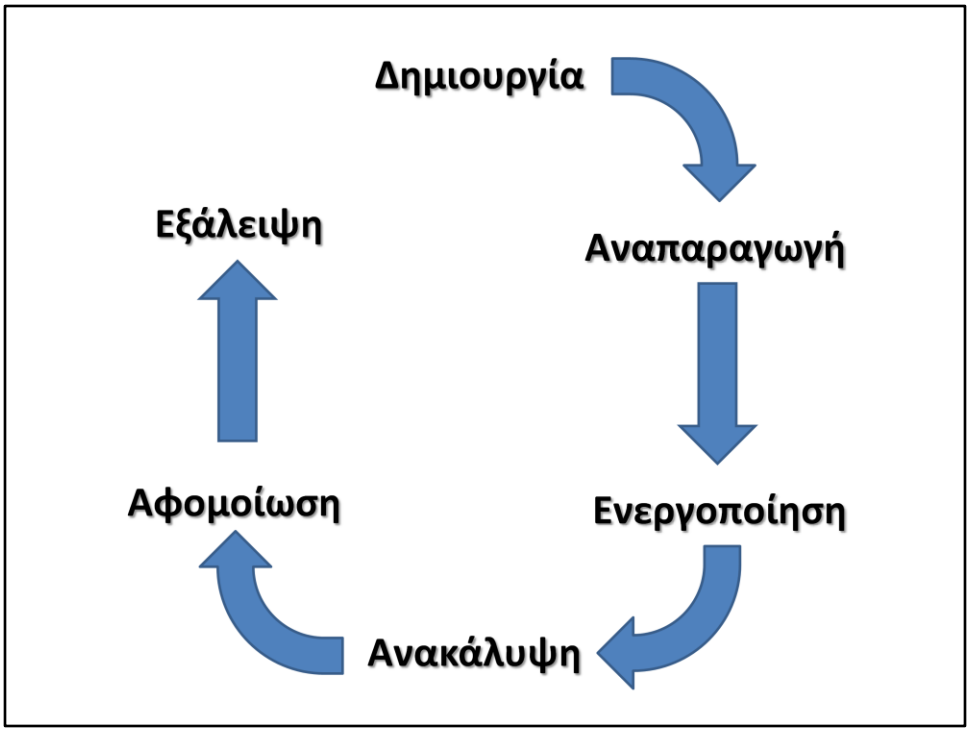
If you find the virus (as I did!) you must contact everyone in your address book and send them these instructions. ASAP.

Ιοί-φάρσες (hoaxes)
Αναφορές σε ανύπαρκτους ιούς
Συνήθως με τη μορφή e-mail τα οποία:
•Προειδοποιούν για πολύ επικίνδυνο ιό
•Ισχυρίζονται ότι προέρχονται από μεγάλη εταιρία κατασκευής αντιβιοτικών
•Προκαλούν να τα προωθήσετε και σε άλλους
•Χρησιμοποιούν «τεχνική» γλώσσα για να πείσουν.

Antivirus
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

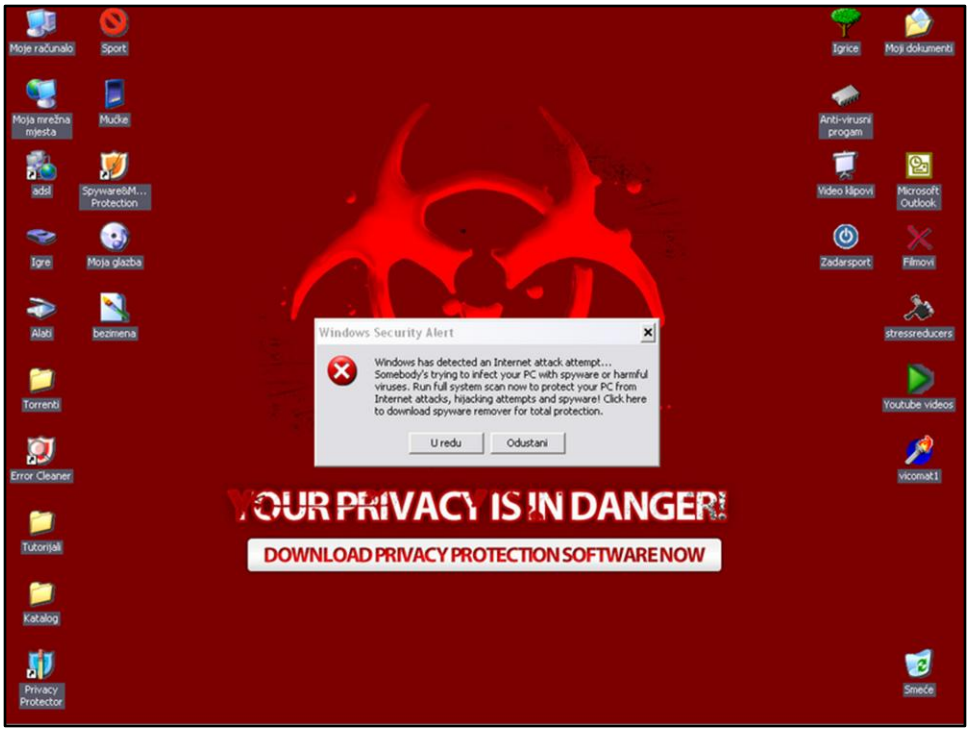
Εντοπισμός «υπογραφών» και αλγοριθμική ανίχνευση
- Χρησιμοποιείται από τα εργαλεία ανίχνευσης που λειτουργούν επίσης και σαν εργαλεία προσδιορισμού ταυτότητας
- Στόχος: εντοπισμός αν υπάρχει ιός σε αρχεία ή στη μνήμη
- Χρήση: συνεχής ή περιοδική
- Ο εντοπισμός «υπογραφών» επιχειρεί να βρει ακολουθίες 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

Τα σύγχρονα αντιβιοτικά είναι πιο εξελιγμένα: προστατεύουν από ποικίλες απειλές (π.χ. δικτυακές, web, κλπ.)
Τα αντίγραφα ασφαλείας (backup) αποτελούν πάντα μια σίγουρη λύση: επαναφορά του συστήματος σε προηγούμενη κατάσταση αρκεί να γνωρίζουμε με σιγουριά πότε μολύνθηκε το σύστημα.



Κύκλος ζωής ιοί

1. Δημιουργία
2. Αναπαραγωγή
3. Ενεργοποίηση
4. Ανακάλυψη
5. Αφομοίωση
6. Εξάλειψη



Rogue software
Κακόβουλο λογισμικό προστασίας: λογισμικό που προσποιείται ότι προστατεύει από ιούς ενώ στην πραγματικότητα είναι το ίδιο ιός.
Εμφανίζεται με παραπλανητικά ονόματα και εικονίδια.
Συνήθως όταν ενεργοποιηθεί εμφανίζει ενοχλητικές οθόνες και μηνύματα ενώ επίσης μολύνει το σύστημα και με άλλους ιούς.
Η αντιμετώπισή του είναι εξαιρετικά δύσκολη.