Κακόβουλο Λογισμικό

Ηλιάδης Ιωάννης

Τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων

Πανεπιστήμιο Αιγαίου

jiliad@aegean.gr

Αθήνα, Ιούλιος 2004

Η έννοια του *Κακόβουλου* Λογισμικού

Το Λογισμικό διαθέτει βούληση;

Το Λογισμικό χαρακτηρίζεται με βάση την πρόθεση του προγραμματιστή;

- Παράδειγμα 1: Προγραμματιστής παράγει λογισμικό με επιβλαβείς συνέπειες έχοντας γνώση των πράξεων του (δόλιοι σκοποί)
- Παράδειγμα 2: Προγραμματιστής παράγει λογισμικό με επιβλαβείς συνέπειες μην έχοντας γνώση των πράξεων του. Ενδεχόμενη άγνοια όσον αφορά στον τρόπο παραγωγής ασφαλούς λογισμικού.

Οριοθέτηση εννοιών

Κακόβουλο Λογισμικό

- το λογισμικό που περιέχει τις *απαιτούμενες εντολές* για μία *επίθεση* σε ένα *υπολογιστικό σύστημα*.

- …*επίθεση*: η παραβίαση (ή η απόπειρα παραβίασης) της εμπιστευτικότητας, ακεραιότητας ή διαθεσιμότητας του συστήματος

Κριτήρια κατηγοριοποίησης

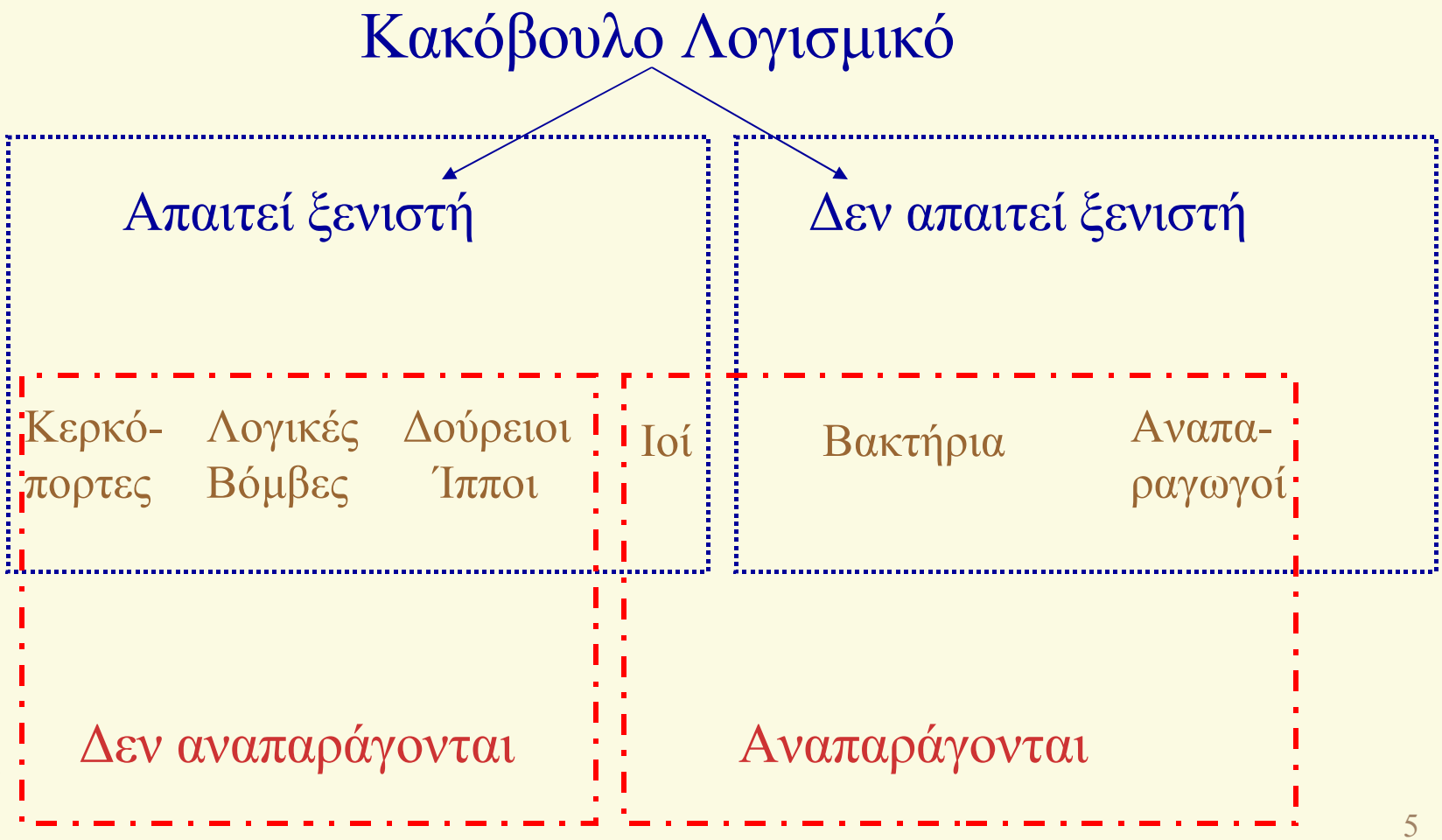
Αυτονομία

- ύπαρξη ανάγκης (ή μη) για λογισμικό-ξενιστή

Αναπαραγωγή

- δυνατότητα αυτό-αναπαραγωγής (ή μη), όταν οι συνθήκες το επιτρέπουν

Κατηγοριοποίηση



Είδη Κακόβουλου Λογισμικού

	Ιομορφικό Κακόβουλο Λογισμικό	**Μη Ιομορφικό Κακόβουλο Λογισμικό**
Μόνιμη ζημιά στο σύστημα	Χαμηλή πιθανότητα	Υψηλή πιθανότητα
Μηχανισμός αναπαραγωγής	Αναπαραγωγή χωρίς ανθρώπινη παρέμβαση	Αναπαραγωγή με ανθρώπινη παρέμβαση
Επεισόδια μεγάλης κλίμακας	Υψηλή πιθανότητα	Χαμηλή πιθανότητα, με εξαιρέσεις
Δυσκολία εντοπισμού	Χαμηλή	Υψηλή
Στοχευμένη απόπειρα επίθεσης	Χαμηλή πιθανότητα	Υψηλή πιθανότητα

University of the Aegean

Ιομορφικό Λογισμικό

Ιός: τμήμα λογισμικού που

ενσωματώνει τον κώδικά του σε ένα πρόγραμμα ξενιστή,

αναπαράγεται με την αντιγραφή του εαυτού του σε άλλα προγράμματα ξενιστές και

εκτελείται στο παρασκήνιο.

Ιομορφικό Λογισμικό:
Κύκλος ζωής

University of the Aegean

Φάση επώασης

- ο ιός παραμένει ανενεργός στο υπολογιστικό σύστημα και ενεργοποιείται από κάποιο γεγονός (π.χ. έλευση χρονικής στιγμής, παρουσία κάποιου αρχείου)

Φάση αναπαραγωγής

- δημιουργία αντιγράφων και ενδεχόμενη ενσωμάτωση σε ξενιστές

Φάση ενεργοποίησης και εκτέλεσης

- εκτέλεση σειράς ενεργειών (payload) με πιθανές επιβλαβείς συνέπειες για το υπολογιστικό σύστημα που φιλοξενεί το ιομορφικό λογισμικό

Ιομορφικό Λογισμικό:
Βασικές υπορουτίνες

University of the Aegean

Υπορουτίνα αναζήτησης

- αναζήτηση νέων ξενιστών

Υπορουτίνα αντιγραφής

- δημιουργία αντιγράφου του ιού και ενσωμάτωση σε νέο ξενιστή

Υπορουτίνα κατά του εντοπισμού

- Παραμετροποίηση τρόπου λειτουργίας υπορουτίνας αναζήτησης και υπορουτίνας αντιγραφής, με σκοπό την αποφυγή εντοπισμού του ιού από αντιβιοτικό λογισμικό

Είδη Ιομορφικού Λογισμικού (1)

Ιοί Τομέα Εκκίνησης

- εγκαθίστανται στον τομέα εκκίνησης ενός δίσκου, μετατοπίζοντας τις υπάρχουσες ρουτίνες

Παρασιτικοί

- ενσωματώνουν τον κώδικα του ιού στον κώδικα εκτελέσιμων αρχείων

Πολυμερείς

- μολύνουν είτε εκτελέσιμα αρχεία (Παρασιτικοί Ιοί) είτε τομείς εκκίνησης (Ιοί Τομέα Εκκίνησης)

Είδη Ιομορφικού Λογισμικού (2)

Διαμένοντες στην Κύρια Μνήμη

- μετά την εκτέλεση του ξενιστή τοποθετούνται στην Κύρια Μνήμη μέχρι τον τερματισμό της λειτουργίας του υπολογιστικού συστήματος

Κρυφοί

- αποκρύπτουν την μόλυνση των αρχείων που έχουν προσβάλλει, αποκτώντας έλεγχο των κλήσεων συστήματος που αφορούν στην πρόσβαση σε αρχεία

Είδη Ιομορφικού Λογισμικού (3)

Κρυπτογραφημένοι

- αποφεύγουν την ανίχνευση, κρυπτογραφώντας το μεγαλύτερο τμήμα του ιού, εκτός από μία ρουτίνα αποκρυπτογράφησης και το αντίστοιχο κλειδί

Πολυμορφικοί

- κρυπτογραφημένοι ιοί, που μεταβάλλουν την ρουτίνα αποκρυπτογράφησης μετά από κάθε προσβολή αρχείου-ξενιστή

Είδη Ιομορφικού Λογισμικού (4)

Ρετρο-Ιοί

- ανιχνεύουν την ύπαρξη αντιβιοτικών προγραμμάτων και τα καθιστούν αναποτελεσματικά

Ιοί που διαγράφουν τμήμα του ξενιστή

Μακρο-Ιοί

- αποτελούνται από ακολουθία εντολών η οποία διερμηνεύεται (interpreted) αντί να εκτελείται (executed), και χρησιμοποιούν συνήθως αρχεία δεδομένων ως ξενιστές

University of the Aegean

Είδη Μη Ιομορφικού Λογισμικού (1)

Κερκόπορτες

- σημεία εισόδου που επιτρέπουν την πρόσβαση σε ένα σύστημα, παρακάμπτοντας την συνηθισμένη διαδικασία ελέγχου πρόσβασης

Λογικές Βόμβες

- προγράμματα που εκτελούν μία ενέργεια η οποία παραβιάζει την πολιτική ασφαλείας ενός συστήματος, όταν πληρείται κάποια λογική συνθήκη στο σύστημα

Είδη Μη Ιομορφικού Λογισμικού (2)

Δούρειοι Ίπποι

- φαινομενικά χρήσιμα προγράμματα που περιλαμβάνουν κρυφές λειτουργίες οι οποίες μπορούν να εκμεταλλευτούν τα δικαιώματα του χρήστη που εκτελεί το πρόγραμμα, με συνέπεια μια απειλή στην ασφάλεια του συστήματος

Αναπαραγωγοί

- προγράμματα που μεταδίδονται από έναν υπολογιστή σε έναν άλλο, δημιουργώντας αντίγραφα του εαυτού τους

Είδη Μη Ιομορφικού Λογισμικού (3)

Βακτήρια

- αναπαράγονται όπως και οι ιοί, και δεν απαιτούν την ύπαρξη ξενιστή. Δεν αλλοιώνουν δεδομένα σκόπιμα.

Παραπλανητική Πληροφόρηση

- διάδοση ψευδούς φήμης σχετικά με την ύπαρξη νεοεμφανιζόμενου Κακόβουλου Λογισμικού

Ιδιαιτερότητες των απειλών από Κακόβουλο Λογισμικό

- **Γενικότητα απειλών:** Το Κακόβουλο Λογισμικό δεν εκμεταλλεύεται συγκεκριμένα ελαττώματα των Λειτουργικών Συστημάτων που προσβάλλει.
- **Έκταση απειλών:** Μία απειλή προερχόμενη από Κακόβουλο Λογισμικό μπορεί να επεκταθεί από ένα υπολογιστικό σύστημα σε ένα άλλο.
- **Αδυναμία εφεδρικών αντιγράφων ασφαλείας:** Το αντίγραφο μπορεί να περιέχει αντίγραφο του Κακόβουλου Λογισμικού.

Εξάπλωση Κακόβουλου Λογισμικού

University of the Aegean

Η αυξανόμενη εξάπλωση οφείλεται:

- στην εξάπλωση της χρήσης των δικτύων δεδομένων
- στην έλλειψη διαχωρισμού μεταξύ αρχείων δεδομένων και εκτελέσιμων αρχείων (π.χ.μακρο-εντολές σε αρχεία δεδομένων)
- στην έλλειψη επίγνωσης από τελικούς χρήστες και διαχειριστές συστημάτων
- στην αναποτελεσματικότητα παραδοσιακών μηχανισμών ελέγχου πρόσβασης

Αντίμετρα κατά Κακόβουλου Λογισμικού

University of the Aegean

Κατηγορίες αντίμετρων:

- *Πρόληψη*
- *Ανίχνευση*
- *Επανόρθωση*

Η συνδυασμένη χρήση των τριών κατηγοριών αντίμετρων οφείλει να οδηγεί σε:

- Ελαχιστοποίηση των προσβολών από Κακόβουλο Λογισμικό, ή
- Ελαχιστοποίηση της ζημίας που μπορεί να επιφέρει η προσβολή από Κακόβουλο Λογισμικό

Επιλογή αντίμετρων κατά Κακόβουλου Λογισμικού

Η επιλογή αντίμετρων (οφείλει να) είναι το τελικό στάδιο της Ανάλυσης Επικινδυνότητας

Η αυθαίρετη επιλογή αντίμετρων ενδέχεται να οδηγήσει

- σε κενά ασφαλείας (μη αναγνωρισμένες ευπάθειες του συστήματος), ή/και
- σε σπατάλη πόρων, χωρίς αντίστοιχο όφελος για την Ασφάλεια του Πληροφοριακού Συστήματος που προστατεύεται

Κατηγοριοποίηση Αντιμέτρων (1)

Κακόβουλο λογισμικό που εμφανίζεται ως ***δεδομένα*** και ως ***εντολές***

- Έλεγχος και πιστοποίηση (από τον διαχειριστή συστήματος) των αρχείων που έχουν δικαίωμα εκτέλεσης
- Οποιαδήποτε μεταβολή σε πιστοποιημένο εκτελέσιμο αρχείο πρέπει να το καθιστά μη εκτελέσιμο, έως ότου ο διαχειριστής πιστοποιήσει εκ νέου το αρχείο αυτό ως εκτελέσιμο

Κατηγοριοποίηση Αντιμέτρων (2)

Διάσχιση Τομέων Προστασίας

- Υποχρεωτικός Έλεγχος Προσπέλασης (Mandatory Access Control – MAC) και Πεδία Προστασίας (Protection Domains)
- Τα υπό προστασία προγράμματα τοποθετούνται στο χαμηλότερο επίπεδο της Πολιτικής Ασφαλείας
- Το συγκεκριμένο αντίμετρο ελαχιστοποιεί παράλληλα και την δυνατότητα διαμοίρασης προγραμμάτων από τους χρήστες

Έλεγχος Ακεραιότητας Αρχείων

- Κρυπτογραφικά αθροίσματα ελέγχου για τον έλεγχο της ακεραιότητας των αρχείων

Κατηγοριοποίηση Αντιμέτρων (3)

Κακόβουλο Λογισμικό που εκμεταλλεύεται τα δικαιώματα του χρήστη

- Ελαχιστοποίηση των αντικειμένων του συστήματος στα οποία έχουν πρόσβαση οι χρήστες:
  - **Μετρικές Ροής Πληροφορίας:** μία πληροφορία είναι διαθέσιμη σε μία διεργασία μόνο όταν η απόστασή της είναι μικρότερη από κάποια τιμή
  - **Μείωση των δικαιωμάτων του χρήστη:** δυναμική μείωση των δικαιωμάτων ενός ύποπτου εκτελέσιμου, με πρωτοβουλία του χρήστη
  - **Εκτέλεση σε περιορισμένο περιβάλλον:** στατικός και δυναμικός έλεγχος ύποπτων προγραμμάτων (sandboxing)

Κατηγοριοποίηση Αντιμέτρων (4)

Έλεγχος ενεργειών που δεν αναφέρονται στις προδιαγραφές

- Εκ των προτέρων υπολογισμός κρυπτογραφικού αθροίσματος ελέγχου για κάθε ακολουθία μη διακλαδωμένων εντολών σε ένα πρόγραμμα
- Υπολογισμός των κρυπτογραφικών αθροισμάτων ελέγχου κατά την εκτέλεση. Σε περίπτωση διαφορών, η ακεραιότητα του προγράμματος έχει παραβιασθεί.
- Απαιτεί ιδιαίτερες διαδικασίες για την διαχείριση των κλειδιών και πιθανόν μειώνει την απόδοση του υπολογιστικού συστήματος σε μεγάλο βαθμό.

Κατηγοριοποίηση Αντιμέτρων (5)

Κρυπτογραφικός έλεγχος ασφαλείας κώδικα

- Διαπίστευση εκτελέσιμου προγράμματος ως προς την ασφάλεια εκτέλεσής του, σύμφωνα με συγκεκριμένες απαιτήσεις/προδιαγραφές του χρήστη
- Η διαπίστευση προέρχεται από τον παραγωγό του κώδικα
- Η διαπίστευση είναι δυνατόν να επαληθευθεί κρυπτογραφικά από τον χρήστη του προγράμματος. Σε περίπτωση μη επαλήθευσης, ο χρήστης δεν εκτελεί το πρόγραμμα

Τεχνικές Αντιμετώπισης Κακόβουλου Λογισμικού (1)

Επίγνωση σε θέματα ασφαλείας

- επίγνωση σε θέματα Κακόβουλου Λογισμικού
- γνώση χειρισμού εφαρμογών κατά Κακόβουλου Λογισμικού
- αποφυγή μεταφόρτωσης και εγκατάστασης μη ελεγμένων προγραμμάτων ή προγραμμάτων από άγνωστες ή μη έμπιστες πηγές

Αντιβιοτικό Λογισμικό

- εφαρμογές που ανιχνεύουν την ύπαρξη ιών και τους αφαιρούν από τα αρχεία ξενιστές, ή απομονώνουν τα αρχεία ξενιστές

Αρχεία Ελέγχου του Λειτουργικού Συστήματος

- εξέταση των Αρχείων Ελέγχου για δραστηριότητα που προδίδει Κακόβουλο Λογισμικό

Τεχνικές Αντιμετώπισης Κακόβουλου Λογισμικού (2)

Αυστηρά μέτρα ασφαλείας

- αυστηρά δικαιώματα πρόσβασης
- εκτέλεση εφαρμογών με τα ελάχιστα δικαιώματα που απαιτούν (least privilege)

Απαγόρευση μεταφόρτωσης εκτελέσιμου κώδικα

- έλεγχος και περιορισμός του κώδικα που είναι δυνατόν να μεταφορτωθεί (πιθανό σημείο ελέγχου: οι Πληρεξούσιοι)

Απομόνωση

- απομόνωση τμημάτων Πληροφοριακών Συστημάτων που περιέχουν διαβαθμισμένες πληροφορίες, από άλλα τμήματα που περιέχουν μη διαβαθμισμένες πληροφορίες
- απομόνωση τμημάτων Πληροφοριακών Συστημάτων που επικοινωνούν με εξωτερικά ΠΣ, από τα υπόλοιπα τμήματα του ΠΣ ενός οργανισμού (Demilitarised Zone)

Τεχνικές Αντιμετώπισης Κακόβουλου Λογισμικού (3)

Αναχώματα Ασφαλείας

- περιορισμός της δυνατότητας του Κακόβουλου Λογισμικού να εξαπλωθεί σε περισσότερα συστήματα ενός ΠΣ

Εργαλεία Ανίχνευσης Εισβολών

- ανίχνευση Κακόβουλου Λογισμικού με βάση γνωστές συμπεριφορές τυπικών προγραμμάτων Κακόβουλου Λογισμικού
- Ανίχνευση Κακόβουλου Λογισμικού με βάση συμπεριφορές που διαφέρουν από τις τυπικές συμπεριφορές έγκυρων χρηστών

Συνεργασία με τους οργανισμούς που προσφέρουν προϊόντα υλικού και λογισμικού για προστασία από Κακόβουλο Λογισμικό

- ενημέρωση των οργανισμών αυτών σε περίπτωση εμφάνισης προγράμματος που ενδέχεται να συνιστά Κακόβουλο Λογισμικό άλλα δεν έχει ήδη καταγραφεί

Τεχνικές Αντιμετώπισης Κακόβουλου Λογισμικού (4)

Διατυπωμένη διαδικασία ανάνηψης από προσβολή και περιορισμού Κακόβουλου Λογισμικού

- Απομόνωση προσβεβλημένων συστημάτων
- Απομάκρυνση Κακόβουλου Λογισμικού από προσβεβλημένο σύστημα
- Αποκατάσταση ακεραιότητας προσβεβλημένου συστήματος
- η διαδικασία πρέπει να είναι τεκμηριωμένη και γνωστή εκ των προτέρων σε όσους οφείλουν να την ακολουθήσουν
- ενημέρωση τελικών χρηστών σχετικά με ενδεχόμενες ενέργειες που οφείλουν να κάνουν οι ίδιοι σε περίπτωση εμφάνισης εφαρμογών που ενδέχεται να συνιστούν Κακόβουλο Λογισμικό

Αντιβιοτικό Λογισμικό

Το αντιβιοτικό λογισμικό διεξάγει:

- ανίχνευση Κακόβουλου Λογισμικού σε ένα σύστημα
- ταυτοποίηση του Κακόβουλου Λογισμικού που έχει προσβάλλει το σύστημα
- Αφαίρεση των τμημάτων κώδικα του Κακόβουλου Λογισμικού από τα αρχεία, ή (αν η αφαίρεση δεν είναι δυνατή) απομόνωση των προσβεβλημένων αρχείων

Αντιβιοτικό Λογισμικό:
Κατηγοριοποίηση Τεχνικών

University of the Aegean

Ανάλογα με τη Σειρά Εκτέλεσης (Order of Play)

- Εκτέλεση Πρώτου Επιπέδου: ανίχνευση ιομορφών προτού διεισδύσουν στο σύστημα
- Εκτέλεση Δευτέρου Επιπέδου: ανίχνευση ιομορφών που έχουν ήδη διεισδύσει το σύστημα

Σύμφωνα με το Χρόνο Εκτέλεσης (Time of Play)

- Κατά την Πρόσβαση: όλα τα αρχεία που προσπελαύνονται από οποιαδήποτε εφαρμογή ελέγχονται, χωρίς μεσολάβηση του χρήστη
- Κατά τη Ζήτηση: ο χρήστης διενεργεί έλεγχο των αρχείων ενός συστήματος σε χρόνο της επιλογής του

Αντιβιοτικό Λογισμικό:
Τεχνικές (1)

University of the Aegean

- Ανιχνευτές
  - Πρώτης γενεάς: ανίχνευση ιομορφών με χρήση υπογραφών (ακολουθίες κώδικα) ταυτοποιημένων ιομορφών
  - Δεύτερης γενεάς: χρήση ευριστικών μεθόδων
- Ελεγκτές Ακεραιότητας
  - Αποθηκεύουν *δεδομένα ακεραιότητας* των αρχείων ενός συστήματος, παρέχοντας έτσι την δυνατότητα στον διαχειριστή να γνωρίζει ποια αρχεία έχουν τροποποιηθεί, από το χρονικό σημείο της τελευταίας καταγραφής δεδομένων ακεραιότητας. Η τροποποίηση ορισμένων αρχείων (π.χ. εκτελέσιμα) πρέπει να εξετάζεται περαιτέρω από τους διαχειριστές

Αντιβιοτικό Λογισμικό:
Τεχνικές (2)

University of the Aegean

Αντιβιοτικό Λογισμικό Ελέγχου Συμπεριφοράς

- εντοπίζει συγκεκριμένες ύποπτες ενέργειες λογισμικού (π.χ. εγγραφή δεδομένων σε ένα εκτελέσιμο αρχείο)

Ανιχνευτές Εικονικής Μηχανής

- Εξομοίωση της εκτέλεσης ενός προγράμματος σε ελεγχόμενο περιβάλλον με σκοπό τον εντοπισμό ιομορφικής συμπεριφοράς

Μελέτες Περίπτωσης

Μεθοδολογία Μελέτης

- Τρόποι Μετάδοσης
- Κακόβουλες Ενέργειες
- Τρόποι Ενεργοποίησης

Περιπτώσεις Κακόβουλου Λογισμικού

- Ιός CIH
- Μακρο-Ιός Melissa
- Μακρο-Ιός ILoveYou