

Ε Κ Δ Ο Σ Ε Ι Σ Κ Λ Ε Ι Δ Α Ρ Ι Θ Μ Ο Σ

ΑΣΦΑΛΕΙΑ ΥΠΟΛΟΓΙΣΤΩΝ

ΑΡΧΕΣ ΚΑΙ ΠΡΑΚΤΙΚΕΣ

3η αμερικανική έκδοση



William Stallings • Lawrie Brown



Κεφάλαιο 6

Κακόβουλο λογισμικό

Κακόβουλο λογισμικό

Στην Ειδική Έκδοση [SOUP13] , το κακόβουλο λογισμικό ορίζεται ως

«ένα πρόγραμμα το οποίο εισάγεται σε ένα σύστημα, συνήθως κρυφά, με στόχο να παραβιαστεί η εμπιστευτικότητα, ακεραιότητα, ή διαθεσιμότητα των δεδομένων, των εφαρμογών, ή του λειτουργικού συστήματος του θύματος, ή να προκληθεί με οποιονδήποτε άλλο τρόπο ενόχληση ή αναστάτωση στο θύμα.»



Πίνακας 6.1 Ορολογία κακόβουλου λογισμικού

Όνομα	Περιγραφή	Προγράμματα αποστολής ενοχλητικών μαζικών μηνυμάτων (spammer programs)	Χρησιμοποιούνται για τη μαζική αποστολή μεγάλου όγκου ανεπιθύμητων μηνυμάτων ηλεκτρονικού ταχυδρομείου.
Προηγμένη επίμονη απειλή (APT)	Εγκληματικές ενέργειες στον κυβερνοχώρο εναντίον επιχειρηματικών και πολιτικών στόχων με χρήση ποικίλων τεχνολογιών εισβολής και κακόβουλου λογισμικού, οι οποίες διαπράττονται επίμονα και αποτελεσματικά εναντίον συγκεκριμένων στόχων για εκτεταμένο χρονικό διάστημα: συγνά αποδίοντα σε οργανώσεις χρηματοδοτούμενες από κυβερνήσεις κρατών.		
Λογισμικό ανεπιθύμητων διαφρήμεσεων (adware)	Διαφημίσεις που έχουν ενσωματωθεί σε λογισμικό. Προκαλεί εμφάνιση αναδυόμενων διαφημίσεων ή ανακατεύθυνση του φυλλομετρητή σε κάποιον ιστότοπο εμπορικού χαρακτήρα.		
Κιτ επίθεσης	Σύνολο εργαλείων για την αντόματη παραγωγή νέου κακόβουλου λογισμικού με χρήση ποικίλων μηχανισμών εξάπλωσης και απελευθέρωσης φορτίου.		
Λογισμικό αντόματης απόκτησης δικαιωμάτων υπερχρήστη (auto-rooter)	Κακόβουλα εργαλεία για χάρη τα οποία χρησιμοποιούνται για την απομακρυσμένη παραβίαση νέων μηχανημάτων.		
Κερκόπορτα (backdoor), ή μυστική πόρτα (trapdoor)	Οποιοσδήποτε μηχανισμός παρακάπτει κάποιον τυπικό έλεγχο ασφαλείας: μπορεί να επιτρέψει τη μη εξουσιοδοτημένη πρόσβαση στις λειτουργίες ενός προγράμματος ή σε ένα εκτεθειμένο σύστημα.		
Προγράμματα λήγης αρχείων (downloaders)	Κώδικας που εγκαθιστά άλλα στοιχεία σε ένα μηχάνημα το οποίο δέχεται επίθεση. Συνήθως συμπεριλαμβάνεται στον κώδικα του κακόβουλου λογισμικού που παρεισφέρει αρχικά σε ένα εκτεθειμένο σύστημα με στόχο να εισαγάγει στη συνέχεια κάποιο μεγαλύτερο πακέτο κακόβουλου λογισμικού.		
Κρυφή λήψη (drive-by-download)	Μια επίθεση που χρησιμοποιεί τον κώδικα ενός εκτεθειμένου ιστότοπου και εκμεταλλεύεται κάποια ευπάθεια του φυλλομετρητή προκειμένου να επιτεθεί σε ένα σύστημα πελάτη όταν προβάλλεται ο ιστότοπος.		
Προγράμματα εκμετάλλευσης ευπαθειών (exploits)	Κώδικας επικεντρωμένος σε μία μόνο ευπάθεια ή σε ένα σύνολο ευπαθειών.		
Προγράμματα κατακλυσμού (flooders) – πελάτης DOS	Χρησιμοποιούνται για την παραγωγή μεγάλου όγκου δεδομένων σε επιθέσεις εναντίον δικτυωμένων υπολογιστικών συστημάτων εκτελούν κάποια μορφή επίθεσης άρνησης εξηνπρέπησης (DoS).		
Προγράμματα καταγραφής πληκτρολογήσεων	Υποκλέπτουν οτιδήποτε πληκτρολογείται σε ένα εκτεθειμένο σύστημα.		
Λογική βόμβα (logic bomb)	Κώδικας που εισάγεται σε κακόβουλο λογισμικό από κάποιον εισβολέα. Η λογική βόμβα παραμένει αδρανής μέχρι να ικανοποιηθεί μια προκαθορισμένη συνθήκη τότε ο κώδικας ξεκινά την εκτέλεση κάποιας μη εξουσιοδοτημένης ενέργειας.		
Μακροϊός (macro virus)	Ένας τύπος ιού που χρησιμοποιεί κώδικα μακροεντολών ή σεναρίων συνήθως είναι ενσωματωμένος σε κάποιο έγγραφο και ενεργοποιείται όταν ο χρήστης βλέπει ή επεξεργάζεται το έγγραφο· η εκτέλεση του κώδικα στοχεύει στην αναπαραγωγή του ιού και τη μόλυνση παρόμοιων εγγράφων.		
Κινητός κώδικας (mobile code)	Λογισμικό (π.χ. σενάρια, μακροεντολές, κ.λπ.) που μπορεί να αποσταλεί χωρίς τροποποίηση σε ετερογενή υπολογιστικά περιβάλλοντα και να εκτελεστεί με πανομοιότυπη σημασιολογία.		
Κιτ υπερχρήστη (rootkit)	Σύνολο εργαλείων για χάρη τα οποία χρησιμοποιεί ένας επιτιθέμενος μετά την παραβίαση ενός υπολογιστικού συστήματος και την απόκτηση δικαιωμάτων πρόσβασης επιπλέου υπερχρήστη.		

(Ο πίνακας βρίσκεται στη σελ. 231 του βιβλίου.)



Ταξινόμηση του κακόβουλου λογισμικού

Δύο γενικές κατηγορίες:

Αρχικά με βάση τον τρόπο που διαδίδεται ή εξαπλώνεται για να φτάσει στους στόχους του

Έπειτα με βάση τις ενέργειες, ή φορτία, που εκτελεί μόλις φτάσει στον στόχο

Άλλη ταξινόμηση:

Λογισμικό που χρειάζεται πρόγραμμα-ξενιστή (παρασιτικός κώδικας όπως οι ΙΟΙ)

Ανεξάρτητα, αυτόνομα προγράμματα (σκουλήκια, Δούρειοι ίπποι, και ρομπότ)

Λογισμικό που δεν αναπαράγεται (Δούρειοι ίπποι και ενοχλητικά μαζικά e-mail)

Λογισμικό που αναπαράγεται (ΙΟΙ και σκουλήκια)

Τύποι κακόβουλου λογισμικού (malware)

Οι μηχανισμοί εξάπλωσης περιλαμβάνουν:

- Μόλυνση υπάρχοντος εκτελέσιμου ή ερμηνευόμενου περιεχομένου από ιούς και επακόλουθη εξάπλωσή του σε άλλα συστήματα
- Εκμετάλλευση ευπαθειών του λογισμικού είτε τοπικά είτε μέσω δικτύου από σκουλήκια ή κρυφές λήψεις με απώτερο στόχο να μπορέσει το κακόβουλο λογισμικό να αναπαραχθεί
- Επιθέσεις κοινωνικής μηχανικής οι οποίες πείθουν τους χρήστες να παρακάμψουν μηχανισμούς ασφαλείας προκειμένου να εγκαταστήσουν Δούρειους ίππους ή να απαντήσουν σε επιθέσεις ηλεκτρονικού ψαρέματος



Στις ενέργειες, ή φορτία, που εκτελούνται από το κακόβουλο λογισμικό μόλις αυτό φτάσει στο σύστημα-στόχο περιλαμβάνονται:

- Άλλοιωση αρχείων δεδομένων ή αρχείων του συστήματος
- Κλοπή υπηρεσιών με στόχο να μετατραπεί το σύστημα σε πράκτορα επίθεσης-ζόμπι ο οποίος θα χρησιμοποιηθεί ως μέρος κάποιου δικτύου ρομπότ (botnet)
- Κλοπή πληροφοριών από το σύστημα/καταγραφή πληκτρολογήσεων
- Συγκάλυψη/μη αντιληπτή παρουσία στο σύστημα

Κιτ επίθεσης

- Αρχικά, η ανάπτυξη και χρήση του κακόβουλου λογισμικού απαιτούσε σημαντικές τεχνικές δεξιότητες από τους προγραμματιστές
 - Η έλευση των κιτ εργαλείων δημιουργίας ιών, και αργότερα –στη δεκαετία του 2000– των πιο γενικών κιτ επίθεσης, συνέβαλλε στην ανάπτυξη και χρήση του κακόβουλου λογισμικού
- Τα κιτ εργαλείων είναι συχνά γνωστά και ως «*crimeware*»
 - Περιλαμβάνουν ποικίλους μηχανισμούς εξάπλωσης και υπομονάδες φορτίων, που μπορούν να χρησιμοποιηθούν ακόμα και από αρχάριους
 - Οι πολλές παραλλαγές που μπορούν να παραχθούν από τους επιτιθέμενους με χρήση τέτοιων κιτ δημιουργεί σημαντικό πρόβλημα σε όσους έχουν την ευθύνη της προστασίας συστημάτων από τέτοιες απειλές
- Ευρέως χρησιμοποιούμενα κιτ εργαλείων:
 - Zeus
 - Blackhole
 - Sakura
 - Phoenix

Πηγές επιθέσεων

- Μια άλλη σημαντική εξέλιξη στον χώρο του κακόβουλου λογισμικού είναι η αλλαγή στο προφίλ των επιτιθέμενων από μεμονωμένα άτομα , τα οποία συχνά ήθελαν να δείξουν τις τεχνικές γνώσεις και δεξιότητές τους στους ομοιδεάτες τους, σε πιο οργανωμένες και επικίνδυνες πηγές επιθέσεων:



- Αυτό έχει αλλάξει σε μεγάλο βαθμό τους διαθέσιμους πόρους και τα κίνητρα πίσω από την έξαρση του κακόβουλου λογισμικού, και έχει οδηγήσει στην ανάπτυξη μιας ακμάζουσας παραοικονομίας που περιλαμβάνει την πώληση κιτ επίθεσης, καθώς και την παροχή πρόσβασης σε εκτεθειμένους υπολογιστές υπηρεσίας και κλεμμένες πληροφορίες

Προηγμένες Επίμονες Απειλές (APT)

- Οργανωμένη, επίμονη εφαρμογή μιας μεγάλης γκάμας κακόβουλου λογισμικού και τεχνολογιών εισβολής σε επιλεγμένους στόχους, συνήθως επιχειρηματικούς ή πολιτικούς
- Αποδίδονται σε οργανώσεις χρηματοδοτούμενες από κυβερνήσεις κρατών και σε εγκληματικά συνδικάτα
- Διαφέρουν από άλλους τύπους επιθέσεων λόγω της προσεκτικής επιλογής στόχων και των συγκεκαλυμμένων προσπαθειών εισβολής για μεγάλα χρονικά διαστήματα
- Επιθέσεις που τράβηξαν τα φώτα της δημοσιότητας:
Aurora, RSA, APT1, και Stuxnet

Χαρακτηριστικά των APT

Προηγμένες

- Οι επιτιθέμενοι χρησιμοποιούν μια μεγάλη γκάμα τεχνολογιών εισβολής και κακόβουλου λογισμικού, συμπεριλαμβανομένης της ανάπτυξης προσαρμοσμένου λογισμικού, αν αυτό κριθεί απαραίτητο
- Τα επιμέρους τμήματα του λογισμικού δεν είναι υποχρεωτικά προηγμένα από τεχνικής άποψης, ωστόσο είναι προσεκτικά διαλεγμένα ώστε να ταιριάζουν με τον επιλεγμένο στόχο

Επίμονες

- Οι επιθέσεις εξαπολύονται με αμείωτη ένταση και για μεγάλο χρονικό διάστημα εναντίον του επιλεγμένου στόχου ώστε να μεγιστοποιηθεί η πιθανότητα επιτυχίας
- Μπορεί να εφαρμοστούν σταδιακά διάφορες επιθέσεις μέχρι να παραβιαστεί ο στόχος

Απειλές

- Οι απειλές για τους επιλεγμένους στόχους είναι το αποτέλεσμα της πρόθεσης των οργανωμένων, ικανών και καλά χρηματοδοτούμενων επιτιθέμενων να παραβιάσουν τους ειδικά επιλεγμένους στόχους τους
- Η ενεργή συμμετοχή του ανθρώπινου παραγόντα στη διαδικασία αυξάνει πολύ το επίπεδο της απειλής σε σύγκριση με το επίπεδο απειλών που προκύπτουν από αυτοματοποιημένα εργαλεία επίθεσης, καθώς και την πιθανότητα επιτυχούς έκβασης της επίθεσης

Επιθέσεις APT

- **Σκοπός:**
 - Ποικίλει από την κλοπή πνευματικής ιδιοκτησίας ή δεδομένων που σχετίζονται με την ασφάλεια και τις υποδομές έως τη διακοπή της λειτουργίας των φυσικών υποδομών
- **Τεχνικές που χρησιμοποιούνται:**
 - Κοινωνική μηχανική
 - Ηλεκτρονικό «καμάκωμα» (spear-phishing) μέσω email
 - Κρυφές λήψεις (drive-by-downloads) από επιλεγμένους εκτεθειμένους ιστότοπους τους οποίους είναι πιθανό να επισκεφθεί το προσωπικό του οργανισμού που έχει μπει στο στόχαστρο του επιτιθέμενου
- **Πρόθεση των επιτιθέμενων:**
 - Να μολύνουν τον στόχο με εξελιγμένο κακόβουλο λογισμικό μέσω πολλών μηχανισμών εξάπλωσης και απελευθέρωσης φορτίων
 - Μόλις αποκτήσουν για πρώτη φορά πρόσβαση στα συστήματα του οργανισμού-στόχου, χρησιμοποιούν και άλλα εργαλεία επίθεσης προκειμένου να διατηρήσουν και να επεκτείνουν την πρόσβασή τους

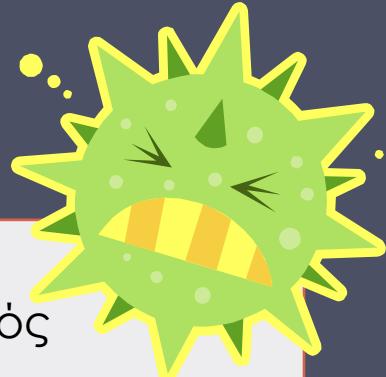


Ioí



- Λογισμικό το οποίο «μολύνει» προγράμματα
 - Τα τροποποιεί ώστε να περιλαμβάνουν ένα αντίγραφο του ιού
 - Δημιουργούνται αντίγραφα του ιού, τα οποία μπορούν να μολύνουν άλλο περιεχόμενο
 - Εύκολη εξάπλωση μέσω δικτυακών περιβαλλόντων
- Όταν ένας ιός προσαρτάται σε κάποιο εκτελέσιμο πρόγραμμα, μπορεί να εκτελέσει οποιαδήποτε από τις επιτρεπτές ενέργειες του προγράμματος
 - Εκτελείται κρυφά όταν εκτελείται το πρόγραμμα-ξενιστής
- Σχεδιασμένοι για συγκεκριμένο λειτουργικό σύστημα και υλικό
 - Εκμεταλλεύονται λεπτομέρειες και αδυναμίες

Συστατικά στοιχεία ιών



Μηχανισμός μόλυνσης

- Οι τρόποι με τους οποίους διαδίδεται ή εξαπλώνεται ένας ιός
- Γνωστός και ως φορέας μόλυνσης (infection vector)

Σκανδάλη

- Το συμβάν ή συνθήκη που καθορίζει πότε ενεργοποιείται ή απελευθερώνεται το φορτίο
- Επίσης γνωστό και ως λογική βόμβα (logic bomb)

Φορτίο

- Οτιδήποτε προκαλεί ο ιός, (επιπλέον της εξάπλωσης)
- Μπορεί να περιλαμβάνει την πρόκληση ζημιάς ή καλοήθους, αλλά εμφανούς, δραστηριότητας



Φάσεις ενός ιού

Λανθάνουσα φάση

Ο ιός είναι αδρανής

Τελικά θα ενεργοποιηθεί από κάποιο συμβάν

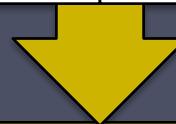
Δεν περνούν όλοι οι ιοί από αυτή τη φάση



Φάση ενεργοποίησης

Ο ιός ενεργοποιείται ώστε να εκτελέσει την ενέργεια για την οποία έχει σχεδιαστεί

Μπορεί να προκληθεί από διάφορα συμβάντα του συστήματος



Φάση εξάπλωσης

Ο ιός εισάγει ένα αντίγραφο του εαυτού του σε άλλα προγράμματα ή σε ορισμένες περιοχές συστήματος στον δίσκο

Το αντίγραφο μπορεί να μην είναι πανομοιότυπο με την έκδοση που εξαπλώνεται

Κάθε μολυσμένο πρόγραμμα θα περιέχει πλέον έναν κλώνο του ιού, και κάθε κλώνος θα εισέλθει με τη σειρά του σε φάση εξάπλωσης



Φάση εκτέλεσης

Εκτελείται η επιδιωκόμενη ενέργεια

Μπορεί να προκαλεί ζημιές ή όχι

Δομή ενός ιού



```
program V
1234567;

procedure attach-to-program;
begin
repeat
    file := get-random-program;
until first-program-line ≠ 1234567;
prepend V to file;
end;

procedure execute-payload;
begin
    (* εκτέλεση ενεργειών φορτίου *)
end;

procedure trigger-condition;
begin
    (* επιστροφή τιμής true αν η συνθήκη ενεργοποίησης είναι αληθής *)
end;

begin (* κύριο τμήμα ενεργειών *)
    attach-to-program;
    if trigger-condition then execute-payload;
    goto original program code;
end;
```

```
program CV
1234567;

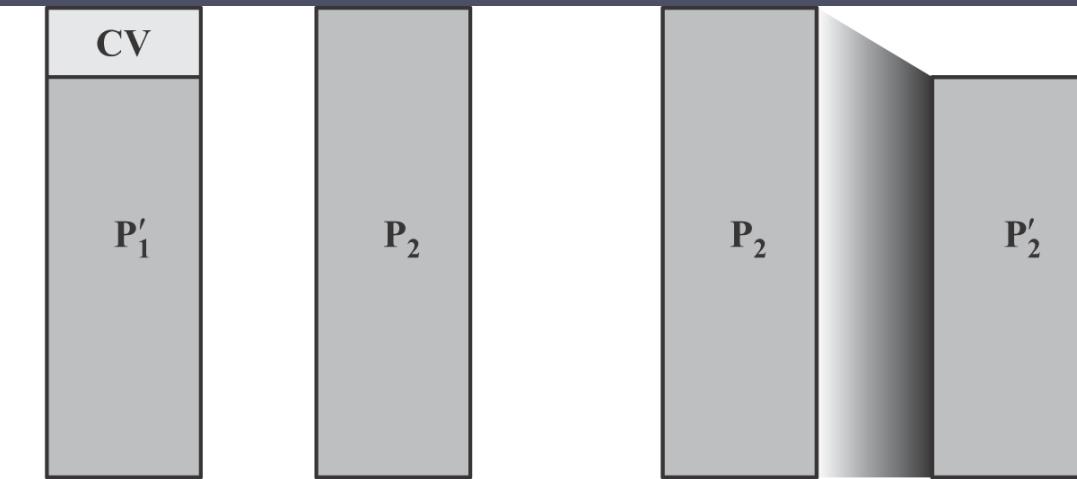
procedure attach-to-program;
begin
repeat
    file := get-random-program;
until first-program-line ≠ 1234567;
compress file;      (* t1 *)
prepend CV to file;  (* t2 *)
end;

begin (* κύριο τμήμα ενεργειών *)
    attach-to-program;
    uncompress rest of this file into tempfile;   (* t3 *)
    execute tempfile;   (* t4 *)
end;
```

(a) Ένας απλός ιός

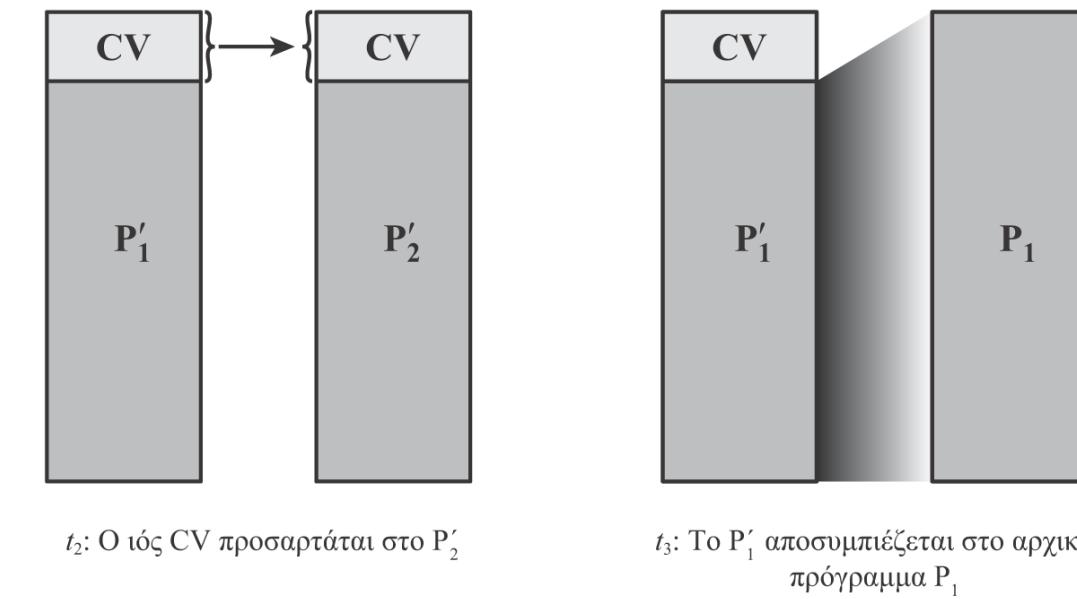
(β) Ένας ιός συμπίεσης

Εικόνα 6.1 Παράδειγμα λογικής ενός ιού



t_0 : Το P'_1 αποτελεί μολυσμένη έκδοση του P_1 .
το P_2 είναι καθαρό

t_1 : Το P_2 συμπιέζεται στο P'_2



Εικόνα 6.2 Ένας ιός συμπίεσης



Ταξινόμηση ιών

Με βάση τον στόχο

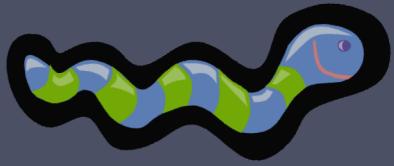
- Ιός τομέα εκκίνησης
 - Μολύνει μια βασική ή απλή εγγραφή εκκίνησης και εξαπλώνεται όταν ένα σύστημα εκκινείται από τον δίσκο που περιέχει τον ιό
- Ιός αρχείων
 - Μολύνει αρχεία τα οποία το λειτουργικό σύστημα ή κέλυφος θεωρεί εκτελέσιμα
- Μακροϊός
 - Μολύνει αρχεία με κώδικα μακροεντολών ή σεναρίων ο οποίος ερμηνεύεται από κάποια εφαρμογή
- Πολυτυμηματικός ιός
 - Μολύνει αρχεία με πολλούς τρόπους

Με βάση τη στρατηγική απόκρυψης

- Κρυπτογραφημένος ιός
 - Ένα τμήμα του ιού δημιουργεί τυχαίο κλειδί κρυπτογράφησης και κρυπτογράφει το υπόλοιπό κομμάτι του ιού
- Συγκεκαλυμμένος ιός
 - Μορφή ιού ειδικά σχεδιασμένη να αποφεύγει την ανίχνευση από λογισμικό προστασίας από ιούς
- Πολυμορφικός ιός
 - Ιός που μεταλλάσσεται με κάθε μόλυνση
- Μεταμορφικός ιός
 - Ιός που μεταλλάσσεται και ξαναγράφει τον εαυτό του εντελώς σε κάθε επανάληψη· ενδέχεται να αλλάζει και συμπεριφορά και έμφανιση

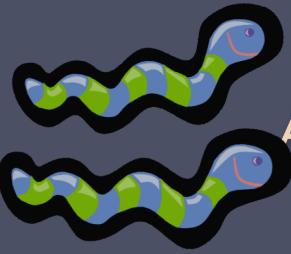
Μακροϊοί και ιοί σεναρίων

- Πολύ διαδεδομένοι στα μέσα της δεκαετίας του 1990
 - Ανεξάρτητοι από το υπολογιστικό περιβάλλον
 - Μολύνουν έγγραφα (όχι εκτελέσιμα τμήματα κώδικα)
 - Εξαπλώνονται εύκολα
- Εκμεταλλεύονται την υποστήριξη μακροεντολών από εφαρμογές της σουίτας MS Office
 - Οι πιο πρόσφατες εκδόσεις των προϊόντων παρέχουν προστασία
- Έχουν αναπτυχθεί διάφορα προγράμματα προστασίας από μακροϊούς, οπότε έχουν πάψει να αποτελούν την κυριαρχη απειλή στον χώρο των ιών



Σκουλήκια

- Πρόγραμμα που αναζητεί με ενεργό τρόπο περισσότερα μηχανήματα τα οποία μπορεί να μολύνει· στη συνέχεια κάθε μολυσμένο μηχάνημα λειτουργεί ως μια «εξέδρα αυτοματοποιημένης εκτόξευσης» από όπου μπορούν να εξαπολυθούν επιθέσεις εναντίον άλλων μηχανημάτων
- Εκμεταλλεύονται ευπάθειες του λογισμικού σε προγράμματα πελάτη ή διακομιστή
- Μπορούν να χρησιμοποιούν συνδέσεις δικτύου για να εξαπλώνονται από το ένα σύστημα στο άλλο
- Εξαπλώνονται μέσω κοινόχρηστων μέσων (μονάδες δίσκων USB ή δίσκοι CD και DVD)
- Τα σκουλήκια ηλεκτρονικού ταχυδρομείου εξαπλώνονται με τη βοήθεια κώδικα μακροεντολών ή σεναρίων ο οποίος περιλαμβάνεται σε συνημμένα έγγραφα μηνυμάτων ή σε μεταφορές αρχείων μέσω εφαρμογών αποστολής άμεσων μηνυμάτων
- Μόλις το σκουλήκι ενεργοποιηθεί, ενδέχεται να αναπαραχθεί και να εξαπλωθεί εκ νέου
- Συνήθως μεταφέρει κάποια μορφή φορτίου
- Η πρώτη γνωστή υλοποίηση σκουληκιού έλαβε χώρα στα εργαστήρια Palo Alto Labs της Xerox στις αρχές της δεκαετίας του 1980



Αναπαραγωγή σκουληκιών

Ηλεκτρονικό ταχυδρομείο
ή αποστολή άμεσων
μηνυμάτων

- Το σκουλήκι στέλνει ένα αντίγραφό του σε άλλα συστήματα
- Στέλνει το αντίγραφο ως συνημμένο αρχείο μέσω κάποιας υπηρεσίας αποστολής άμεσων μηνυμάτων

Κοινή χρήση αρχείων

- Το σκουλήκι είτε δημιουργεί ένα αντίγραφό του είτε μολύνει ως ίός ένα αρχείο σε αφαιρούμενα μέσα

Απομακρυσμένη εκτέλεση

- Το σκουλήκι εκτελεί ένα αντίγραφό του σε κάποιο άλλο σύστημα

Απομακρυσμένη
προσπέλαση
ή μεταφορά αρχείων

- Το σκουλήκι χρησιμοποιεί μια υπηρεσία απομακρυσμένης προσπέλασης ή μεταφοράς αρχείων σε κάποιο άλλο σύστημα για να αντιγράψει τον εαυτό του από το ένα σύστημα στο άλλο

Απομακρυσμένη σύνδεση

- Αφού το σκουλήκι συνδεθεί σε ένα απομακρυσμένο σύστημα ως χρήστης, χρησιμοποιεί εντολές για να αντιγράψει τον εαυτό του από το ένα σύστημα στο άλλο

Εντοπισμός στόχων

• Σάρωση (ή «δακτυλοσκόπηση»)

- Πρώτη ενέργεια στη φάση εξάπλωσης ενός δικτυακού σκουληκιού
- Ψάχνει για άλλα συστήματα για να τα μολύνει

Πιθανές στρατηγικές σάρωσης:

Τυχαία σάρωση

- Κάθε εκτεθειμένος υπολογιστής υπηρεσίας σαρώνει τυχαίες διευθύνσεις στον χώρο των διευθύνσεων IP, χρησιμοποιώντας διαφορετικό εκκινητή (seed)
- Αυτό παράγει μεγάλο όγκο κυκλοφορίας δεδομένων στο Διαδίκτυο, κάτι που μπορεί να προκαλέσει γενικευμένη διακοπή παροχής υπηρεσιών ακόμα και πριν από την έναρξη της ίδιας της επίθεσης

«Λίστα θανάτου»

- Ο επιτιθέμενος συντάσσει μια μεγάλη λίστα υποψήφιων ευάλωτων μηχανημάτων
- Μόλις ολοκληρώσει τη σύνταξη της λίστας, αρχίζει να μολύνει τα μηχανήματα
- Σε κάθε μολυσμένο μηχάνημα δίνεται ένα κομμάτι της λίστας για σάρωση
- Το αποτέλεσμα είναι ότι η περιόδος σάρωσης έχει πολύ μικρή διάρκεια, κάτι που ενδέχεται να δυσκολέψει την ανίχνευση της μόλυνσης η οποία λαμβάνει χώρα

Τοπολογική

- Χρησιμοποιεί πληροφορίες που περιέχονται στο μολυσμένο μηχάνημα-θύμα για να βρει περισσότερους υποψήφιους υπολογιστές υπηρεσίας προς σάρωση

Τοπικό υποδίκτυο

- Αν είναι εφικτό να μολυνθεί ένας υπολογιστής υπηρεσίας πίσω από κάποιο τείχος προστασίας, ο συγκεκριμένος υπολογιστής αρχίζει να αναζητεί στόχους στο τοπικό δίκτυο
- Χρησιμοποιεί τη δομή διευθύνσεων υποδικτύου για να εντοπίσει άλλους υπολογιστές υπηρεσίας οι οποίοι, υπό διαφορετικές συνθήκες, θα προστατεύονταν από το τείχος προστασίας



Εικόνα 6.3 Μοντέλο εξάπλωσης σκουληκιών

Το σκουλήκι του Morris

- Η πρώτη σημαντική μόλυνση από σκουλήκι
- Το απελευθέρωση ο Robert Morris το 1988
- Σχεδιασμένο να εξαπλώνεται σε συστήματα UNIX
 - Προσπαθούσε να παραβιάσει το αρχείο με τους τοπικούς κωδικούς πρόσβασης και να χρησιμοποιήσει τα σχετικά στοιχεία για να συνδεθεί σε άλλα συστήματα
 - Εκμεταλλευόταν ένα σφάλμα (bug) στο πρωτόκολλο finger, το οποίο αναφέρει τις κινήσεις ενός απομακρυσμένου χρήστη στο σύστημα
 - Εκμεταλλευόταν μια μυστική πόρτα (trapdoor) στην επιλογή αποσφαλμάτωσης της απομακρυσμένης διεργασίας η οποία λαμβάνει και στέλνει μηνύματα ηλεκτρονικού ταχυδρομείου
- Αν η επίθεση ήταν επιτυχής, το σκουλήκι ερχόταν σε επικοινωνία με τον ερμηνευτή εντολών (command interpreter) του λειτουργικού συστήματος
 - Ήστελνε στον ερμηνευτή ένα μικρό πρόγραμμα εκκίνησης για την αντιγραφή του σκουληκιού



Πρόσφατες επιθέσεις σκουληκιών

Melissa	1998	Σκουλήκι ηλεκτρονικού ταχυδρομείου Το πρώτο που συνδύαζε ιό, σκουλήκι και Δούρειο ίππο σε ένα πακέτο
Code Red	Ιούλιος 2001	Εκμεταλλευόταν ένα κενό ασφαλείας στον Microsoft IIS Σάρωνε τυχαίες διευθύνσεις IP Όταν ήταν ενεργό, κατανάλωνε πολλή από τη χωρητικότητα του Διαδικτύου
Code Red II	Αύγουστος 2001	Είχε επίσης ως στόχο τον Microsoft IIS Εγκαθιστούσε μια κερκόπορτα πρόσβασης
Nimda	Σεπτέμβριος 2001	Διέθετε χαρακτηριστικά σκουληκιού, ιού, και κινητού κώδικα Εξαπλωνόταν μέσω e-mail, κοινόχρηστων στοιχείων των Windows, διακομιστών Ιστού, πελατών Ιστού, κερκοπορτών
SQL Slammer	Αρχές του 2003	Εκμεταλλευόταν μια ευπάθεια υπερχείλισης περιοχής προσωρινής αποθήκης (buffer overflow) στον Microsoft SQL server Είχε συνεπυγμένο μέγεθος και μεγάλη ταχύτητα εξάπλωσης
Sobig.F	Τέλη του 2003	Εκμεταλλευόταν ανοικτούς διακομιστές μεσολάβησης (proxy servers) για να μετατρέψει τους μολυσμένους υπολογιστές σε μηχανές παραγωγής ενοχλητικών μαζικών μηνυμάτων (spam)
Mydoom	2004	Σκουλήκι μαζικής αποστολής e-mail Εγκαθιστούσε κερκόπορτα στους μολυσμένους υπολογιστές
Warezov	2006	Δημιουργούσε εκτελέσιμα αρχεία σε καταλόγους του συστήματος Έστελνε ένα αντίγραφο του ως συνημμένο αρχείο σε μηνύματα e-mail Μπορούσε να αχρηστεύει προγράμματα σχετικά με την ασφάλεια
Conficker (Downadup)	Νοέμβριος 2008	Εκμεταλλευόταν μια ευπάθεια υπερχείλισης περιοχής προσωρινής αποθήκευσης των Windows Πιο εκτεταμένη μόλυνση από την εποχή του SQL Slammer
Stuxnet	2010	Περιόριζε εσκεμμένα τον ρυθμό εξάπλωσής του για να μειώσει τις πιθανότητες ανίχνευσής του Έβαζε στο στόχαστρό του συστήματα βιομηχανικού ελέγχου



Κινητός κώδικας

- Προγράμματα τα οποία μπορούν να μεταφερθούν αμετάβλητα σε διάφορα υπολογιστικά περιβάλλοντα
- Μεταδίδεται από ένα απομακρυσμένο σε ένα τοπικό σύστημα, όπου και εκτελείται
- Συχνά λειτουργεί ως μηχανισμός για τη μετάδοση ιών, σκουληκιών, ή Δούρειων ίππων
- Εκμεταλλεύεται ευπάθειες για να επιτύχει διάφορους δικούς του στόχους
- Στα δημοφιλή οχήματα για τον κινητό κώδικα περιλαμβάνονται οι μικροεφαρμογές Java (Java applets), η τεχνολογία ActiveX, καθώς και οι γλώσσες JavaScript και VBScript

Σκουλήκια κινητών τηλεφόνων

- Πρώτα ανακαλύφθηκε το σκουλήκι Cabir το 2004
- Ακολούθησαν τα σκουλήκια Lasco CommWarrior το 2005
- Επικοινωνούσαν μέσω ασύρματων συνδέσεων Bluetooth ή MMS
- Ο στόχος τους ήταν τα «έξυπνα τηλέφωνα»
- Μπορούν να απενεργοποιούν πλήρως το τηλέφωνο, να διαγράφουν δεδομένα από αυτό, ή να αναγκάσουν τη συσκευή να στέλνει ακριβά μηνύματα
- Το CommWarrior μεταδιδόταν μέσω Bluetooth σε άλλα τηλέφωνα εντός εμβέλειας, έστελνε ένα αντίγραφό ως αρχείο στους αριθμούς που υπήρχαν στο βιβλίο διευθύνσεων του κινητού τηλεφόνου καθώς και σε αυτόματες απαντήσεις εισερχόμενων μηνυμάτων κειμένου

Κρυφές λήψεις

- Όταν ο χρήστης μεταβεί σε μια ιστοσελίδα που ελέγχεται από τον επιτιθέμενο, ο κώδικας της σελίδας εκμεταλλεύεται ευπάθειες των φυλλομετρητών για να κατεβάσει και να εγκαταστήσει κακόβουλο λογισμικό στο σύστημα
- Στις περισσότερες περιπτώσεις, αυτό το κακόβουλο λογισμικό δεν εξαπλώνεται ενεργά
- Εξαπλώνεται όταν οι χρήστες επισκέπτονται την κακόβουλη ιστοσελίδα



«Πειρατεία» των κλικ

- Γνωστή και ως επίθεση αποκατάστασης διασύνδεσης με τον χρήστη (user-interface (UI) redress attack)
- Με χρήση μιας παρόμοιας τεχνικής, είναι εφικτή και η «πειρατεία» των πληκτρολογήσεων
 - Ο χρήστης μπορεί να νομίσει ότι πληκτρολογεί τον κωδικό πρόσβασης του λογαριασμού ηλεκτρονικού ταχυδρομείου ή του τραπεζικού λογαριασμού του, ενώ στην πραγματικότητα πληκτρολογεί μέσα σε ένα αόρατο πλαίσιο το οποίο ελέγχεται από τον επιτιθέμενο
- Ευπάθεια που χρησιμοποιεί ο επιτιθέμενος για να συλλέξει τα κλικ ενός μολυσμένου χρήστη
 - Ο επιτιθέμενος μπορεί να αναγκάσει τον χρήστη να κάνει διάφορα πράγματα, από το να προσαρμόσει τις ρυθμίσεις του υπολογιστή του έως να μεταβεί ανυποψίαστος σε ιστότοπους που μπορεί να περιέχουν κακόβουλο κώδικα
 - Αξιοποιώντας τη γλώσσα JavaScript ή το λογισμικό Adobe Flash, θα μπορούσε ακόμα και να τοποθετήσει ένα δικό του κουμπί κάτω ή πάνω από ένα έγκυρο κουμπί, κάτι που δεν είναι εύκολο να εντοπίσουν οι χρήστες
 - Μια τυπική επίθεση χρησιμοποιεί πολλά διαφανή ή αδιαφανή επίπεδα ώστε να πείσει τον χρήστη να πατήσει σε ένα κουμπί ή σύνδεσμο που βρίσκεται σε μια διαφορετική σελίδα, ενώ ο χρήστης θα ήθελε στην πραγματικότητα να πατήσει σε ένα σημείο της σελίδας που βρίσκεται στο ανώτερο επίπεδο
 - Ο επιτιθέμενος προχωρά στην «πειρατεία» των κλικ που προορίζονται για μία σελίδα και τα δρομολογεί σε άλλη σελίδα

Κοινωνική μηχανική

- Οι χρήστες ξεγελιούνται και βοηθούν ακούσια στην παραβίαση των συστημάτων τους

Ενοχλητικά μαζικά email

Μαζικά ενοχλητικά μηνύματα ηλεκτρονικού ταχυδρομείου (spam)

Σημαντικός φορέας κακόβουλου λογισμικού

Χρησιμοποιούνται για επιθέσεις ηλεκτρονικού ψαρέματος

Δούρειοι ίπποι

Πρόγραμμα ή βοηθητική εφαρμογή που περιέχει κρυμμένο επιβλαβή κώδικα

Χρησιμοποιούνται για την εκτέλεση ενεργειών τις οποίες ο επιτιθέμενος δεν θα μπορούσε να εκτελέσει απευθείας

Δούρειοι ίπποι κινητών τηλεφώνων

Πρωτοεμφανίστηκαν το 2004 (Skuller)

Ο στόχος τους είναι τα «έξυπνα τηλέφωνα»

Φορτίο – Αλλοίωση συστήματος

Ιός Chernobyl

- Εμφανίστηκε το 1998
- Ιός των Windows 95 και 98
- Μόλυνε εκτελέσιμα αρχεία, ενώ η έλευση της ημερομηνίας ενεργοποίησης αλλοίωνε ολόκληρο το σύστημα αρχείων



Klez

- Σκουλήκι μαζικής αποστολής εμπορίου μόλυνε συστήματα με Windows 95 έως XP
- Με την έλευση της ημερομηνίας ενεργοποίησης, άδειαζε τα περιεχόμενα των αρχείων του τοπικού σκληρού δίσκου



Λογισμικό λύτρων

- Κρυπτογραφεί τα δεδομένα και εκβιάζει τους χρήστες, οι οποίοι πρέπει να πληρώσουν ένα χρηματικό ποσό για να λάβουν το κλειδί που θα τους επιτρέψει να τα ανακτήσουν
- Δούρειος ίππος PC Cyborg (1989)
- Δούρειος ίππος Gpcode Trojan (2006)



Φορτίο – Αλλοίωση συστήματος

- Πραγματική ζημιά
 - Προκαλείται ζημιά στον φυσικό εξοπλισμό
 - Ο ιός Chernobyl ξαναέγραφε τον κώδικα του BIOS
 - Σκουλήκι Stuxnet
 - Έβαζε στο στόχαστρό του συγκεκριμένο λογισμικό συστημάτων βιομηχανικού ελέγχου
 - Αυτό έχει εγείρει ανησυχίες σχετικά με τη χρήση πολύπλοκου κακόβουλου λογισμικού για στοχευμένη βιομηχανική δολιοφθορά
- Λογική βόμβα
 - Ενσωματωμένος κώδικας στο κακόβουλο λογισμικό, ο οποίος έχει οριστεί να «εκραγεί» μόλις ικανοποιηθούν καθορισμένες συνθήκες

Φορτίο – Πράκτορες επίθεσης – Ρομπότ

- Παίρνει κρυφά τον έλεγχο ενός άλλου υπολογιστή συνδεδεμένου στο Διαδίκτυο και μετά τον χρησιμοποιεί για να εξαπολύσει ή να διαχειριστεί επιθέσεις
- Δίκτυο ρομπότ – ομάδα ρομπότ η οποία είναι σε θέση να λειτουργεί με συντονισμένο τρόπο
- Χρήσεις:
 - Επιθέσεις κατανεμημένης άρνησης εξυπηρέτησης (DDoS)
 - Αποστολή ενοχλητικών μαζικών μηνυμάτων
 - Ανίχνευση κυκλοφορίας δεδομένων
 - Καταγραφή πληκτρολογήσεων
 - Εξάπλωση νέου κακόβουλου λογισμικού
 - Εγκατάσταση πρόσθετων (add-ons) και βιοηθητικών αντικειμένων φυλλομετρητή (browser helper objects, BHO) για διαφήμιση
 - Επιθέσεις σε δίκτυα συνομιλιών IRC
 - Παραποίηση διαδικτυακών δημοσκοπήσεων/παιχνιδιών



Δυνατότητα απομακρυσμένου ελέγχου

- Ξεχωρίζει τα ρομπότ από τα σκουλήκια
 - Το σκουλήκι εξαπλώνεται και ενεργοποιείται μόνο του
 - Το ρομπότ ελέγχεται αρχικά από κάποιο κεντρικό σύστημα
- Ένας τυπικός τρόπος υλοποίησης της δυνατότητας απομακρυσμένου ελέγχου βασίζεται σε διακομιστή IRC
 - Τα ρομπότ προσχωρούν σε συγκεκριμένο κανάλι αυτού του διακομιστή και εκλαμβαναν τα εισερχόμενα μηνύματα ως εντολές
 - Τα νεότερα δίκτυα ρομπότ χρησιμοποιούν συγκεκαλυμμένα κανάλια επικοινωνίας μέσω πρωτοκόλλων όπως το HTTP
 - Κατανεμημένοι μηχανισμοί ελέγχου χρησιμοποιούν πρωτόκολλα ομότιμης (peer-to-peer) επικοινωνίας ώστε να αποφεύγουν τη δημιουργία ενός μοναδικού σημείου αστοχίας

Φορτίο – Κλοπή πληροφοριών – Καταγραφή πληκτρολογήσεων, κατασκοπευτικό λογισμικό

Πρόγραμμα καταγραφής πληκτρολογήσεων

- Υποκλέπτει οτιδήποτε πληκτρολογείται και επιτρέπει έτσι στον επιτιθέμενο να παρακολουθεί ευαίσθητες πληροφορίες
- Συνήθως εφαρμόζει κάποια μορφή μηχανισμού φιλτραρίσματος ο οποίος επιστρέφει μόνο πληροφορίες που μοιάζουν με ζητούμενες λέξεις-κλειδιά

Κατασκοπευτικό λογισμικό

- Πείθει το εκτεθειμένο μηχάνημα να επιτρέψει την παρακολούθηση μιας μεγάλης γκάμας δραστηριοτήτων που λαμβάνουν χώρα στο σύστημα
- Παρακολούθηση ιστορικού και περιεχομένου της περιήγησης στο Διαδίκτυο
- Ανακατεύθυνση ορισμένων αιτήσεων ιστοσελίδων σε πλαστούς ιστότοπους
- Δυναμική τροποποίηση δεδομένων που ανταλλάσσονται μεταξύ του φυλλομετρητή και ορισμένων ιστότοπων

Φορτίο – Ηλεκτρονικό ψάρεμα και κλοπή ταυτότητας



- Αξιοποιεί την κοινωνική μηχανική (social engineering)· προσπαθεί να κερδίσει την εμπιστοσύνη του χρήστη μέσω «μεταμφιεσμένων» μηνυμάτων που παραπέμπουν σε εμπιστη πηγή
 - Συμπεριλαμβάνει σε ένα ενοχλητικό μαζικό email ένα URL που κατευθύνει τους χρήστες σε έναν πλαστό ιστότοπο, ο οποίος έχει παραπλήσια εμφάνιση με τη σελίδα σύνδεσης κάποιου ιστότοπου εκτέλεσης τραπεζικών συναλλαγών, παιχνιδιών, κ.λπ.
 - Ζητά από τον χρήστη να προβεί σε κάποια επείγουσα ενέργεια για να πιστοποιήσει τη γνησιότητα του λογαριασμού του
 - Ο επιτιθέμενος χρησιμοποιεί τον λογαριασμό αξιοποιώντας τα διαπιστευτήρια που υπέκλεψε
- Ηλεκτρονικό «καμάκωμα»
 - Ο επιτιθέμενος έχει ερευνήσει διεξοδικά τους υποψήφιους παραλήπτες
 - Κάθε μήνυμα είναι προσεκτικά φτιαγμένο ώστε να ταιριάζει με το προφίλ του παραλήπτη· συχνά περιέχει διάφορες πληροφορίες σε μια προσπάθεια να τον πείσει για τη γνησιότητά του

Φορτίο – Αόρατες απειλές – Κερκόπορτες

- Γνωστή και ως μυστική πόρτα (trapdoor)
- Μυστικό σημείο εισόδου σε ένα πρόγραμμα το οποίο επιτρέπει στον επιτιθέμενο να αποκτήσει πρόσβαση παρακάμπτοντας τις διαδικασίες ασφαλούς πρόσβασης
- Το άγκιστρο συντήρησης είναι μια κερκόπορτα την οποία χρησιμοποιούν οι προγραμματιστές για αποσφαλμάτωση και δοκιμή προγραμμάτων
- Είναι δύσκολο να υλοποιηθούν μηχανισμοί ελέγχου του λειτουργικού συστήματος για κερκόπορτες σε εφαρμογές



Φορτίο – Αόρατες απειλές – Κιτ υπερχρήστη

- Σύνολο προγραμμάτων τα οποία εγκαθίστανται σε ένα σύστημα με στόχο να παρέχουν αδιάλειπτη, συγκεκαλυμμένη πρόσβαση σε αυτό
- Κρύβεται, υπονομεύοντας τους μηχανισμούς ενός υπολογιστή οι οποίοι παρακολουθούν και δίνουν αναφορές για τις διεργασίες, τα αρχεία και τις καταχωρίσεις μητρώου
- Παρέχει στον επιτιθέμενο δικαιώματα διαχειριστή (administrator), ή υπερχρήστη (root)
 - Μπορεί να προσθέτει ή να τροποποιεί προγράμματα και αρχεία, να παρακολουθεί διεργασίες, να στέλνει και να λαμβάνει δεδομένα μέσω δικτύου, καθώς και να αποκτά πρόσβαση κατ' απαίτηση μέσω κάποιας κερκόπορτας

Χαρακτηριστικά ταξινόμησης

κιτ υπερχρήστη

Επίμονα

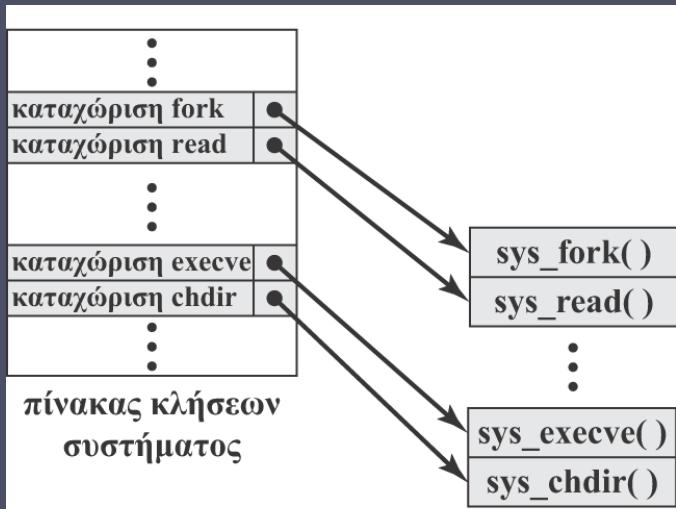
Βασισμένα
στη μνήμη

Κατάσταση
χρήστη

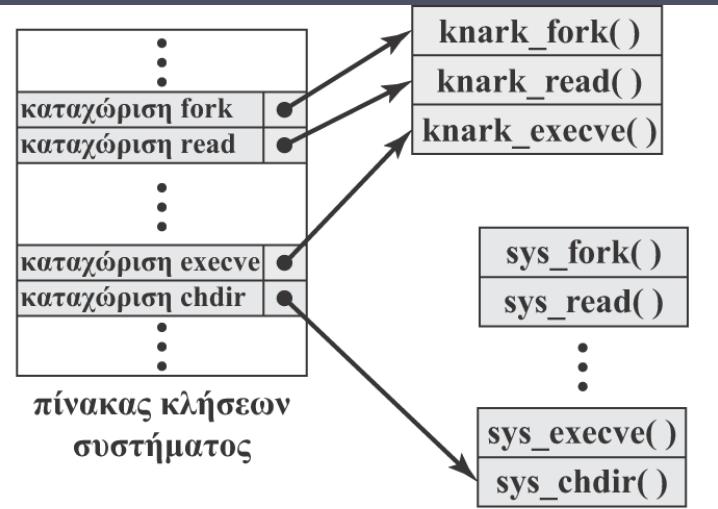
Κατάσταση
πυρήνα

Βασισμένα
σε εικονικό
μηχάνημα

Κατάσταση
εξωτερικής
λειτουργίας



(α) Φυσιολογική διάταξη μνήμης πυρήνα



(β) Διάταξη μετά από την εγκατάσταση του knark

Εικόνα 6.4 Τροποποίηση του πίνακα κλήσεων συστήματος από κιτ υπερχρήστη

Αντίμετρα για κακόβουλο λογισμικό

- Η ιδανική λύση για την απειλή του κακόβουλου λογισμικού είναι η αποτροπή

Τέσσερα κύρια στοιχεία αποτροπής:

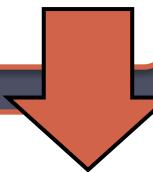
- Πολιτική
- Ενημέρωση
- Άμβλυνση ευπαθειών
- Μετριασμός απειλών

- Αν η αποτροπή δεν λειτουργήσει, μπορούν να χρησιμοποιηθούν τεχνικοί μηχανισμοί για να υποστηριχθούν οι παρακάτω επιλογές μετριασμού των απειλών:
 - Ανίχνευση
 - Ταυτοποίηση
 - Αφαίρεση

Γενιές λογισμικού προστασίας από ιούς

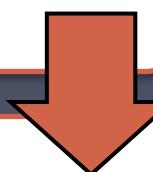
1η γενιά: απλές εφαρμογές ανίχνευσης

- Απαιτούν να έχει το κακόβουλο λογισμικό υπογραφή (signature) προκειμένου να το ταυτοποιήσουν
- Ανιχνεύουν μόνο γνωστό κακόβουλο λογισμικό



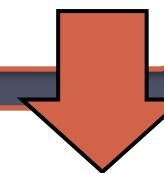
2η γενιά: ευρετικές εφαρμογές ανίχνευσης

- Χρησιμοποιούν ευρετικούς κανόνες για την αναζήτηση πιθανών εμφανίσεων κακόβουλου λογισμικού
- Μια άλλη τεχνική είναι ο έλεγχος ακεραιότητας



3η γενιά: παγίδες δραστηριότητας

- Παραμένουν στη μνήμη και ταυτοποιούν το κακόβουλο λογισμικό σε ένα μολυσμένο πρόγραμμα μελετώντας τις ενέργειές του και όχι τη δομή του



4η γενιά: πλήρης προστασία

- Πακέτα που χρησιμοποιούν συνδυαστικά διάφορες τεχνικές προστασίας από ιούς
- Ανίχνευση και παγίδα δραστηριοτήτων, καθώς και δυνατότητες ελέγχου πρόσβασης

Γενική αποκρυπτογράφηση (GD)

- Επιτρέπει στο πρόγραμμα προστασίας από ιούς να ανιχνεύει εύκολα ακόμα και τους πιο σύνθετους πολυμορφικούς ιούς και άλλο κακόβουλο λογισμικό, χωρίς να επηρεάζεται ιδιαίτερα η ταχύτητα σάρωσης
- Τα εκτελέσιμα αρχεία σαρώνονται από μια εφαρμογή GD, η οποία περιέχει τα εξής στοιχεία:
 - Εξομοιωτή CPU
 - Υπομονάδα ανιχνευσης υπογραφής ιών
 - Υπομονάδα ελέγχου εξομοίωσης
- Το πιο δύσκολο σχεδιαστικό ζήτημα των εφαρμογών GD είναι ο προσδιορισμός του χρονικού διαστήματος που πρέπει να διαρκεί η κάθε ερμηνεία

Λογισμικό παρεμπόδισης συμπεριφοράς βασισμένο σε υπολογιστή υπηρεσίας

- Ενσωματώνεται στο λειτουργικό σύστημα ενός υπολογιστή υπηρεσίας και παρακολουθεί τη συμπεριφορά των προγραμμάτων σε πραγματικό χρόνο για τυχόν κακόβουλες ενέργειες
 - Παρεμποδίζει τις δυνητικά κακόβουλες ενέργειες πριν καν αυτές έχουν την ευκαιρία να επηρεάσουν το σύστημα
 - Μπλοκάρει ύποπτο λογισμικό σε πραγματικό χρόνο, άρα έχει πλεονέκτημα έναντι τεχνικών ανίχνευσης ιών όπως η «δακτυλοσκόπηση» και οι ευρετικές τεχνικές

Περιορισμοί

- Επειδή ο κακόβουλος κώδικας πρέπει να εκτελεστεί στο μηχάνημα-στόχο πριν προλάβουν να ταυτοποιηθούν όλες οι συμπεριφορές του, είναι σε θέση να προκαλέσει ζημιές πριν ανιχνευθεί και παρεμποδιστεί

Τεχνικές περιμετρικής σάρωσης

- Λογισμικό προστασίας από ιούς το οποίο εμπεριέχεται συνήθως σε υπηρεσίες email και μεσολάβησης Ιστού στο τείχος προστασίας και το σύστημα IDS ενός οργανισμού
- Μπορεί επίσης να εμπεριέχεται στην υπομονάδα ανάλυσης κυκλοφορίας ενός IDS
- Ενδέχεται να περιλαμβάνει μέτρα αποτροπής εισβολών, μπλοκάροντας τη ροή τυχόν ύποπτης κυκλοφορίας δεδομένων
- Περιορίζεται στη σάρωση του περιεχομένου του κακόβουλου λογισμικού

Ελεγκτές εισόδου

Θέση: όρια μεταξύ εταιρικού δικτύου και Διαδικτύου

Ελεγκτές εξόδου

Θέση: σημείο εξόδου επιμέρους LAN του εταιρικού δικτύου, όρια μεταξύ εταιρικού δικτύου και Διαδικτύου

Μια τεχνική είναι η αναζήτηση κυκλοφορίας προς αχρησιμοποίητες διευθύνσεις IP

Παρακολουθεί την εξερχόμενη κυκλοφορία δεδομένων για σημάδια σάρωσης ή άλλης ύποπτης συμπεριφοράς

Δύο τύποι λογισμικού παρακολούθησης

Σύνοψη

- Τύποι κακόβουλου λογισμικού (malware)
- Προηγμένη επίμονη απειλή
- Εξάπλωση
 - Μολυσμένο περιεχόμενο
 - Ioi
 - Εκμετάλλευση ευπαθειών
 - Σκουλήκια
 - Κοινωνική μηχανική
 - Ενοχλητικά μαζικά e-mail
 - Δούρειοι ίπποι



- Φορτίο
 - Αλλοίωση συστήματος
 - Πράκτορας επίθεσης
 - Ζόμπι
 - Ρομπότ
 - Κλοπή πληροφοριών
 - Προγράμματα καταγραφής πληκτρολογήσεων
 - Ηλεκτρονικό ψάρεμα
 - Κατασκοπευτικό λογισμικό
 - Συγκάλυψη
- Αντίμετρα