Το Πρόβλημα των Επιθέσεων DoS/DDoS (Denial of Service Attacks)

Γεώργιος Κουτέπας, Γεώργιος Αδαμόπουλος
Τράπεζα Πληροφοριών του ΤΕΕ

Ημερίδα: Ηλεκτρονικές Επικοινωνίες – Πόσο Ασφαλείς είναι;
Τεχνικό Επιμελητήριο Ελλάδας – Δικηγορικός Σύλλογος Αθηνών
1η Ιουνίου 2006

Τί είναι "*Denial of Service*";

- Επιθέσεις που έχουν σκοπό να αποτρέψουν τη χρήση ενός συστήματος από όλους (δηλαδή τους νόμιμους χρήστες του)
- Δεν γίνονται προσπάθειες παραβίασης ή κλοπής στοιχείων
  - Είναι όμως δυνατός ο συνδυασμός τους με άλλες επιθέσεις που γίνονται παράλληλα με σκοπό να "παραπλάνήσουν" τα συστήματα ανίνχνευσης (Intrusion Detection Systems) και τους διαχειριστές από την πραγματική απειλή.
- Δεν υπάρχει η "Εύκολη Λύση". Οι επιθέσεις DoS/DDoS είναι ακόμα σε μεγάλο βαθμό πεδιό έρευνας

Κύρια Χαρακτηριστικά των επιθέσεων DoS

- Δυνητικός στόχος, οποιοδήποτε σύστημα στο Διαδίκτυο
  - Απλά υπολογιστικά συστήματα (hosts) ή ολόκληρα δίκτυα (domains)
  - Ιδιαίτερα Σημαντικό: Τα ενεργά στοιχεία δικτύου (π.χ. routers) είναι επίσης ευάλωτα και αποτελούν πιθανούς στόχους!
- Διάφορες χρήσεις και αποτελέσματα:
  - "Πόλεμοι" – παιχνίδια hackers
  - Επιθέσεις σε σημαντικούς επιχειρηματικούς ή πολιτικούς στόχους
    - Μπορεί να αποτελέσουν και εργαλείο των ανταγωνιστών σας...
  - Κυβερνοπόλεμος (ακύρυχτος), τρομοκρατία κ.λπ...

Σύντομη Ιστορία

Πρώτη Φάση (δεκαετία του '90): DoS – Επιθέσεις Άρνησης Υπηρεσίας

- Αρχικά εκμετάλευση προβλημάτων (bugs) ή αδυναμιών λογισμικού
- Πρώτοι στόχοι: Single hosts - single services
- Σε κάποιες περιπτώσεις αρκεί ένα μοναδικό, κατάλληλα κατασκευασμένο, πακέτο

Δεύτερη Φάση (1996-2000)

- Κλήσεις εξυπηρέτησης από πολλές πηγές για κατανάλωση πόρων
- Οι υποδομές του Internet χρησιμοποιούνται για "ενίσχυση" της έντασης των επιθέσεων

Τρίτη Φάση (μετά το 2000): Distributed DoS – Κατανεμημένες Επιθέσεις Άρνησης Υπηρεσίας

- Στόχο αποτελεί το δικτυακό εύρος (Bandwidth)
- Χρήση πολλαπλών ελεγχόμενων υπολογιστών, σε πολλαπλά στάδια επίθεσης με κλιμάκωση της επίθεσης

Εξάπλωση

- Μεγάλα περιστατικά στις αρχές του 2000
  - Θύματα μεγάλες εταιρείες που ενεργοποιούνται στο Διαδίκτυο (CNN, Amazon, Yahoo, eBay κ.λπ.), Ενδιαφέρον του κοινού
  - Αντιμετώπιση ως "έκτακτη κατάσταση" εναντίον μιας "κρίσιμης υποδομής" (Internet)
- Ιανουάριος 2002: ο ISP Cloud Nine αναγκάζεται να διακόψει την επιχειρηματική του δραστηριότητα
- Οκτώβριος 2002: Προσπάθεια προσβολής των Root Name Servers
- Computer Security Institute: Κόστος DoS/DDoS 26 εκ. δολ. το 2004
- Παρατηρήσεις Moore et al. (2001)
  - 12.000 περιστατικά σε 3 εβδομάδες
  - Σε περιστατικά εμφανίστηκαν 500.000 πακέτα/δευτ.
- Παρατηρήσεις Hussain et al. (2003)
  - Τουλάχιστον 10.000 περιστατικά ανά μήνα

Επιθέσεις DoS εναντίον Hosts

- Συνήθως ένας επιτιθέμενος, ένας στόχος
- Μέθοδολογίες σχετικές με αυτές που χρησιμοποιούνται για παράνομη πρόσβαση:
  - "*Buffer Overflows" σε (άσχημα σχεδιασμένα) σημεία εισόδου στοιχείων είναι δυνατόν να οδηγήσουν σε εγγραφές τμημάτων της μήμης του συστήματος. Αποτελέσματα*: Άνοιγμα "διόδων πρόσβασης" ή πλήρης αστοχία του συστήματος
  - "Αοριστίες" σε ορισμένες προδιαγραφές δικτυακών πρωτοκόλλων μπορούν να οδηγήσουν σε προβλήματα στις υλοποιήσεις τους. Ειδικά σχεδιασμένα κακόβουλα πακέτα που στοχεύουν σε αυτές τις αδυναμίες μπορούν να οδηγήσουν σε σημαντικά προβλήματα

Παραδείγματα

- *Land IP DoS attack*: Ειδικά πακέτα TCP/SYN με ίδια τη διεύθυνση προέλευσης και προορισμού

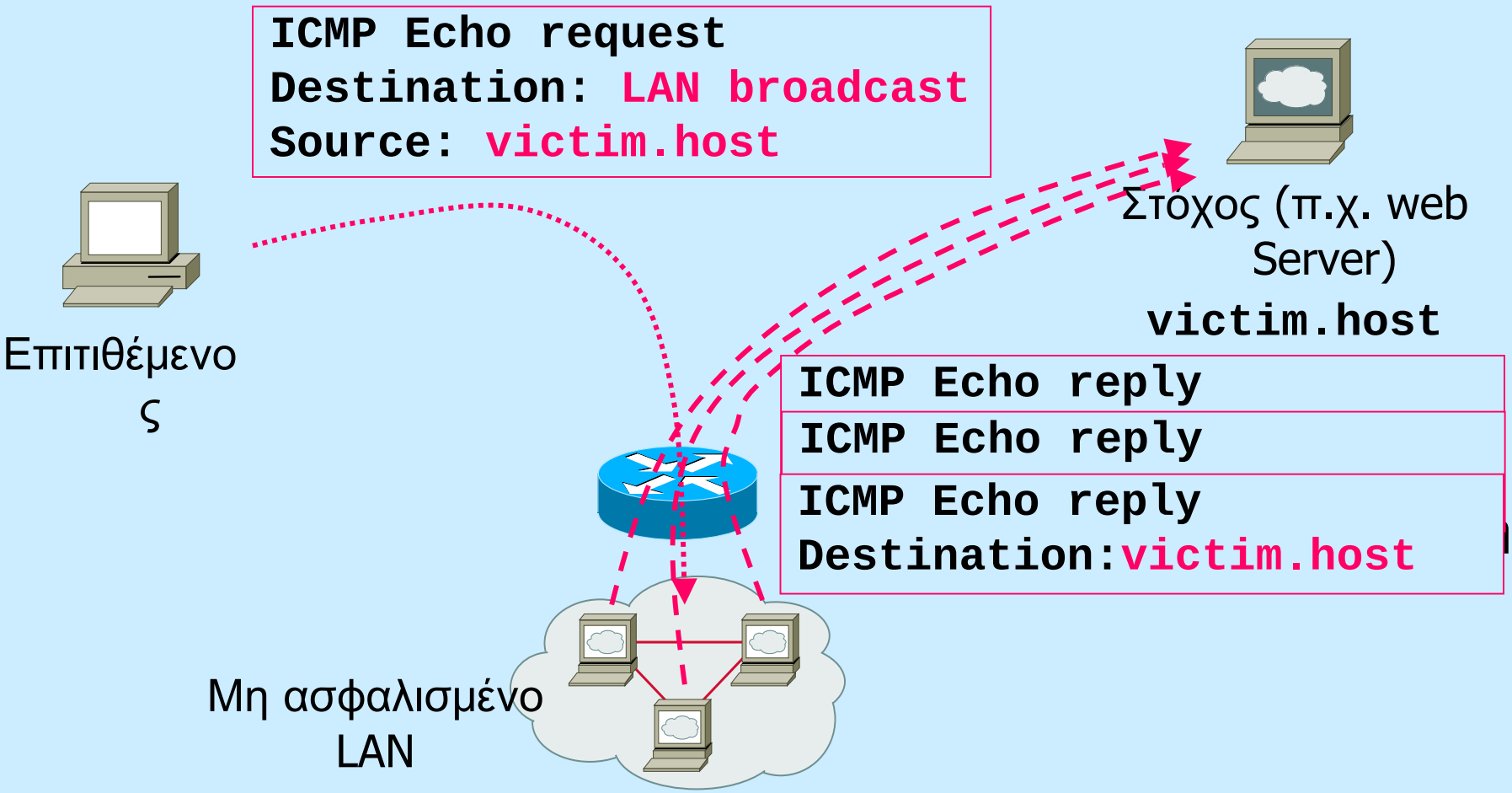
- *Teardrop attack*: Αποστολή "κατακερματισμένων" (fragmented) πακέτων IP σε συστήματα συνδεδεμένα στο δίκτυο. Εκμεταλεύεται πρόβλημα χειρισμού τέτοιων πακέτων που υπάρχει σε διάφορες υλοποιήσεις TCP/IP

Επιθέσεις DoS Εναντίον Υπολογιστικών Πόρων

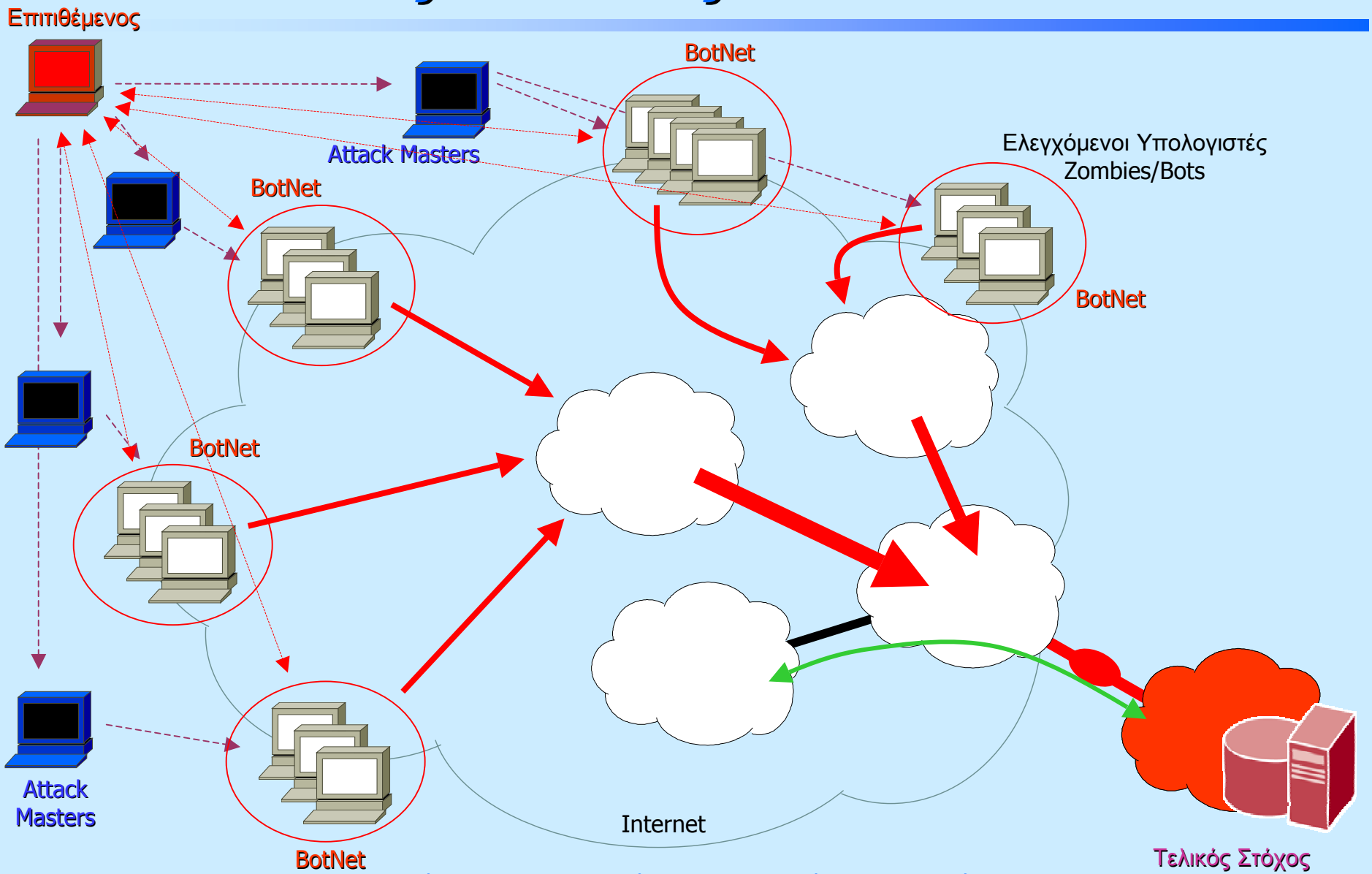
- Εξάντληση υπολογιστικών πόρων με τη συνεχή αποστολή μεγάλου αριθμού "νομιμων" αιτημάτων εξυπηρέτησης
- Ο στόχος (συνήθως) συνεχίζει τη λειτουργία του αλλά δε μπορεί να προσφέρει οποιαδήποτε χρήσιμη υπηρεσία

  - *SYN Flooding attack*
  - *Ping Flooding attack*
  - *Smurf attack*: ροή πακέτων ping η οποία "ενισχύεται" με την αποστολή της πρώτα σε ένα αριθμό από διευθύνσεις network broadcast με διεύθυνση επιστροφής των πακέτων, αυτή του θύματος

Παράδειγμα Επίθεσης "*Smurf*"



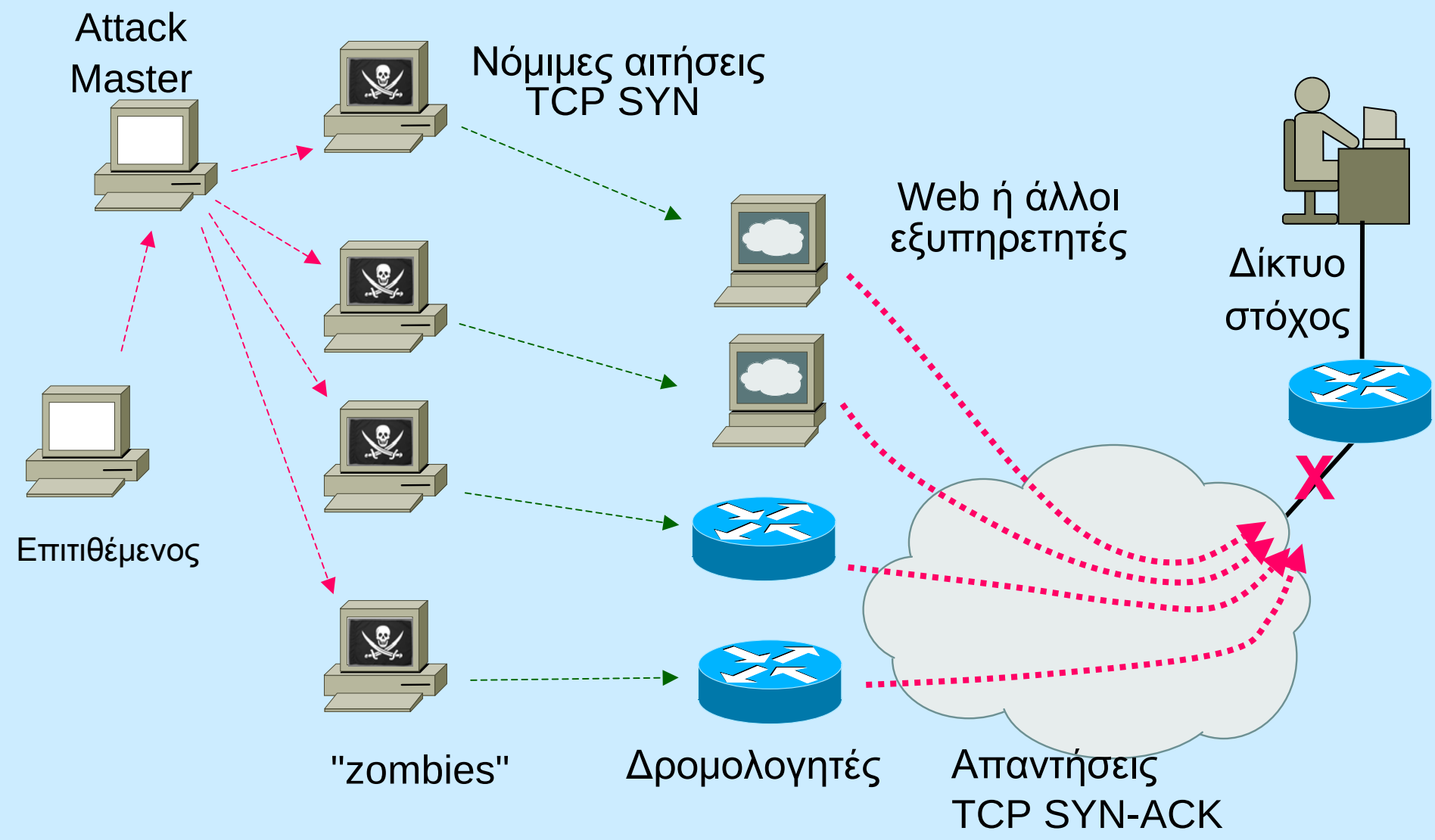
Δικτυακές Επιθέσεις: Distributed DoS



Κύρια χαρακτηριστικά των επιθέσεων DDoS

- Μερικές εκατοντάδες συνεχείς ροές κίνησης (flows) αρκούν για να επιρρεάσουν σημαντικά ακόμα και ένα μεγάλο δίκτυο
- Η εισερχόμενη κίνηση μπορεί να ελεγχθεί μόνον πριν από το δίκτυο του τελικού στόχου, στους παρόχους δικτυακής διασύνδεσης (upstream providers)
- Συνήθως οι διευθύνσεις προέλευσης στα πακέτα επίθεσης είναι παραποιημένες (spoofing)
- Σημαντικό: τα συστήματα που λαμβάνουν μέρος στην επίθεση μπορεί να ελέγχονται χωρίς γνώση των χρηστών τους
- Πολλά εργαλεία διαθέσιμα για τέτοιου είδους "χτίσιμο" επιθετικών δικτύων: *rootkits*

Επιθέσεις DDoS τύπου "Ανάκλασης"



Μέρος ΙΙ
Τί μπορούμε να κάνουμε

Ανίχνευση

- Επιθέσεις DoS εναντίον απλών συστημάτων:
  - Επικαιροποιημένες άμυνες στα σημεία διασύνδεσης
  - Host και Network based Intrusion Detection Systems
    - Τα συστήματα IDS είναι πολύ καλά στην ανίχνευση τέτοιου είδους επιθέσεων (signature based detection)
  - Διερεύνηση κάθε ένδειξης "ύποπτης" δραστηριότητας
    - Μπορεί να υποδεικνύει τη συλογή κρίσιμων πληροφοριών για σχεδιασμό της επίθεσης

Ανίχνευση (2)

- Κατανεμημένες επιθέσεις DoS – στο δίκτυο
  - Δικτυακές ροές (flows) επίθεσης πρέπει να αναγνωρίζονται το συντομότερο δυνατόν
    - Συμβουλή: γενικά φίλτρα που επιτρέπουν τη διέλευση κίνησης στους δρομολογητές συνόρου (border routers) για να δύμε τι μπορούμε να ανιχνεύσουμε (μεγάλος αριθμός ενός μόνον συγκεκριμένου είδους κίνησης: πιθανή επίθεση)
    - Χρησιμοποιείστε το Netflow ή άλλα εργαλεία παρακολούθησης της κίνησης σας
  - Παρακολούθηση ενδείξεων στους δρομολογητές
    - Συμβουκή: Παρακολουθηστε το φόρτο δρομολογητών για ασυνήθιστα σημάδια
- Κατανεμημένες επιθέσεις DoS – πρόληψη κατάχρησης του δικτύου μας
  - Συχνά security audits για κρυμμένο κακόβουλο κώδικα ("zombies") ή rootkits
  - Anti-virus package

Αντίδραση στις επιθέσεις DDoS

- Οι κακόβουλες ροές πρέπει να επισημαίνονται. Η έγκαιρη αντίδραση είναι κρίσιμη για την αντιμετώπιση της επίθεσης!
- Τα χαρακτηριστικά της επίθεσης πρέπει να μεταδοθούν σε δίκτυα στα προηγούμενα βήματα της (upstream). Συνήθως γίνεται με τηλεφωνήματα, email κ.λπ. και παίρνει πολύ χρόνο...
- Φίλτρα που θα μπολοκάρουν την κακόβουλη κίνηση. Τα φίλτρα αυτά πρέπει να διατηρούνται σύμφωνα με τα χαρακτηριστικά της επίθεσης, για όσο διάστημα αυτή συνεχίζεται και να επιβεβαιώνεται η αποτελεσματικότητα τους
- Υπάρχει κατανάλωση εύρους (bandwidth) σε όλα τα δίκτυα που διατρέχει η επίθεση – απαιτούνται ενέργειες στο μεγαλύτερο δυνατό αριθμό στο μονοπάτι

Αντίδραση στις επιθέσεις DdoS (συνεχ.)

- Άλλη λύση (βοηθά τον ISP): σταμάτημα όλης της κίνησης προς το στόχο. Δρομολόγηση στο null. Πιο αποδοτική για τους πόρους των δρομολογητών αλλά ολοκληρώνει τους στόχους της επίθεσης!
  - Balackhole routing
- Προσπάθειες αναγνώρισης της διαδρομής της επίθεσης (Trace-back):
  - Χρησιμοποιούντας την πληροφορία δρομολόγησης (αν οι πραγματικές πηγές δεν έχουν παραποιηθεί - spoofed)
  - Βήμα – βήμα διαμέσου των ISPs...
    - Δύσκολο αν δεν υπάρχει άμεσο κόστος σε bandwidth
- Κύριο Συμπέρασμα: η αντίμετώπιση δεν είναι υπόθεση μόνον ενός δικτύου

Πρόληψη - Προετοιμασία

- Καλές διαχειριστικές πρακτικές: Αναγκαίες!
  - Patch patch patch!
  - Προετοιμάστε ένα σχέδιο αντιμετώπισης & επαναφοράς, ίσως κάποιο σύστημα σε εφεδρεία
  - Backup backup backup!
  - Προετοιμάστε και εκπαιδεύστε το προσωπικό σας, φροντίστε να υπάρχει πάντα κάποιος που καταλαβαίνει ζητήματα ασφαλείας
- Δημιουργήστε σημεία αναφοράς με τον ISP σας και ομάδες CERT που μπορούν να βοηθήσουν. Φροντίστε να γνωρίζετε εξ' αρχής ποιους να καλέσετε. Συμφωνήστε σε συγκεκριμένες πολιτικές υποστήριξης ώστε να είναι ξεκάθαρες οι υποχρεώσεις του ISP.

Πρόληψη - Προετοιμασία

- Φροντίστε για τον υπόλοιπο κόσμο και προφυλαχθείτε από καταχρήσεις του δικτύου σας
  - Απαγορεύεται να εξέρχονται από το δίκτυο μας πακέτα που δεν έχουν το σωστή διεύθυνση αποστολέα (spoofed traffic)
  - Φιλτράρισμα πακέτων προς διευθύνσεις broadcast (για αποφυγή επιθέσεων ενίσχυσης)
  - Παρακολούθηση κύριων (δημόσια γνωστών) συστημάτων για πρόληψη χρήσης τους σε επιθέσεις "ανάκλασης"

Ερωτήσεις;