Denial of Service (DoS)

Advanced Internet Architectures

Telematics Engineering Master

Iván Vidal Fernández

2010-2011

Departamento de INGENIERIA TELEMATICA
www.it.uc3m.es

Contact data

Iván Vidal Fernández

Email: *ividal@it.uc3m.es*

Office: 4.0F02

INTRODUCTION

Denial of Service (DoS)

Definitions

- **Denial-of-Service (DoS) attack [RFC 4732]:**
  - One or more machines target a victim and attempt to prevent the victim from doing useful work
  - Victims can be:
    - ✓ Servers, clients, routers, network links, Internet users, ISPs, etc.
  - Almost all Internet services are vulnerable to DoS attacks of sufficient scale

- **Distributed DoS (DDoS) attack:**
  - The DoS attack is perpetrated by a large number of compromised hosts or routers

Example of DDoS attack: flooding against a web site

February 2000, DoS attack targeted to Amazon.com, ebay, Buy.com and CNN interactive

"*We were seriously affected. We were serving content, but it was very inconsistent and very little*"

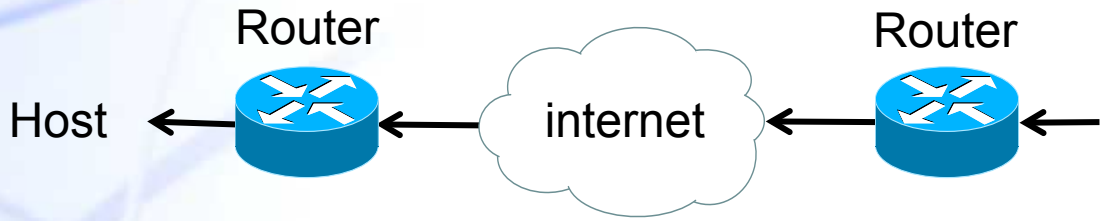
"*By 8:45 p.m., our upstream providers had put blocks in place that are shielding us, and we are now serving content*"

Overview of DoS attacks

- **DoS attacks on end-systems:**
  - **Exploiting poor software quality**
    - ✓ Examples: buffer overflow attacks, sending overlapping IP fragments, etc.
    - ✓ Once identified, the problem can be solved by patching the relevant code
  - **Application resource exhaustion**
    - ✓ Memory, CPU cycles, disk space, maximum number of processes/ threads, maximum number of simultaneous connections, etc.
  - **Triggered lockouts and quota exhaustion**
    - ✓ Examples: blocking a known user with a password-guessing attack, exhausting the traffic quota of small web servers, etc.
  - **Operating system resource exhaustion**
    - ✓ More troublesome than application resource exhaustion
    - ✓ Ex: TCP SYN flood attack

Overview of DoS attacks

- **Example: TCP SYN flood attack**



① Sends a flood of TCP SYN packets to the victim, but does not complete the connection setup

TCP/SYN

Send SYN/ACK

TCP/SYN

Send SYN/ACK

TCP/SYN

Send SYN/ACK

⋮

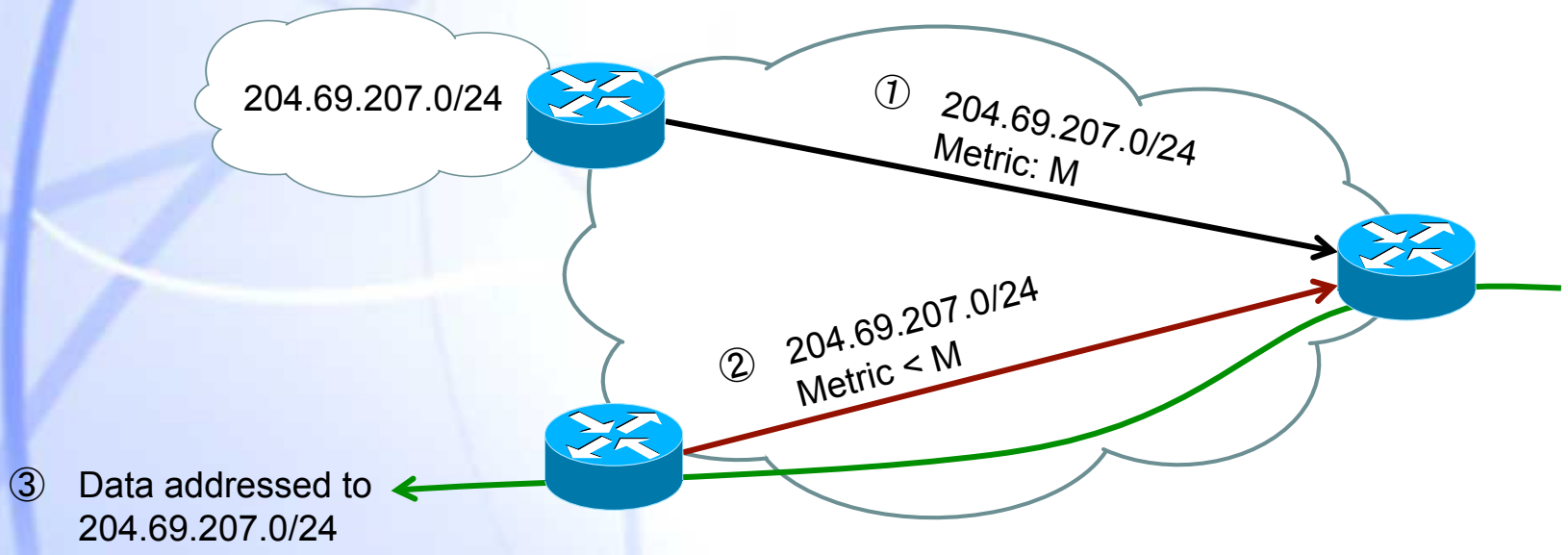
② The victim instantiates state to handle the incoming connections

③ Victim runs out of memory used to hold TCP state, so it cannot serve a legitimate TCP connection setup

✓ It is essentially a memory exhaustion attack
✓ May cause a system crash in poorly coded operating system

Overview of DoS attacks

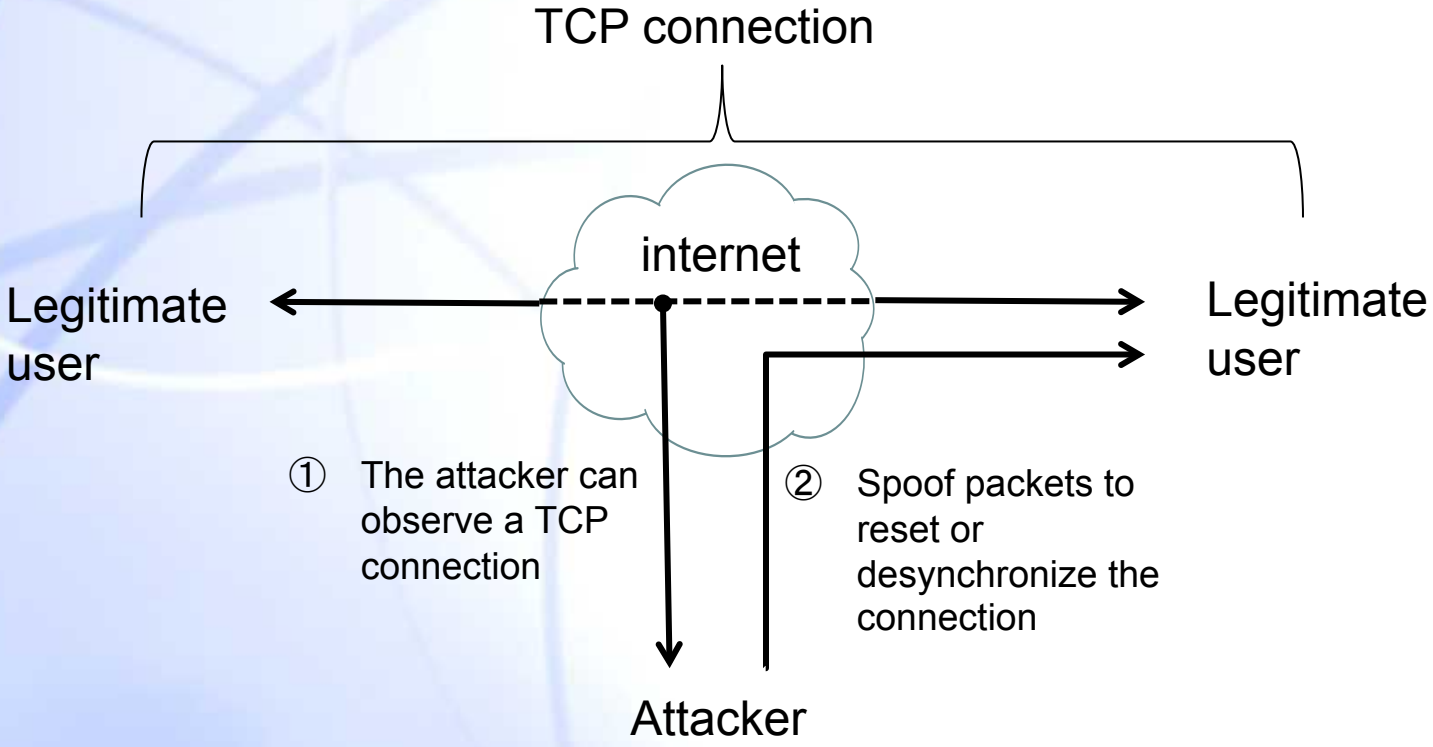
- **DoS attacks on routers:**
  - **Attacks through routing protocols**
    - ✓ **Requires the ability to send traffic from appropriate addresses**
    - ✓ **Ex: announcing a spoofed desirable route to a given destination**



  - **Attacks based on IP Multicast**
    - ✓ **Ex: sending packets to many different multicast addresses in PIM-SM**

Overview of DoS attacks

- **DoS attacks on ongoing communications:**
  - **Ex: disrupting an ongoing TCP communication**



Overview of DoS attacks

- **DoS attacks on local infrastructure:**
  - Some attacks can only be performed by a local attacker
  - Examples:
    - ✓ Exhausting the address pool allocated by a DHCP server,
    - ✓ ARP spoofing,
    - ✓ etc.
- **Link flooding attacks**
  - Causing severe congestion on a bottleneck link
- **Physical DoS:**
  - Previous DoS attacks are perpetrated using the network
  - It can be easier to perform a physical DoS attack
  - Examples:
    - ✓ Causing a power failure,
    - ✓ cutting network cables,
    - ✓ switching a system off,
    - ✓ etc.

Overview of DoS attacks

- **Social engineering DoS**
  - The weakest link can be human
  - Example: convincing an employee to make a configuration change that prevents normal operation

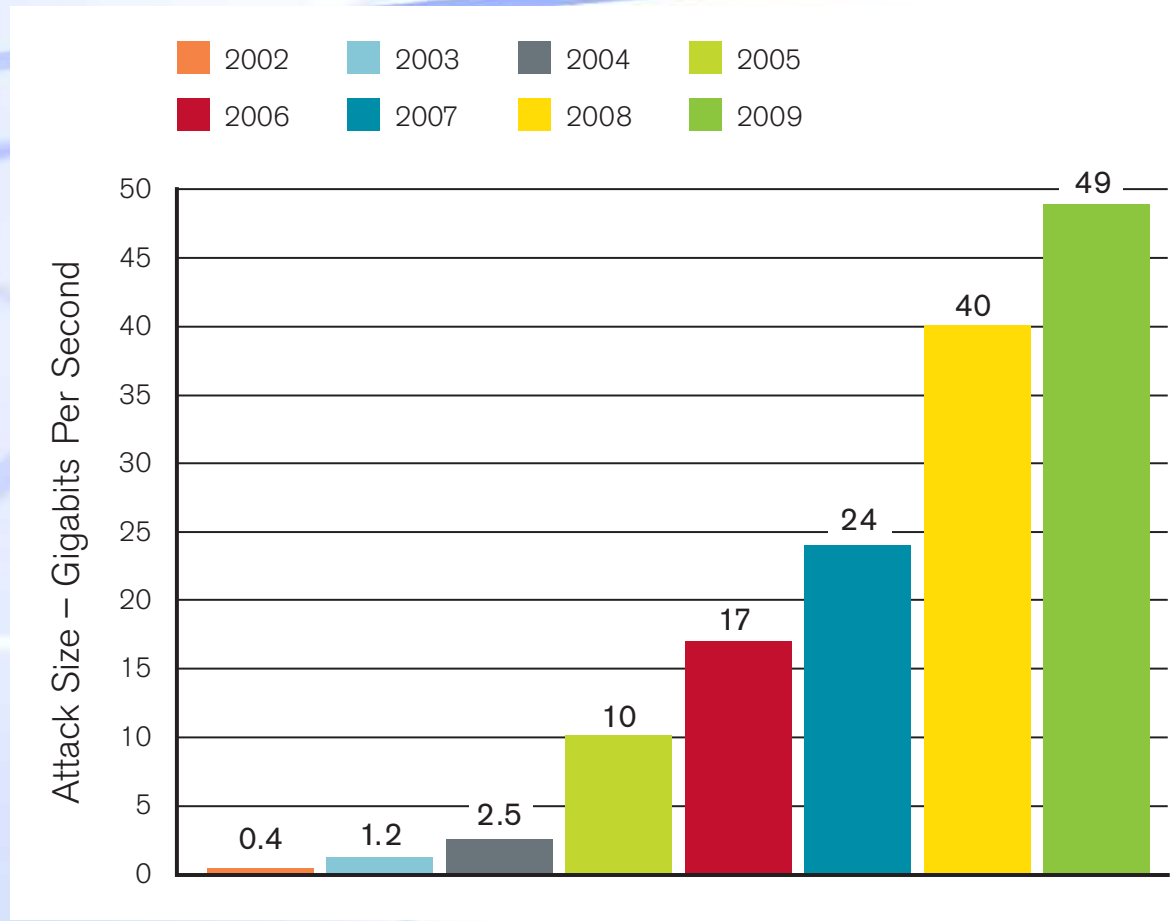
- **Unsolicited commercial email (spam)**
  - Although the intention is not DoS, spam can cause denial-of-service
    - ✓ Spam can waste the recipient's time or cause legitimate email to be misplaced
    - ✓ Spam filtering can produce some level of false positives

US-CERT recommendations

- ***How do you know if an attack is happening?***
  - ***Unusually slow network performance (opening files or accessing websites)***
  - ***Unavailability of a particular website***
  - ***Inability to access any website***
  - ***Dramatic increase in the amount of spam you receive in your account***
- ***What do you do if you think you are experiencing an attack?***
  - ***If you notice that you cannot access your own files or reach any external websites from your work computer, contact your network administrators. This may indicate that your computer or your organization's network is being attacked.***
  - ***If you are having a similar experience on your home computer, consider contacting your internet service provider (ISP). If there is a problem, the ISP might be able to advise you of an appropriate course of action.***

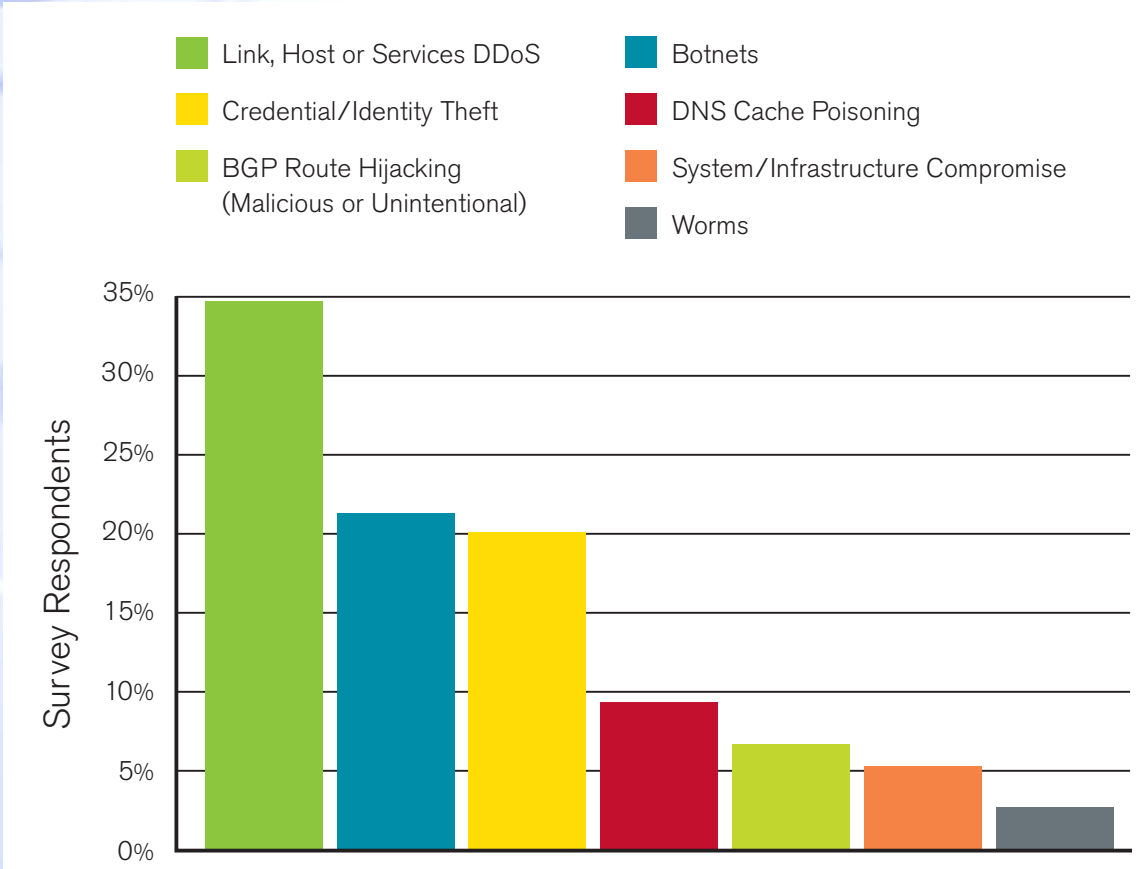
US-CERT
United States Computer Emergency Readiness Team
http://www.us-cert.gov/cas/tips/ST04-015.html

Largest DDoS attack



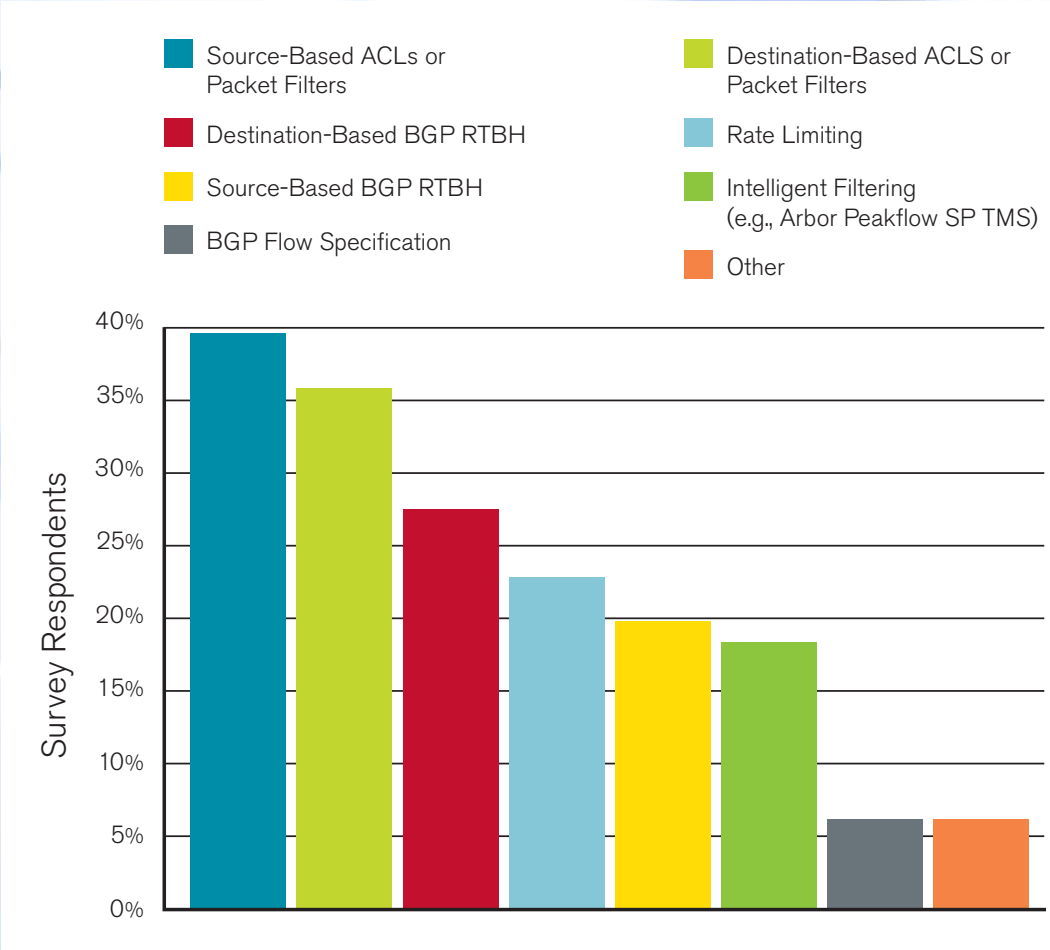
Source: 2009 Worldwide infrastructure security report, Arbor Networks, Inc.

Largest anticipated threat: next 12 months



Source: 2009 Worldwide infrastructure security report, Arbor Networks, Inc.

Primary attack mitigation techniques

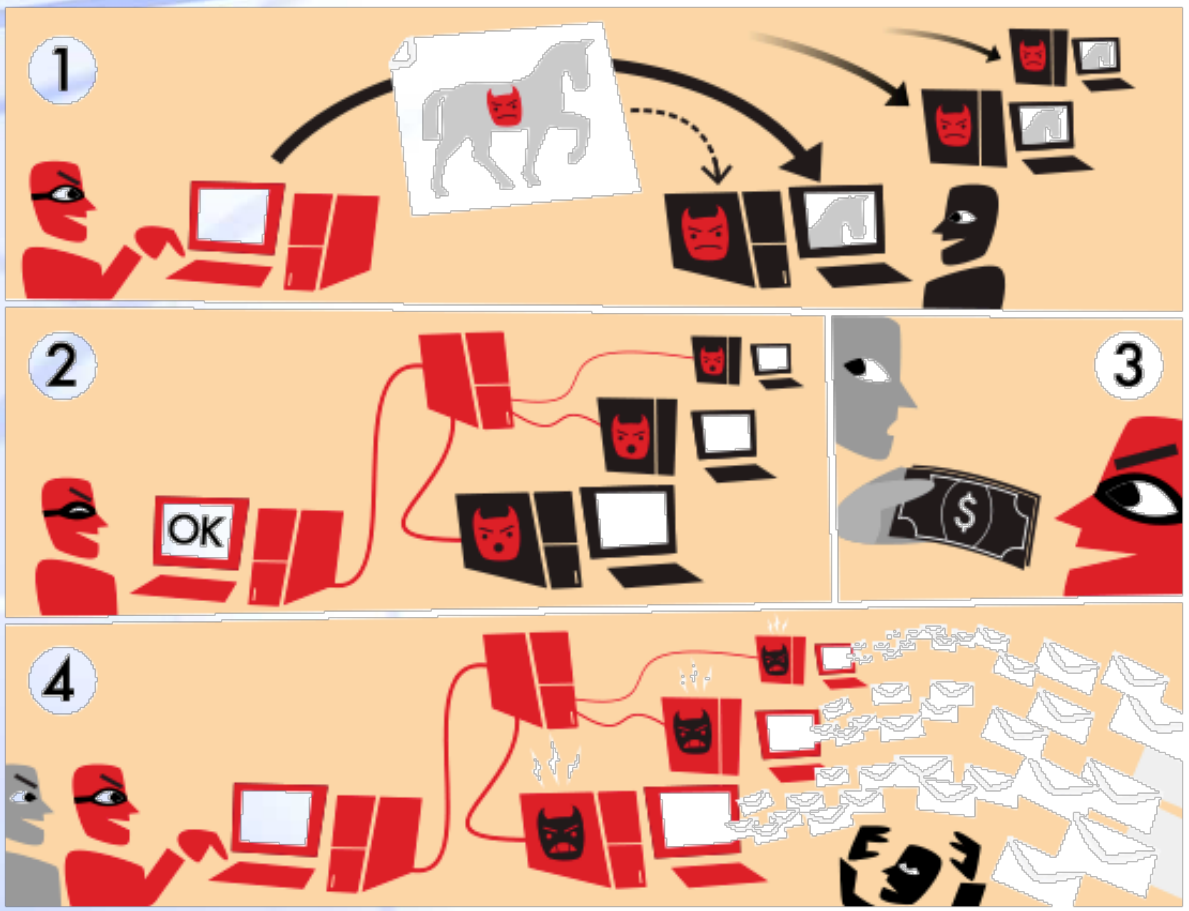


Source: 2009 Worldwide infrastructure security report, Arbor Networks, Inc.

Bots and botnets

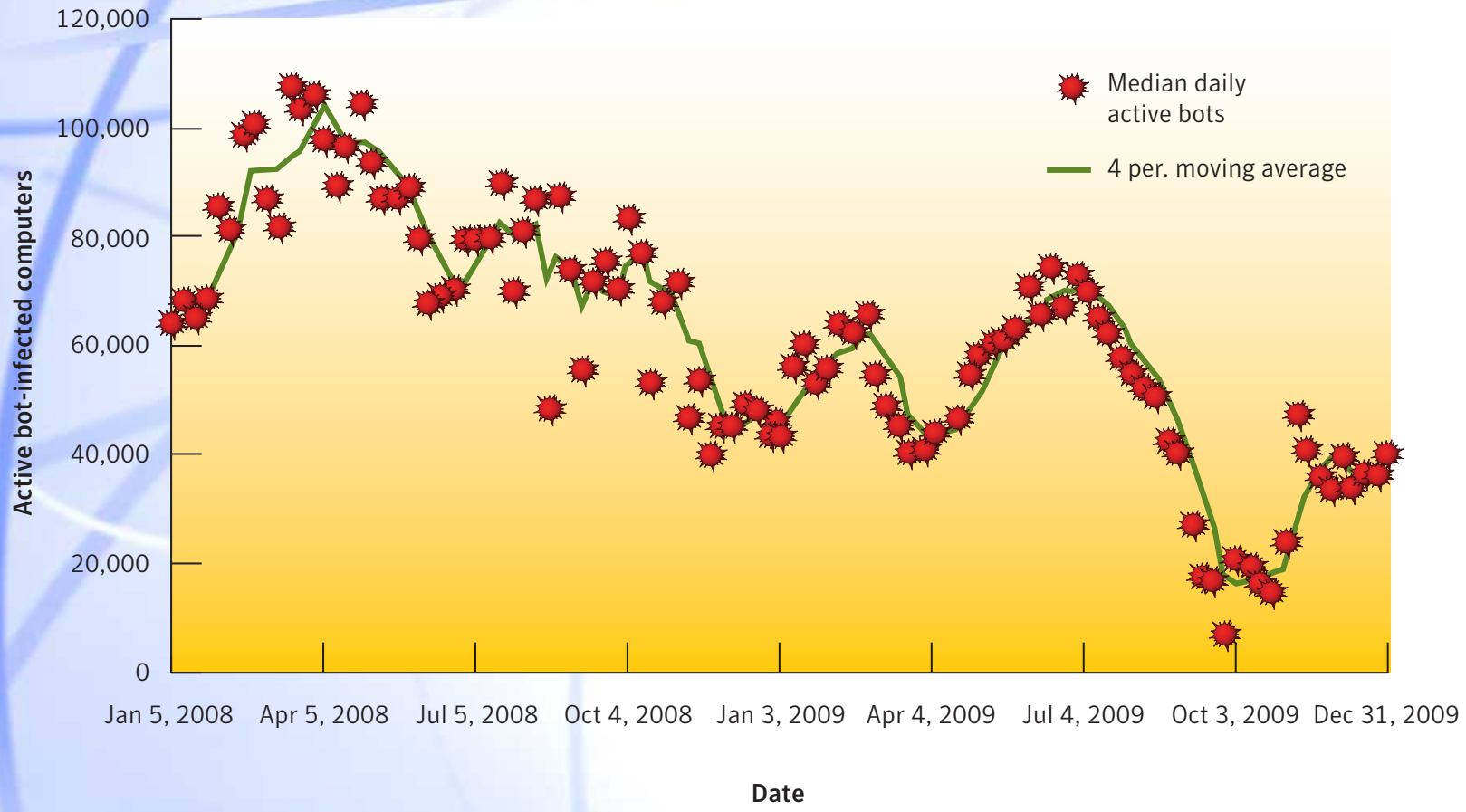
- **Bot:**
  - Short for *robot*
  - Programs that are covertly installed on a user computer
  - Allow an attacker to remotely control the computer (e.g. via IRC, P2P or HTTP).
- **Botnet:**
  - Also known as *zombie army*
  - A large number of compromised computers controlled by an attacker
  - It can be used to launch coordinated attacks
- **Bots can be used for:**
  - DoS attacks, distributing spam, distributing spyware, propagating malicious code, obtaining confidential information, etc
    - ✓ Can lead to serious financial and legal consequences
  - Botnet owners profit from their activities

Example: using a botnet to distribute spam



http://en.wikipedia.org/wiki/File:Botnet.svg

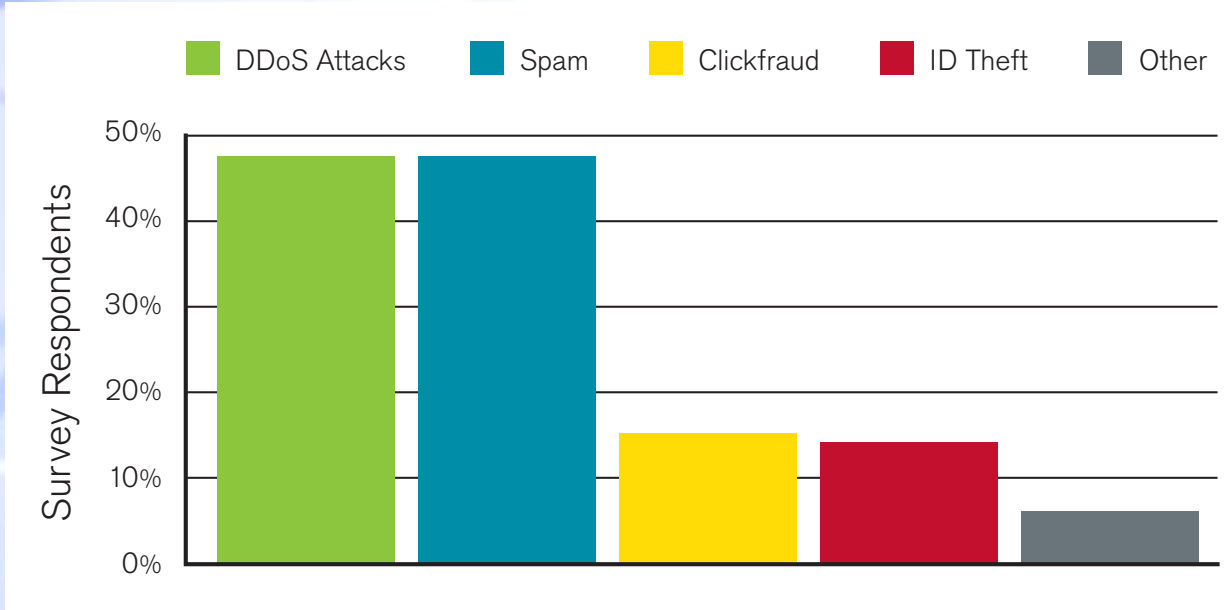
Statistics: bot-infected computers



Active bot-infected computers by day

Source: *Symantec* corporation

Observed bots: past 12 months



Source: 2009 Worldwide infrastructure security report, Arbor Networks, Inc.

Additional statistics: bot-infected computers

- 2009 (XV Symantec Global Internet Security Threat Report):
  - US was the country most frequently targeted by DoS attacks
    - ✓ 56% of the worldwide total
    - ✓ Increase from 51% in 2008
  - Average of 46,541 active bot-infected computers per day, 38% decrease from 2008
  - 6,798,338 distinct bot-infected computers during this period, 28% decrease from 2008.
  - US had the most bot-infected computers, 11% of the worldwide total
  - Taipei was the city with the most bot-infected computers, 5% of the worldwide total

Addressing DoS: the research perspective

- Many solutions have been proposed to address DoS
  - Currently, there is no consensus
- Two schools of thought:
  - Capability-based approach:
    - ✓ Lets a receiver to explicitly authorize the traffic it desires to receive
  - Filter-based approach:
    - ✓ Lets a receiver to install dynamic network filters that block the traffic it does not desire to receive