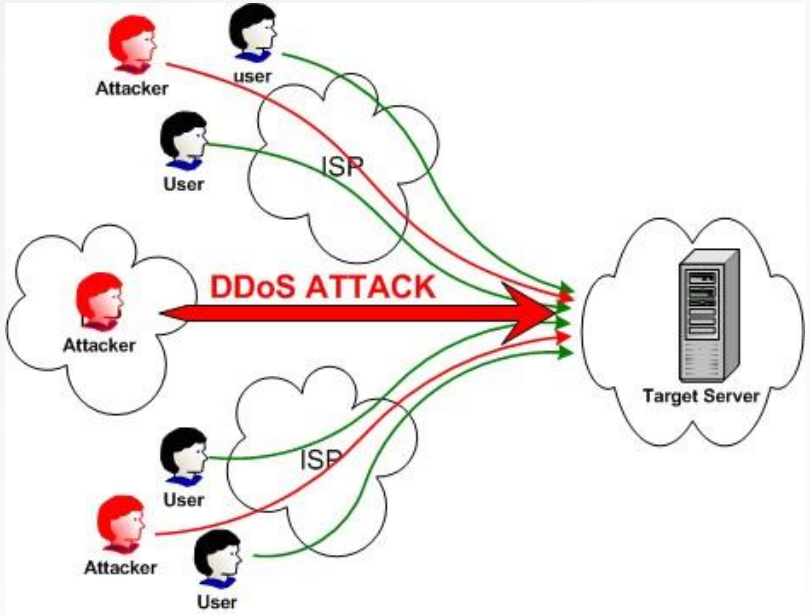
Denial of Service

DENIAL OF SERVICE

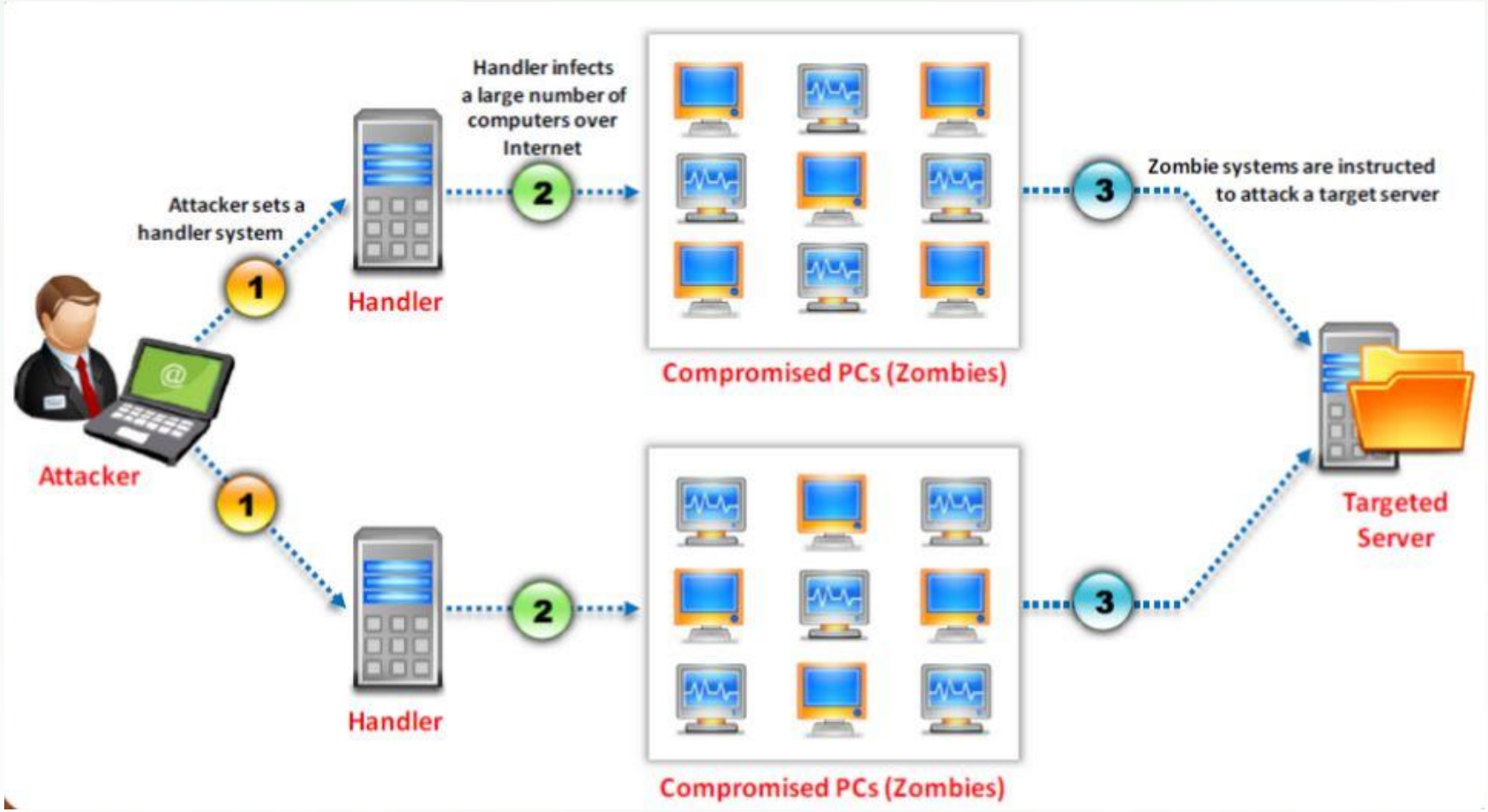
- An attack that prevents authorized users from accessing a computer or network
- Objective of the attack is render the system or service useless



DISTRIBUTED DOS (DDOS)

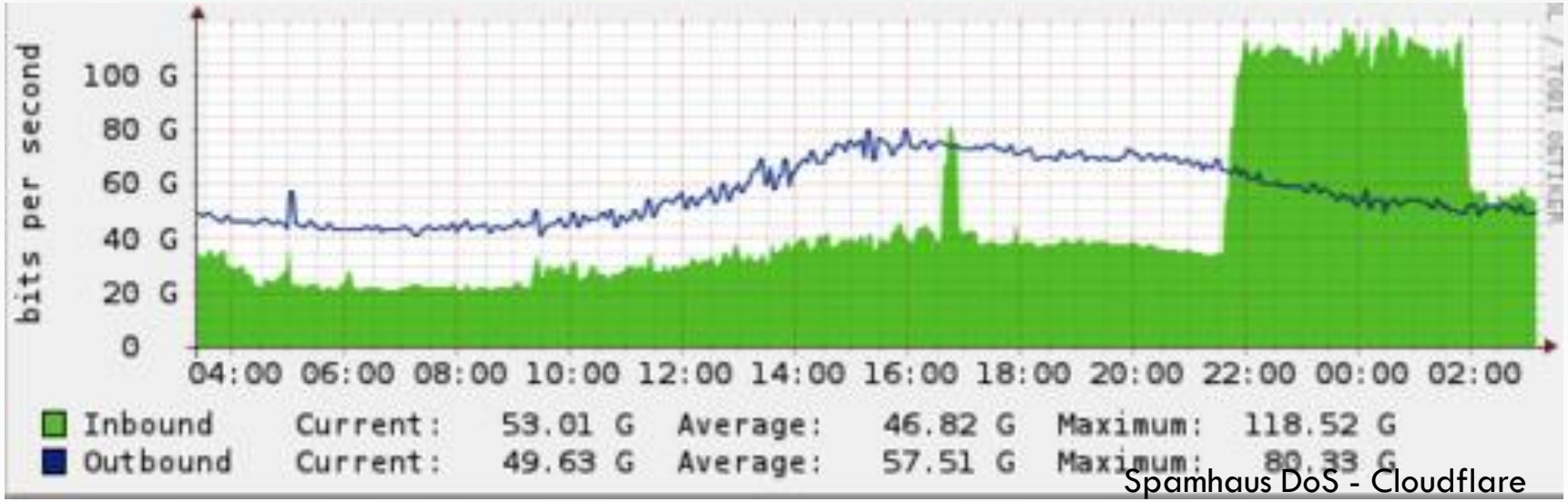
- A large scale coordinated attack on the target computer
- Attack is launched indirectly through a botnet (group of compromised computers)
  - Primary target – actual target computer or service
  - Secondary target – compromised computer

HOW DOES IT WORK?



SYMPTOMS OF A DOS ATTACK

- Unavailability of a particular website
- Inability to access any website
- Unusually slow network performance
- Dramatic increase in amount of email spam



Spamhaus DoS - Cloudflare

DOS IMPACT

- Loss of goodwill
- Disabled network
- Financial loss
- Disabled organization

ATTACK TECHNIQUES

DENIAL OF SERVICE ATTACK (DOS)

- Bandwidth Attack
  - focuses on network traffic
- Protocol Attack
  - focuses on flaws in the implementation of protocols
- Logic Attack
  - focuses on flaws in the implementation of software

BANDWIDTH ATTACK

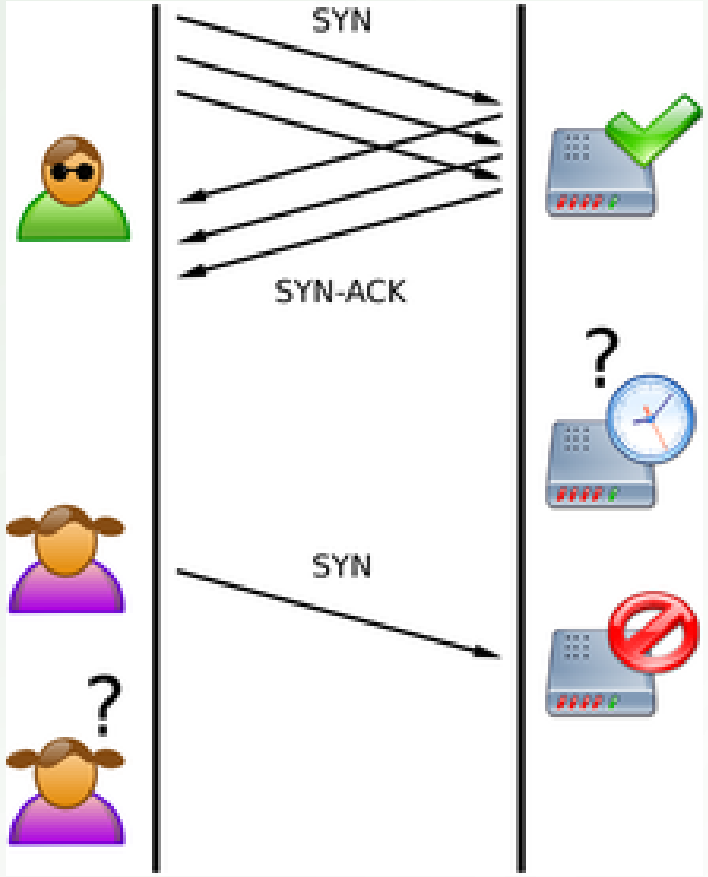
- Floods network with a large volume of malicious packets
- Overwhelms the network bandwidth
  - Network drop packets even for legitimate users
- Carried out by multiple machines to generate large volume of traffic
- Can be difficult to detect origin because of too may computers carrying the attack

SERVICE REQUEST FLOODS

- Attackers or group of zombies attempts to exhaust server resources by setting up and tearing down TCP connections
- Floods server with high rate of connection from a valid connection
- Initiates a request on every connection
- Makes the service look sluggish

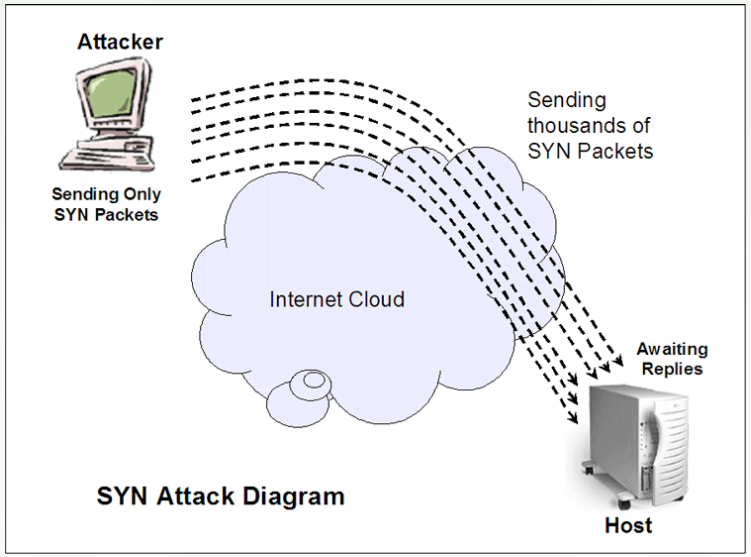
SYN ATTACK

- Attacker sends a series of SYN request from a fake source to the target machine
- Target machine never gets any response after replying with SYN+ACK packet
- Server will have too many connections open which eats up the resources



SYN FLOOD

- Attack occurs when the intruder sends unlimited SYN packets to the host system
- Process of transmitting of SYN packets is faster than the system can handle

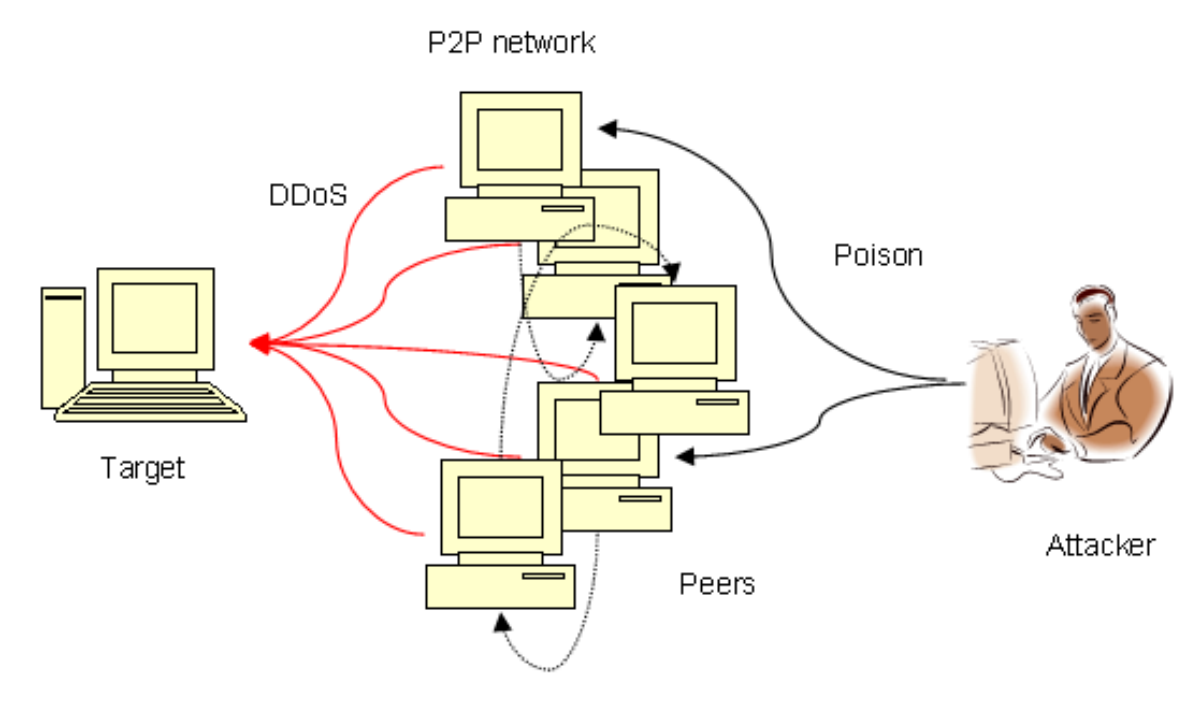


ICMP FLOOD ATTACK

- Attack occurs when zombies send large volume of ICMP Echo packets to a target computer
  - Saturates the bandwidth of target's network connection
  - Packets have spoofed IP to crash the target
- When the ICMP threshold is reached, router rejects further ICMP Echo request from all addresses in the same security zone

PEER-TO-PEER ATTACK

- Attacker exploits bugs in a peer-to-peer servers to initiate attack
  - Instructs clients of peer-to-peer file sharing hubs to connect to the victim website
- Creates large traffic on the victim website to slow it down



PERMANENT DOS

- Also known as phlashing
- Sabotages the system hardware
- This is done through a Trojan and bricks the system

APPLICATION LEVEL FLOOD ATTACK

- Loss of service of a particular network
- Exploit software to cause confusion in the application
  - Fills up disk space
  - Consume memory or CPU cycles
  - Disrupt access through locking out an account
  - Jam database connections using malicious SQL

BOTNET

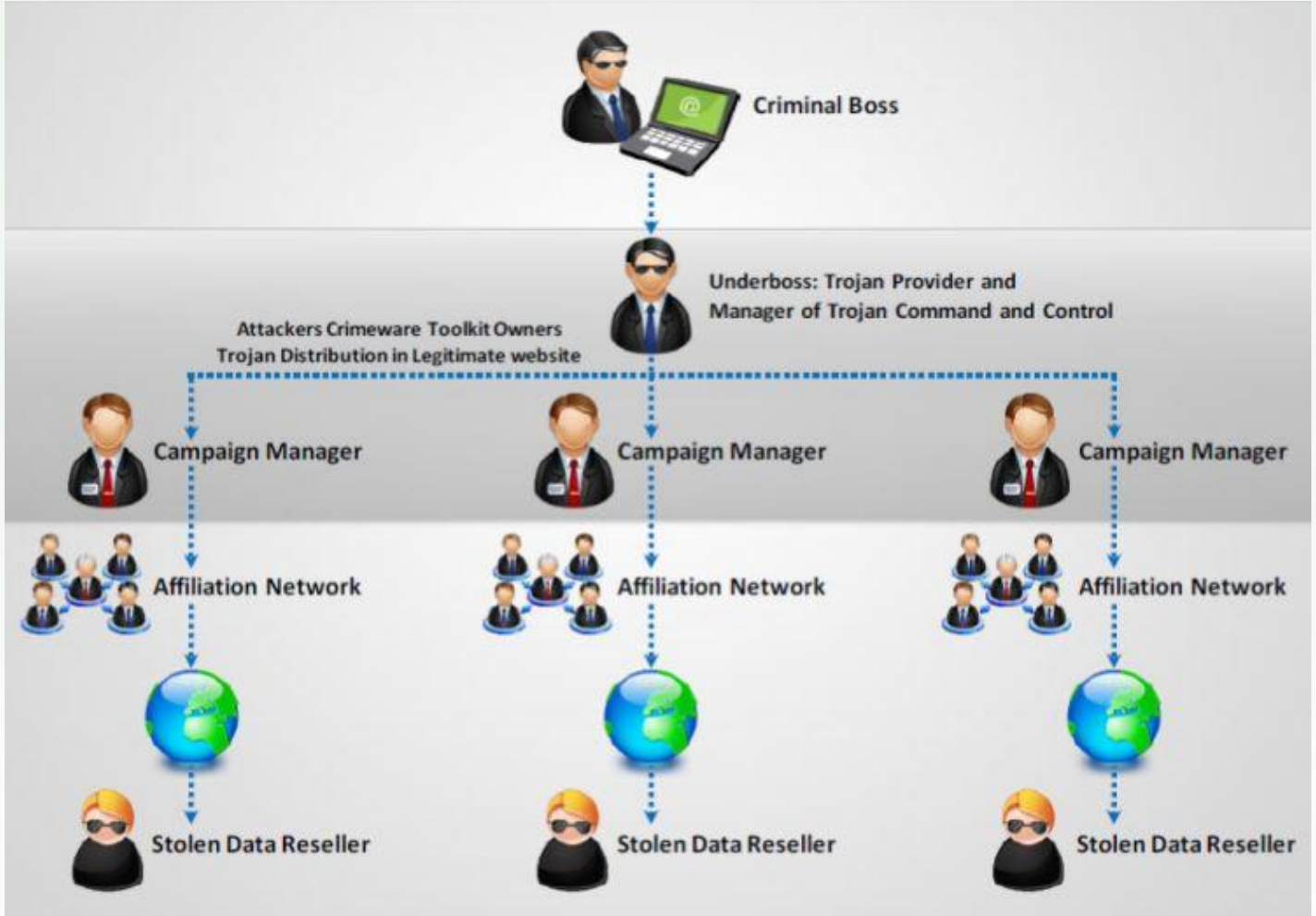
ORGANIZED CRIME SYNDICATE

- Groups of cybercriminals who work in a hierarchical setup to offer services
  - Create and rent botnets
  - Malware writing
  - Hack bank accounts
  - Launch DoS

BOTNET

- A software on a computer that performs automated task over the Internet without the knowledge of the user or administrator
  - Huge compromised systems to perform DOS attacks
- This is the from the word “Robot Network”
- Normally used by cyber crime syndicates to perpetrate
  - Politically motivated cyber warfare
  - Hacktivism
  - Steal data

HIERARCHY


Criminal Boss
Underboss: Trojan Provider and
Manager of Trojan Command and Control
Attackers Crimeware Toolkit Owners
Trojan Distribution in Legitimate website
Campaign Manager
Campaign Manager
Campaign Manager
Affiliation Network
Affiliation Network
Affiliation Network
Stolen Data Reseller
Stolen Data Reseller
Stolen Data Reseller

DOS DETECTION AND COUNTERMEASURES

DOS DETECTION TECHNIQUES

- Activity Profiling
  - Monitoring header information
  - Monitoring rate of consecutive packets with similar headers
- Sequential Change-point Detection
  - Uses expected average traffic statistics to determine attacks
  - Detects abrupt changes in traffic patterns

DOS COUNTERMEASURES STRATEGIES

- Absorb the attack
  - Additional resources are deployed to absorb attack
- Degrade services
  - Only allow critical services to operate
  - Allow poor service performance until attack subsides
- Shutdown services
  - Shutdown service until attack subsides

SOME MORE DDOS COUNTERMEASURES

- Protect secondary targets
- Neutralize handlers
- Prevent potential attacks
  - Ingres and egress filtering, TCP intercept
- Deflect attacks
  - Uses honeypots to deflect attacks
- Mitigate attacks
  - Load balancing
  - Throttling
- Post-attack forensics
  - Study the DOS/DDOS attack to be able to get rid of it

HOW ABOUT BOTNETS?

- RFC 3704 (unused / reserved address) filtering
- Blackhole filtering
- IP reputation filtering
- DDOS products