DDoS

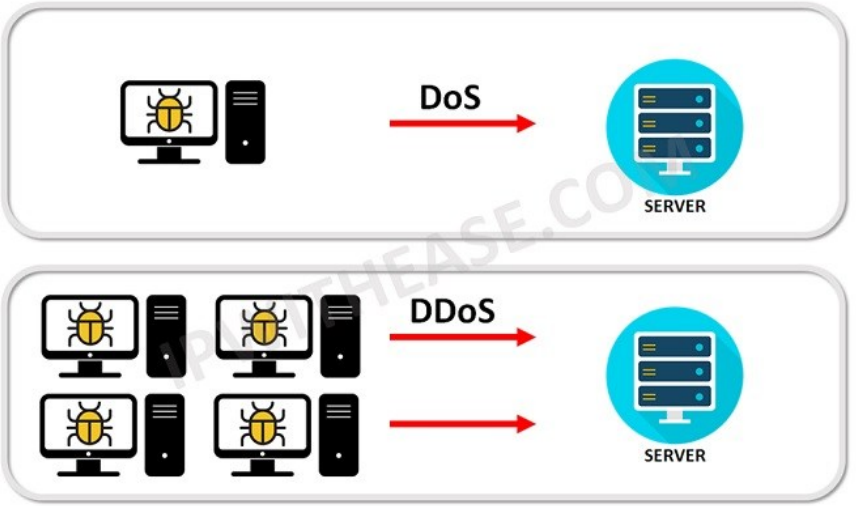
outline

- DoS attacks
- botnet
- DDoS attacks

DoS attacks

DoS vs DDoS

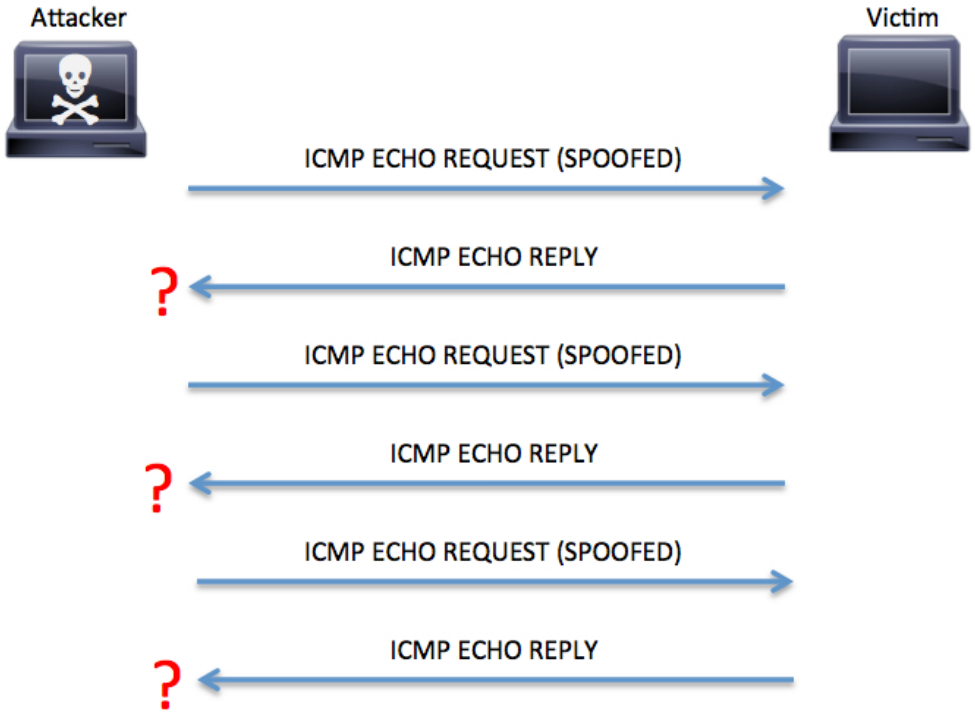
- A denial-of-service attack (DoS attack) or distributed DoS attack (DDoS attack) is an attempt to make a computer resource unavailable to its intended users
  - DoS: a single machine performs attacks
    - Exploits system design weaknesses (e.g., ping of death)
    - often uses flooding as well
  - DDoS: a botnet performs attacks
    - flooding-based
- DoS/DDoS denies a victim (host, router, or entire network) from providing or receiving normal services



source: https://ipwithease.com/dos-vs-ddos/

DoS attacks

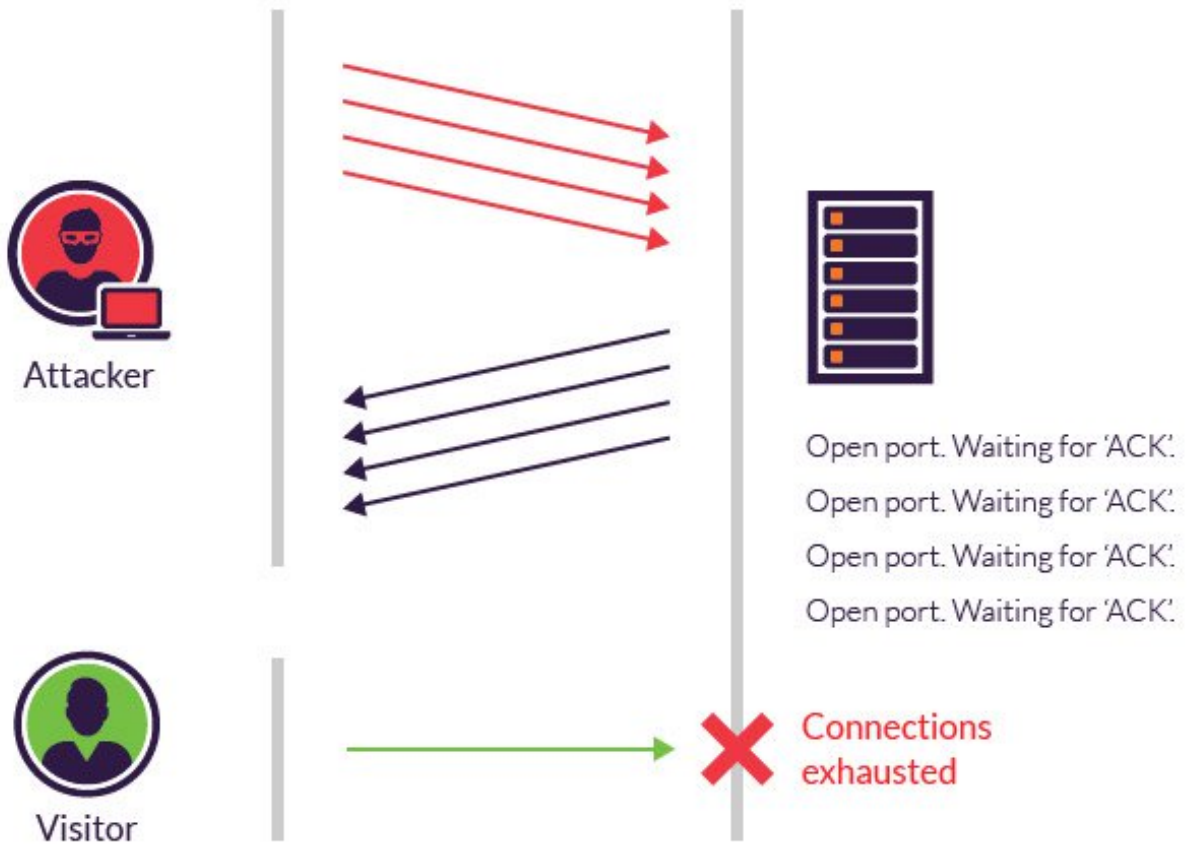
- Scenario
  - Attacker uses forged source addresses
    - given sufficient privilege to “raw sockets”
    - easy to create
  - generates a large volume of packets
    - directed at target
    - with different, random, source addresses
    - May cause some congestion
  - responses are scattered across Internet
  - real source is much harder to identify
- Example
  - Ping of death (a series of fragmented packets)
  - Ping flooding



source: https://admin-ahead.com/blog/ping-flood-attack/

SYN flooding attack

- attacker sends SYN packets with spoofed source addresses
- but does not send ACK packets



source: https://www.imperva.com/learn/ddos/syn-flood/

SYN cookies

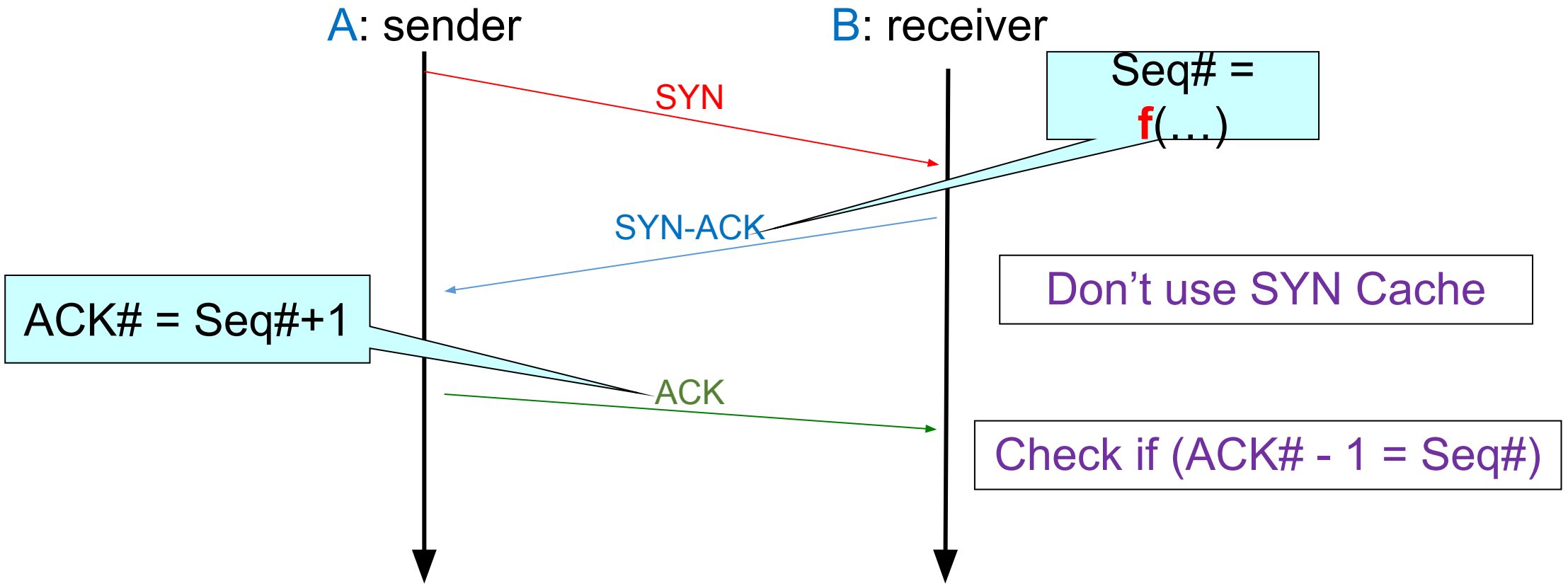
- A SYN flooding attack leaves half-open connections
  - The “SYN queue” keeps track of these half-open connections
    - a transmission control block (TCB) is created for each new TCP connection
  - We track the 4-tuple (source IP and port, destination IP and port), seq # of client, seq # of server
  - Idea: we don’t really need to keep all of this
    - We just need enough to recognize the ACK of the client
    - Can we get away without storing *anything* locally?

stateful vs stateless

SYN cookies: illustration

There are some variations in implementing SYN cookies

- server's sequence number is determined cryptographically
  - seq# = **f**(4-tuple, current_time, server_secret), which is written in SYN-ACK packet
  - only the client knows the correct seq#, to be included in ACK and verified by server



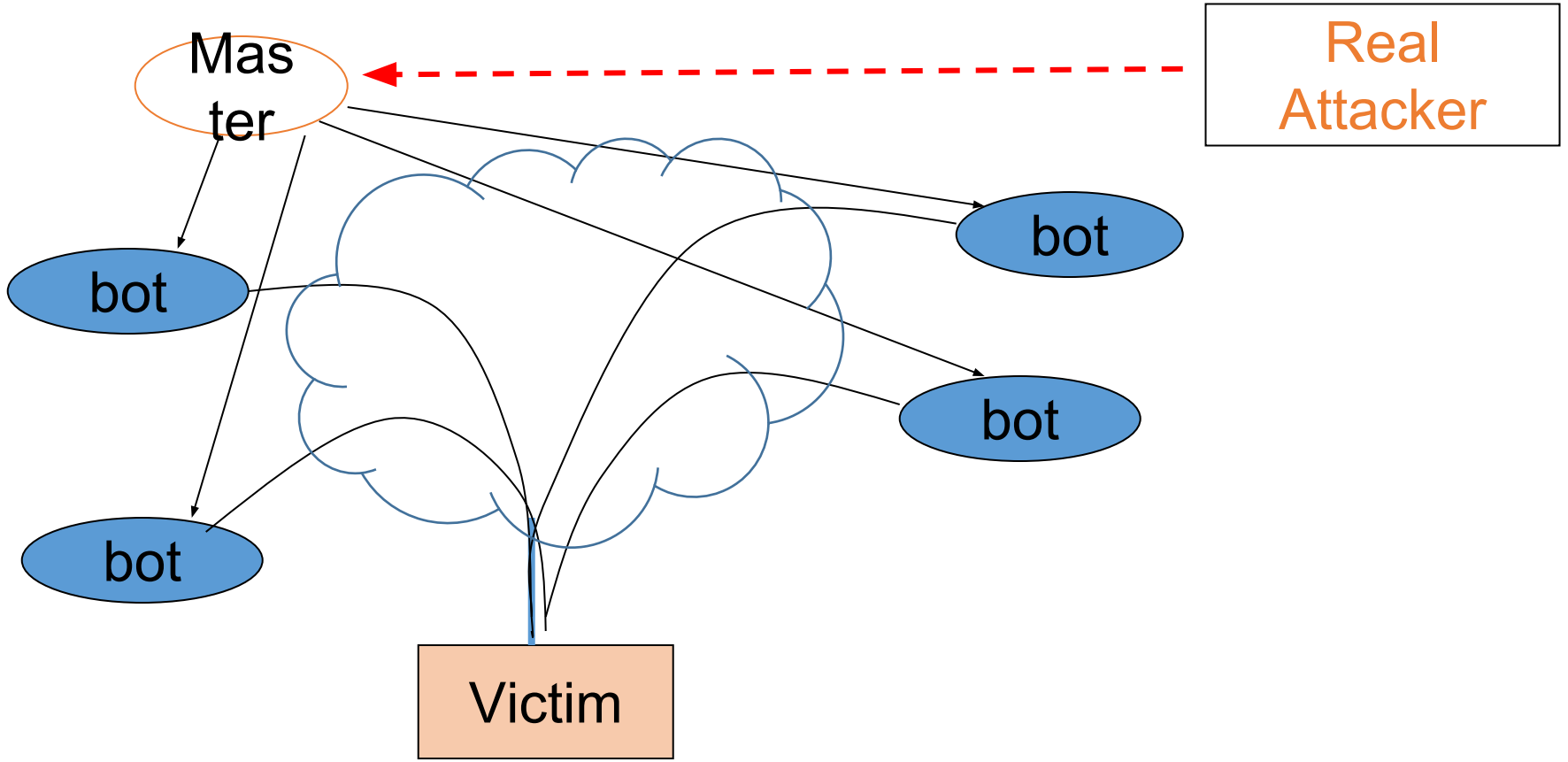
limitation of DoS attacks

- have limited volume if a single source used
- multiple systems can generate much higher traffic volume to form a DDoS Attack
  - Often compromised PC's / workstations
  - Zombies with backdoor programs installed
- Botnet: bot + network
  - Bot: a compromised machine installed with remote controlled code
  - Networked bots under a single commander (botmaster)

botnet

botnet: a network of bots

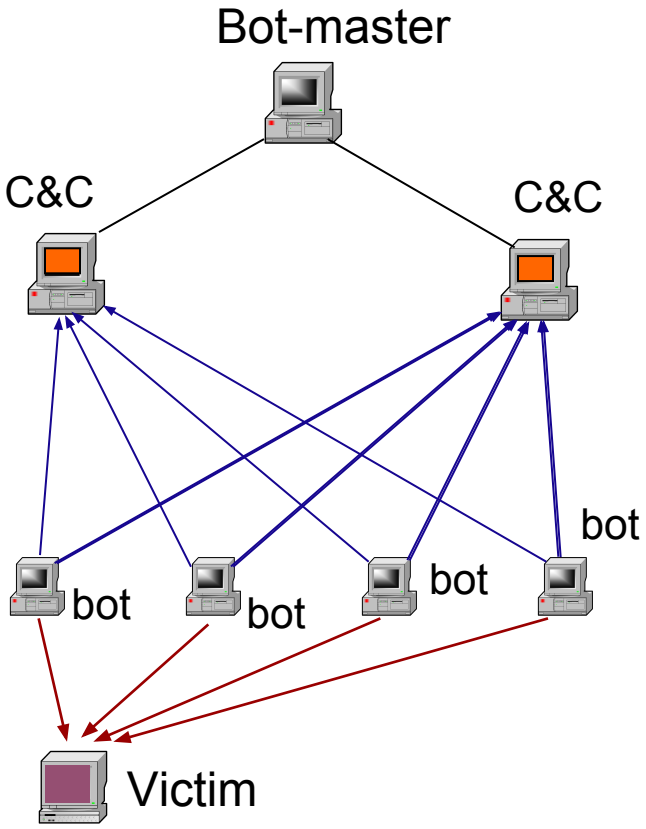
- DDoS attack illustration
  - A botnet is the workhorse



botnet: a detailed view

- a real botnet is more complicated

Bot-master	•composes botnet using malware •sends commands and control to bots
C&C server	•intermediate server that delivers commands and control from bot-master to bots
Bot	•malware developed by a bot-master •performs malicious activities in a client machine •Hard-coded IPs or DNS names of C&C servers
botnet	•a network composed of a number of bots, C&C servers, and a bot-master

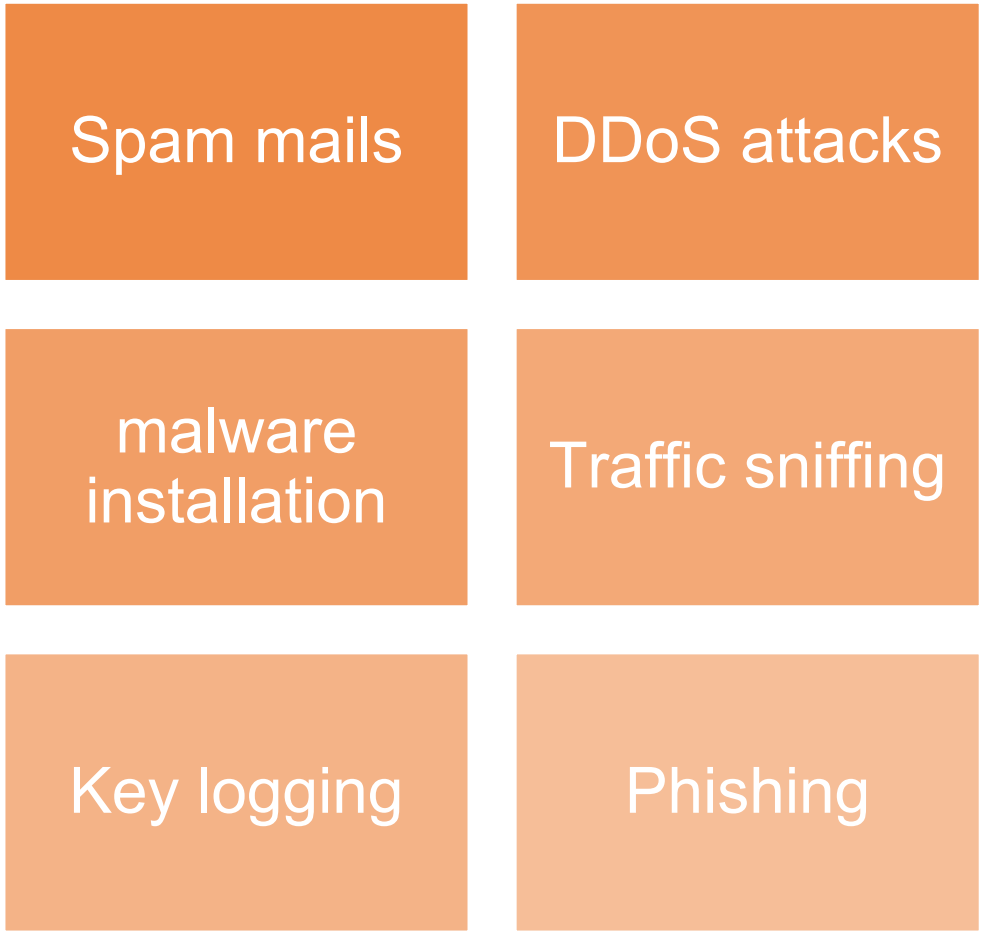


how to make a botnet

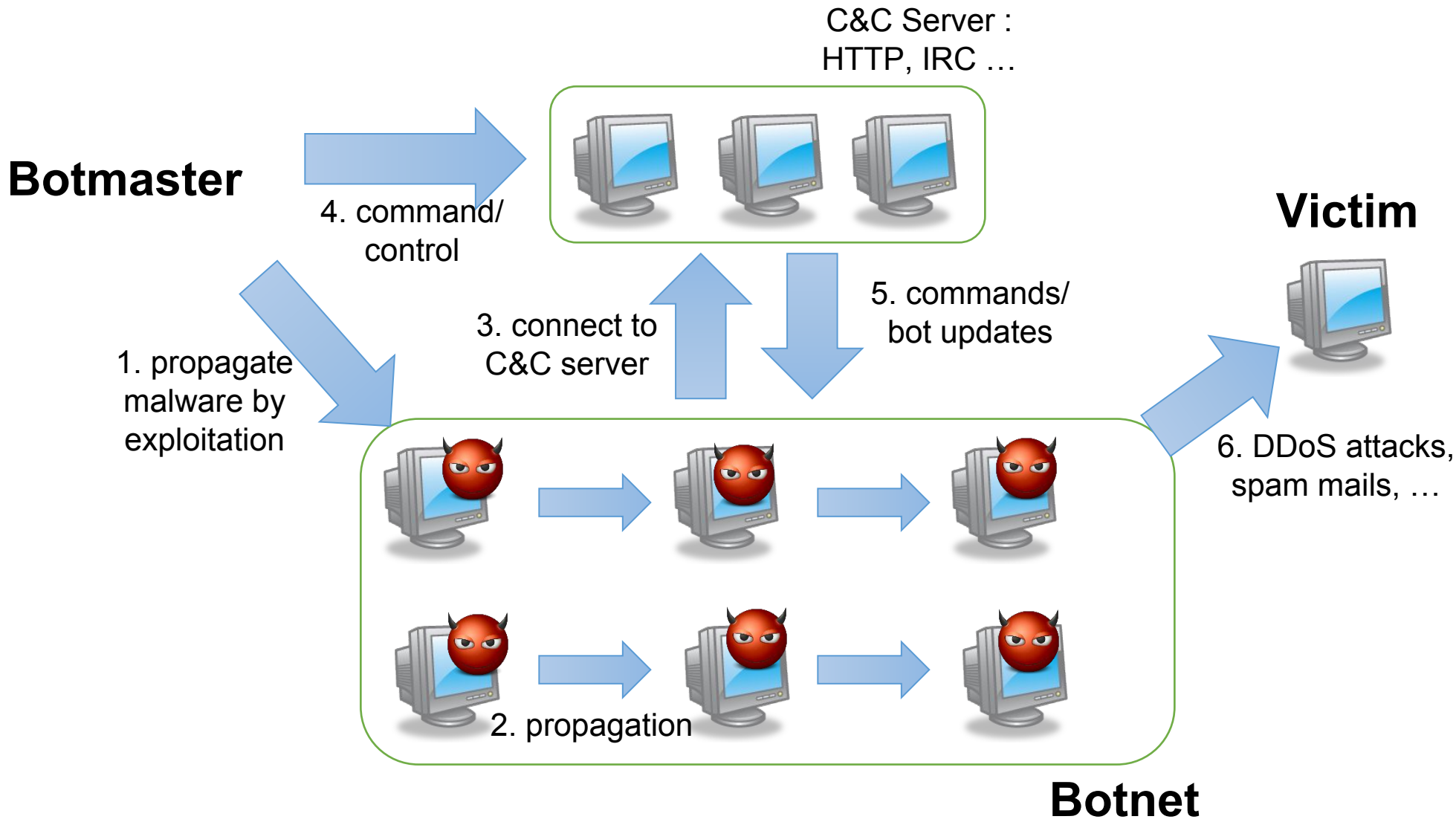
- aka botnet infection
- representative infection methods
  - email attachments
  - clicking on malicious pop up ads
  - downloading dangerous software from a website
- complex botnets may self-propagate, finding and infecting devices automatically
  - worms and Trojan horses

What botnets do

- botnets do malicious activities

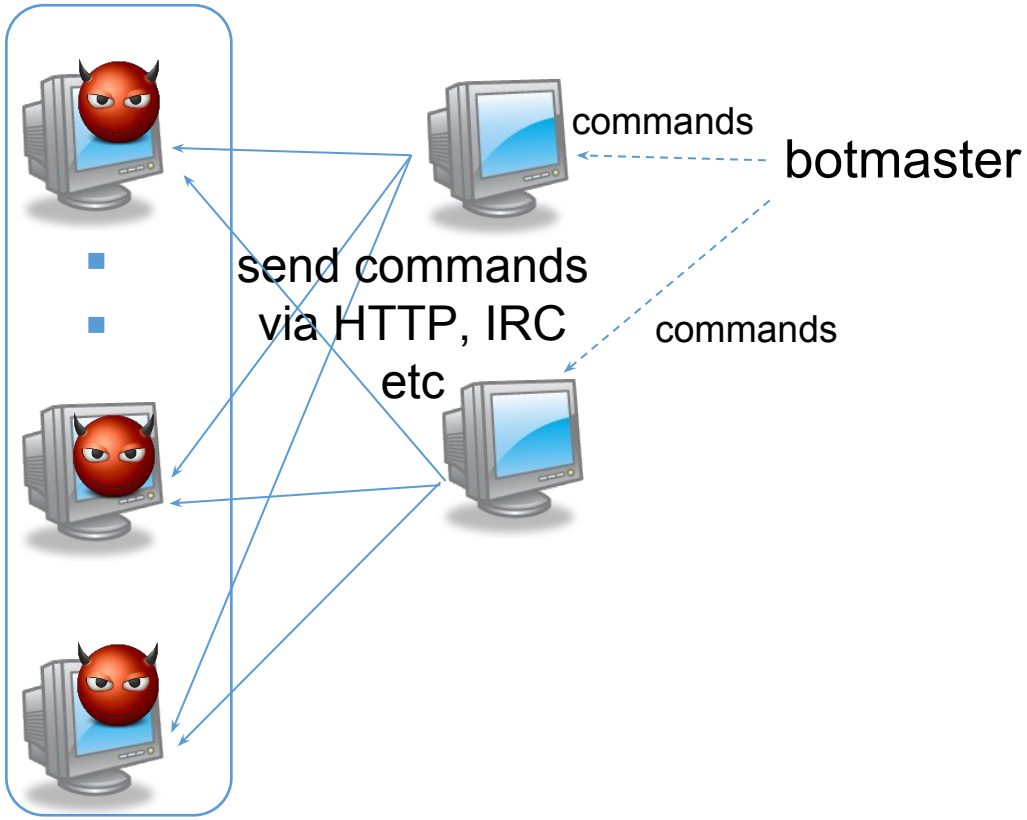


Botnet construction

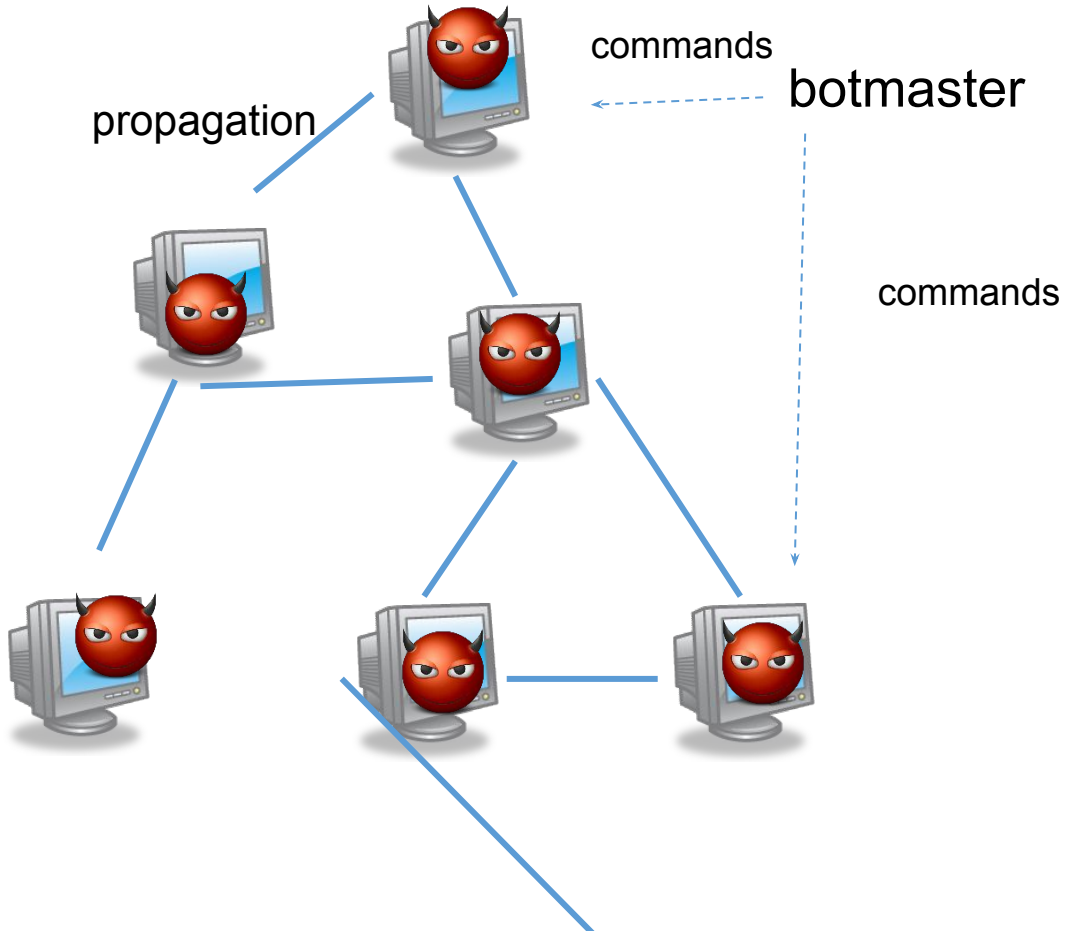


Botnet evolution

- **Centralized model**



- **decentralized model (P2P)**



P2P-based Botnet

- Weakness of C&C botnets
  - A captured bot (e.g., honeypot) could reveal C&C servers
  - The few C&C servers can be shut down at the same time
  - A captured/hijacked C&C server could reveal all or most of the members of the botnet
- C&C centralized P2P control is a natural evolution
  - P2P-based network is believed to be much harder to shut down

botnet features

- Complex propagation/techniques
  - combination of worm/virus, backdoor, spyware, rootkit, …
- Difficult to countermeasure
  - uses normal users' PCs i.e. legitimate IP addresses
  - generates a relatively small number of attack packets by each PC
  - upon DDoS attacks, difficult to distinguish normal user traffic from botnet traffic
  - new botnet techniques have been continually developed

DDoS-as-a-service

- Aka stresser or booter service
  - Can be used in good or evil way
- So easy to attack any host

Source: https://datadome.co/bot-management-protection/ddos-layer-7-security-protection/

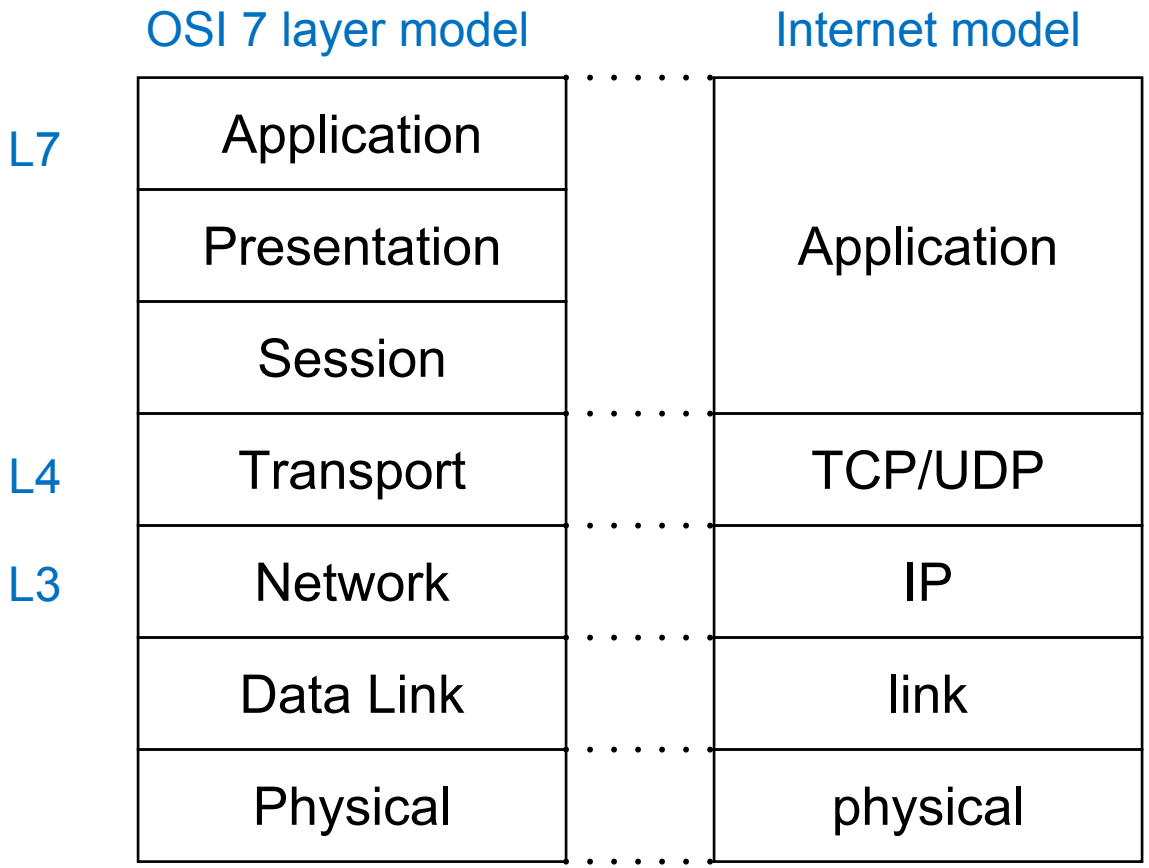
DDoS attacks

DDoS attack classification

- bandwidth depletion vs (system) resource depletion
- L7 vs L4 vs L3
- direct vs reflection vs amplification
- other criteria...

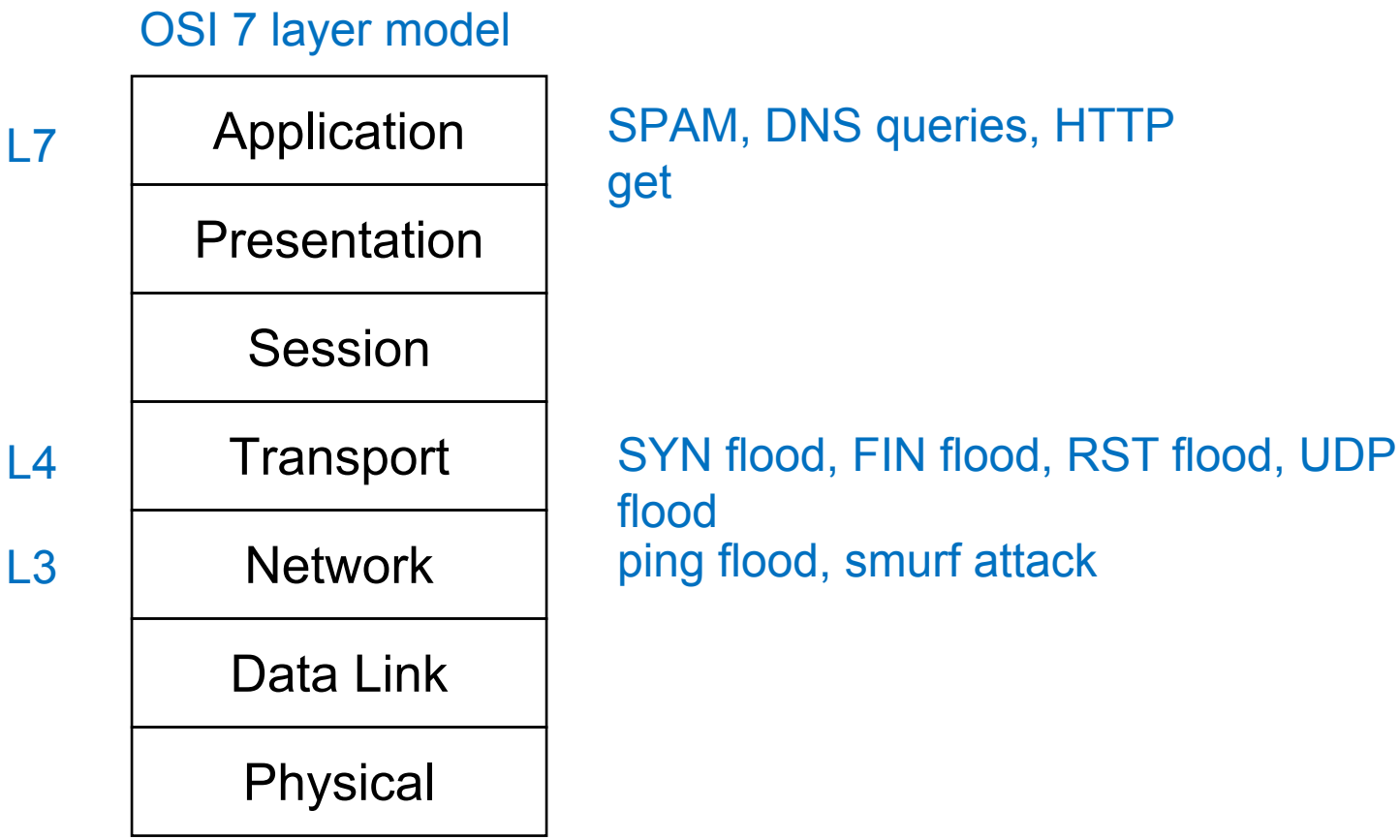
OSI 7 layer reference model

- two reference models for networking



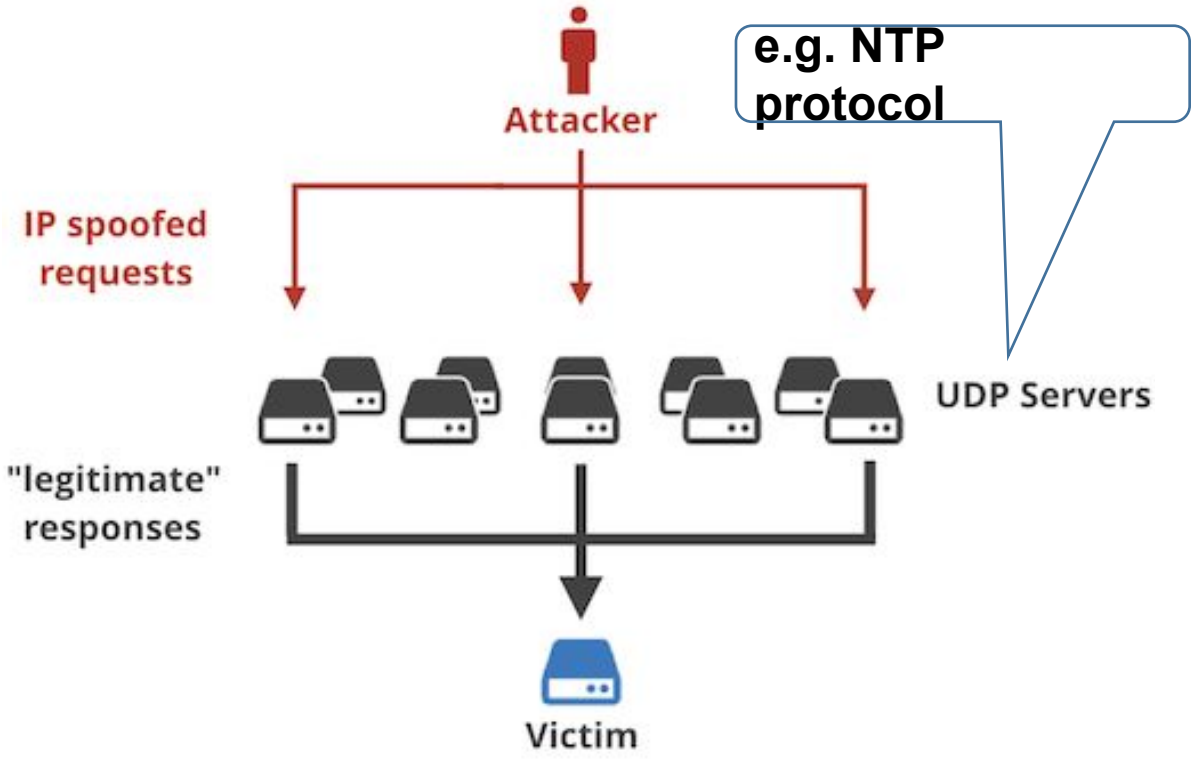
DDoS attacks on different layers

- well-known attacks in each layer
- packets are for some particular protocol in a layer



reflection attack

- use normal behavior of network
- bots send packets with spoofed source addresses, which is the target
- server response is directed at target
- if bots send many requests to multiple servers, response can flood target

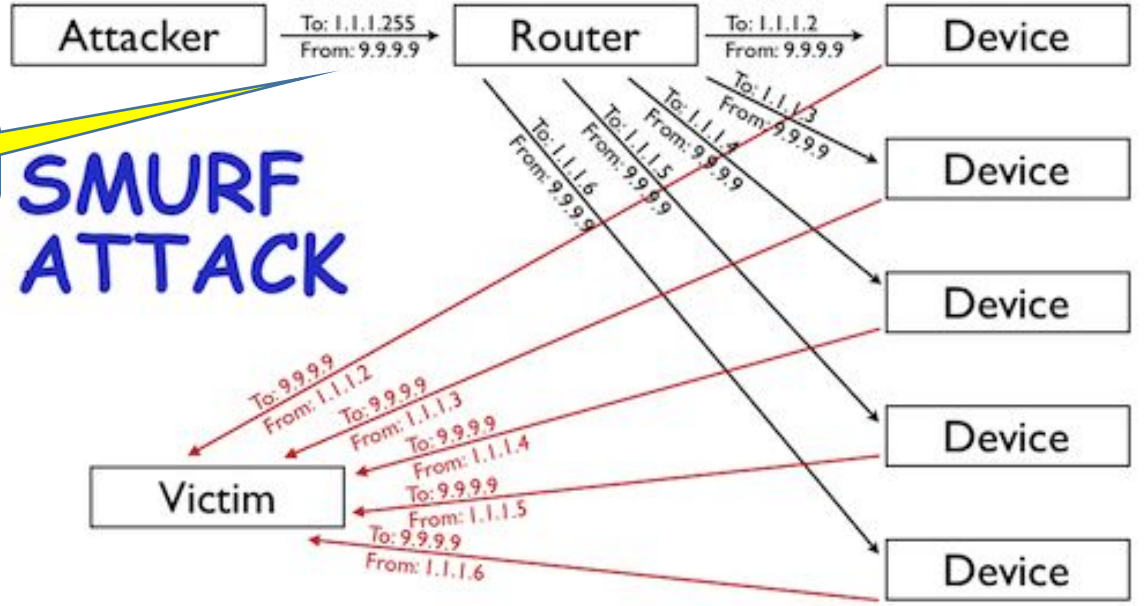


source: https://blog.cloudflare.com/reflections-on-reflections/

amplification attack

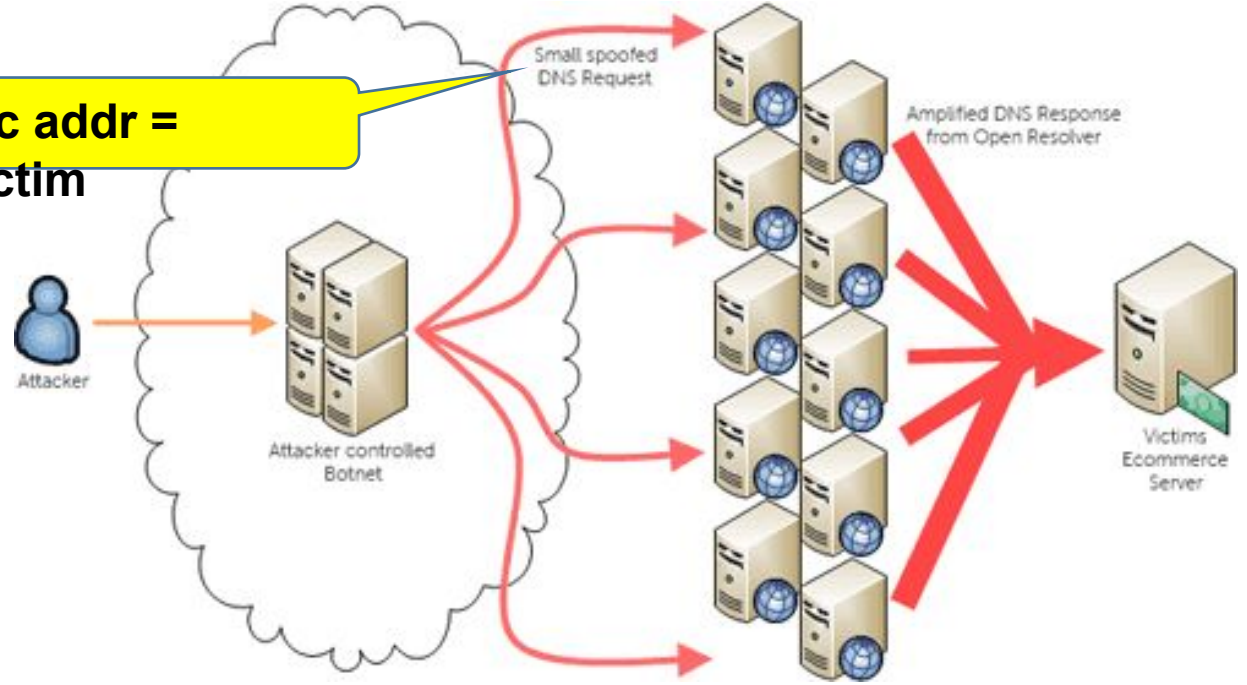
- Amplification attacks are a variant of reflection attacks
  - Two types
- the original request to the broadcast address
  - all hosts on that network can potentially respond to the request
  - called a smurf attack
- Or the response is much bigger than the request
  - DNS request/response

dest addr = broadcast



source: https://blog.cloudflare.com/deep-inside-a-dns-amplification-ddos-attack/

src addr = victim

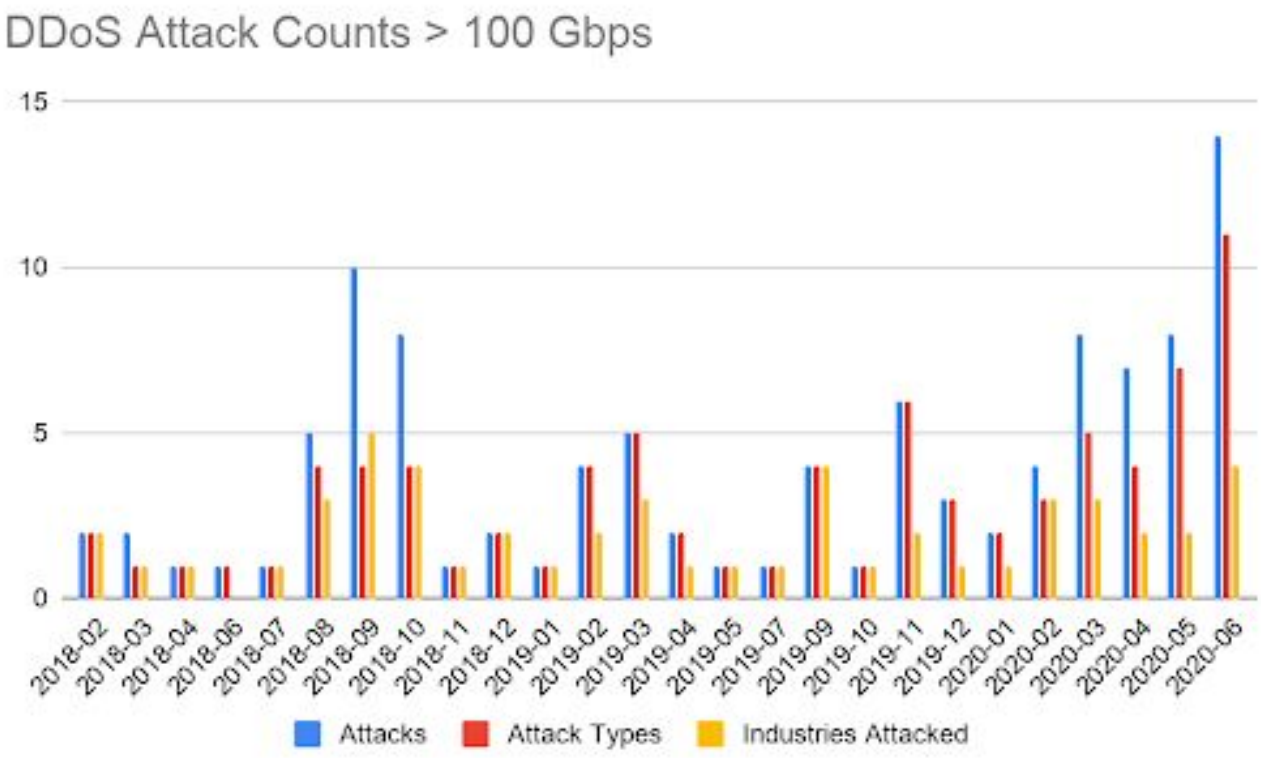


source: https://blog.sflow.com/2013/10/dns-amplification-attacks.html

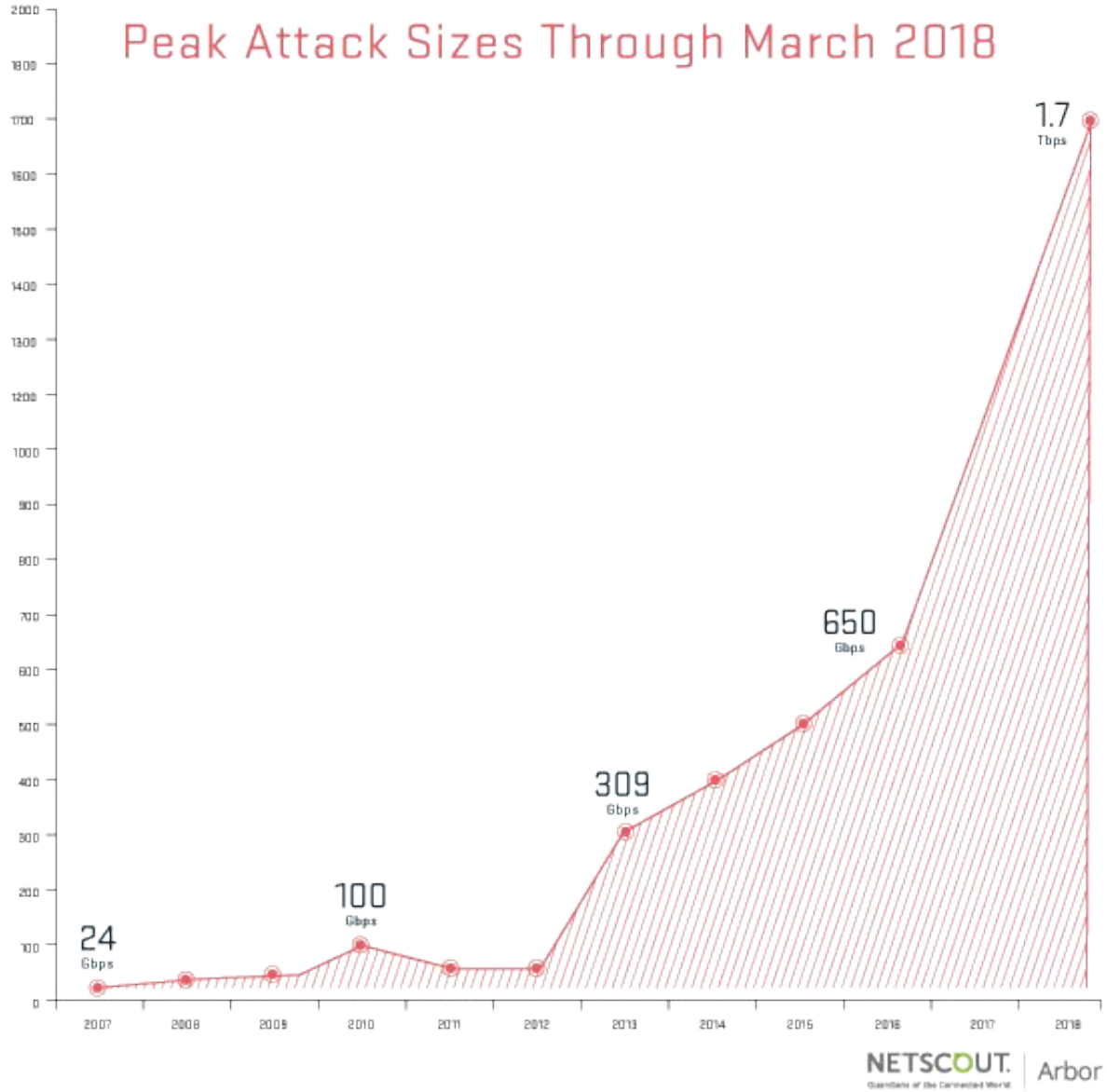
general response to DDoS

- blackholing
- Access control list
- Firewall
- Intrusion Detecting System (IDS)
  - Intrusion prevention system (IPS)
- manual response
- Load Balancing

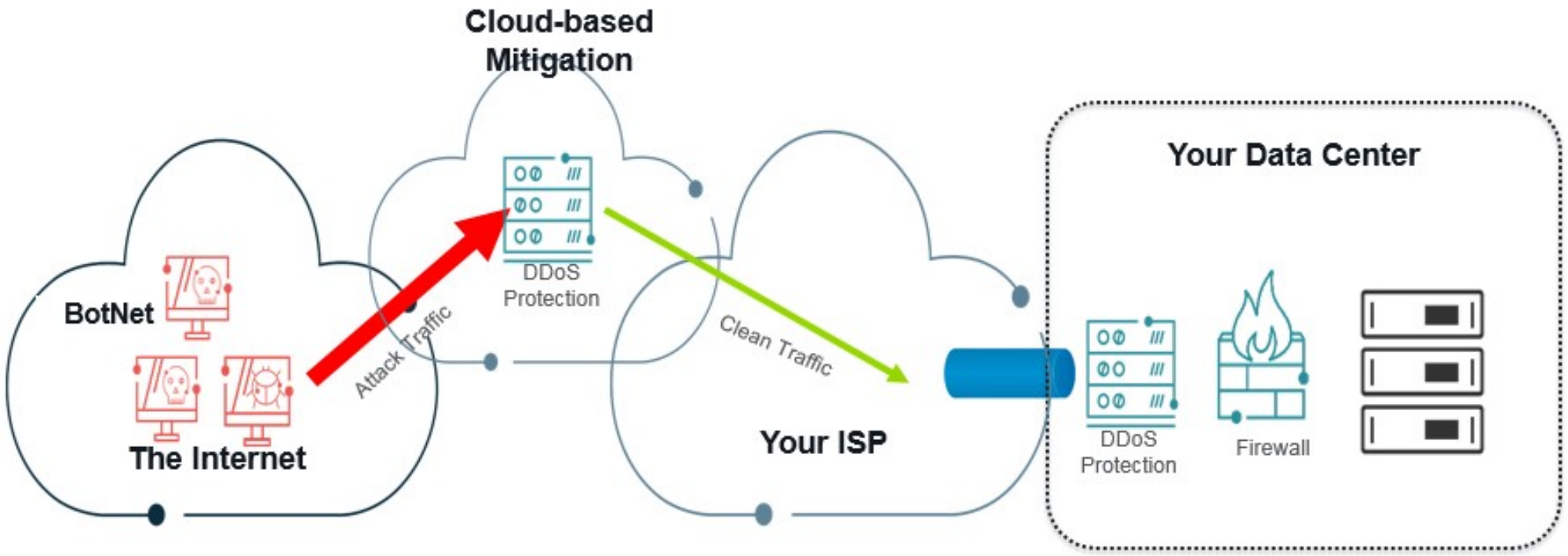
trends in DDoS attacks



Source: https://blogs.akamai.com/2020/07/large-complex-ddos-attacks-on-the-rise-in-2020.html



Cloud-based DDoS mitigation



- Route attack to cloud based scrubbing center.

Source: netscout.com

carpet-bombing attacks

- DDoS attacks on entire subnets instead of focusing on specific target IPs
- Detection systems usually focus on a single destination IP, not a subnet, often resulting in the attack not being detected until too late
- Example
  - SSDP Amplification misuse is set to trigger at 4 Mbps
  - A 40 Gbps attack distributed among 16384 addresses in a 14bit address block is 2.42 Mbps per address
  - Host-based detection will therefore not trigger
- Defense should consider the subnet-wide destinations

SSDP: Simple Service Discovery Protocol