Bot & DDoS Deep Dive – Part I

COMP90073
Security Analytics

Dr. Yi Han, CIS

Semester 2, 2021

Outline

- Botnet Deep Dive
- DDoS Deep Dive

Botnet Deep Dive

- How Big is the Botnet P
- Terminologies
- Botnet Architectures
- Botnet Lifecycle
- Botnet Propagation

How Big is the Botnet Problem

https://www.spamhaustech.com/threat-map/

How Big is the Botnet Problem

Gameover Zeus botnet infection map on July 25, 2014

Terminologies

- **Botnet**

  A network of compromised computers controlled by attackers from remote location via C&C (Command and Control) channels

- **Zombies / Drones / Bots**

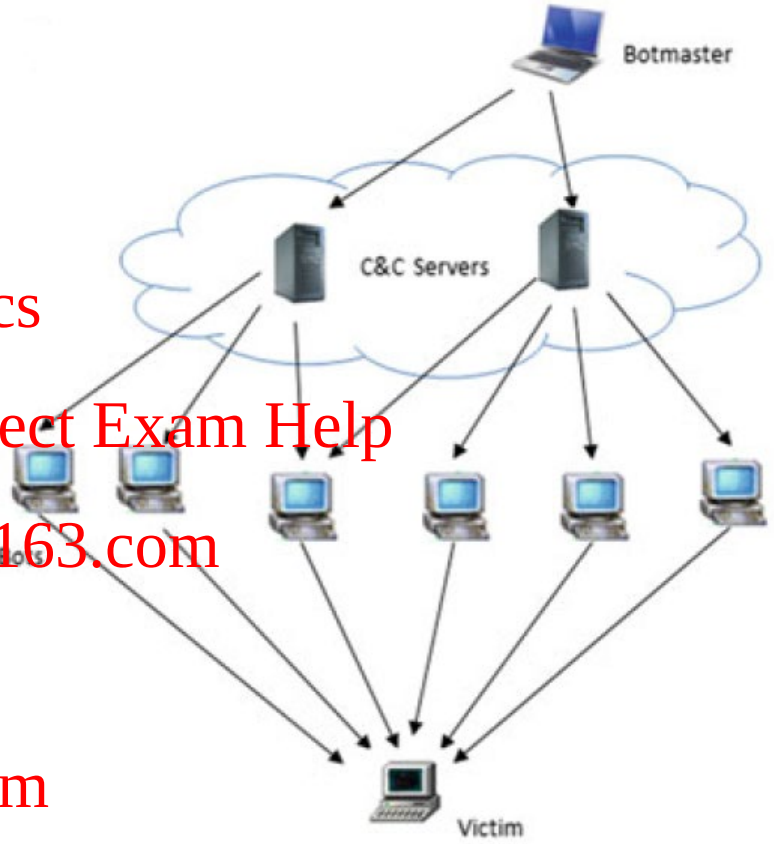
  Compromised computers

- **Botmaster**

  Attacker who is controlling the botnet

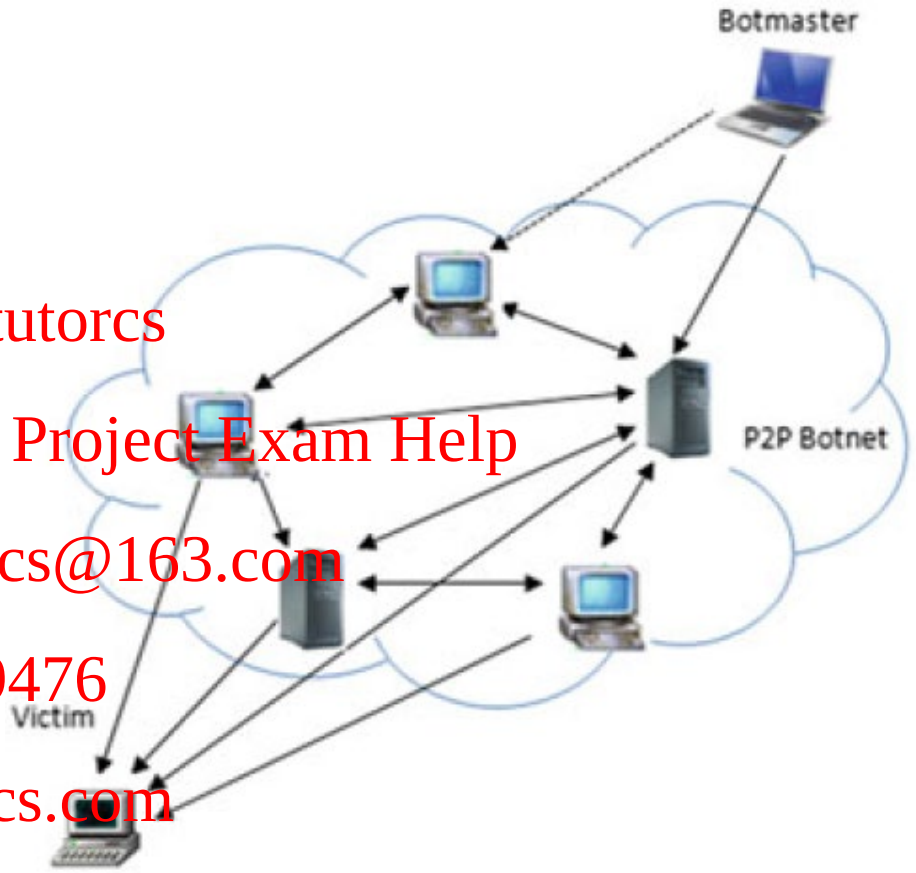
Botnet Architecture

- Topology: Centralized model
- Communication protocol: IRC (Internet Relay Chat) / HTTP
- Pros: Speed of control
- Cons: Single point of failure



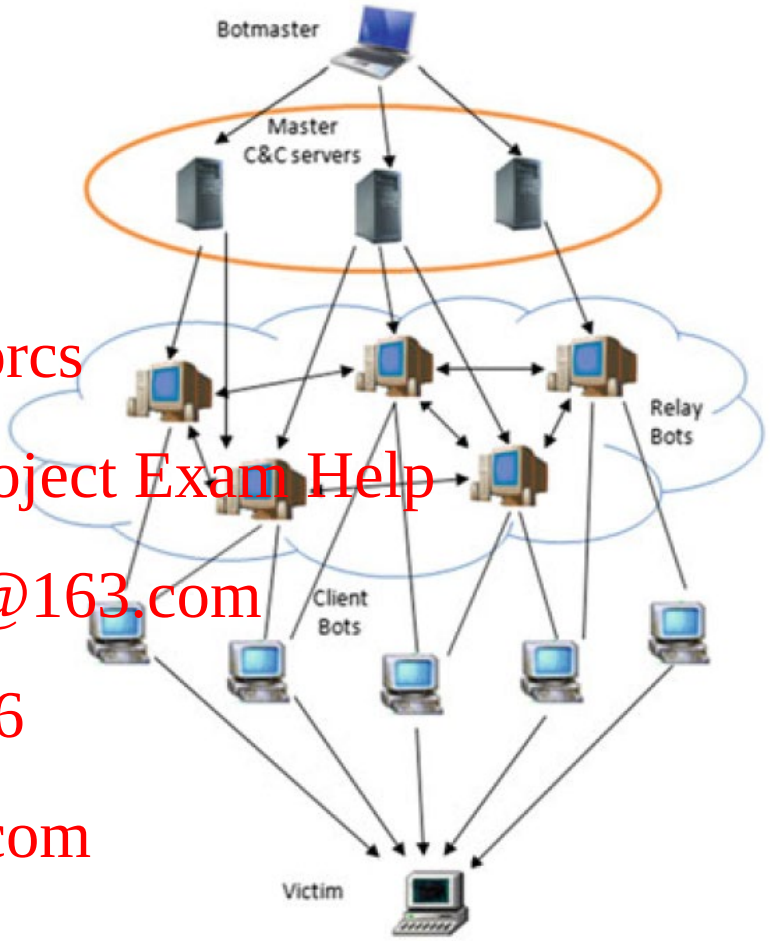
Botnet Architecture

- Topology: Decentra[illegible] model
- Communication protocol: P2P (Peer to Peer)
- Pros: No single point of failure
- Cons: Complicated network and non-efficient control



Botnet Architecture

- Topology: Hybrid
- Communication protocol: P2P (Peer to Peer)
- Pros: High resilient
- Cons: Command latency



Botnet Lifecycle

- **Recruitment**

  Infecting vulnerable con compromised websites, email attachment and removable media, a

- **Interaction**

  Membership registering & maintenance operations such as code update

- **Marketing**

  Advertising for profit or other reasons

- **Attack execution**

  Launching attacks such as DDoS, Spam, and etc.

Botnet Propagation

- **Push-based**

  Employ network scanning techniques to find the vulnerable hosts and infect them to turn into a bot

  e.g., Conficker and Sim

- **Pull-based**

  Botmasters compromise Web servers, upload the malicious codes, and lure users to download the malicious codes

  e.g., MegaD and Srizbi botnets

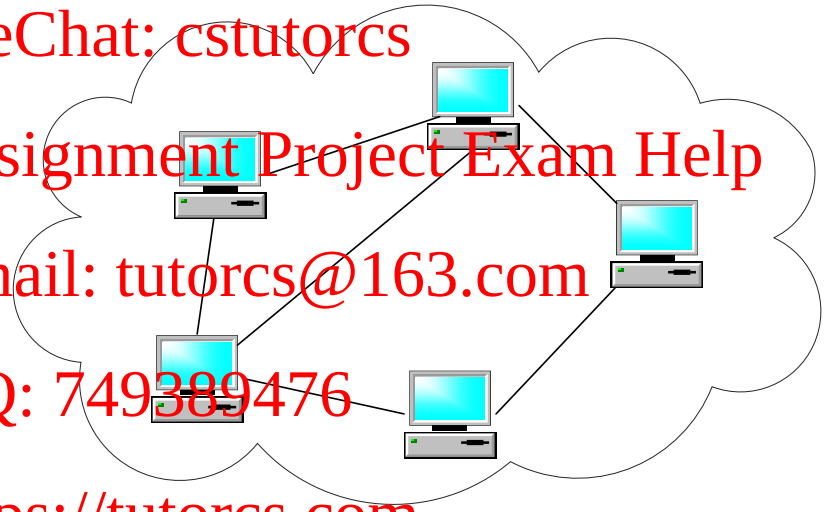
DDoS Deep Dive

- An early example: Morris worm
- How Big is the DDoS P
- Who is Behind the Attacks
- Common Types of DDoS Attacks
- Low-rate DoS attacks
- Trends

Morris worm

- An early example: Morris worm
  - November, 1988
  - Robert Morris, gradua[illegible]nt @Cornell

http://www.flickr.com/photos/intelfreepress/10477292993/



Morris worm

- An early example: Morris worm
  - November, 1988
  - Robert Morris, gradua[illegible]nt @Cornell

http://www.flickr.com/photos/intelfreepress/10477292993/

Morris worm

- An early example: Morris worm
  - November, 1988
  - Robert Morris, gradua[illegible]nt @Cornell

ltiple copies → roll a dice to decide which to kill
But 1/7 times the program would not terminate itself

http://www.flickr.com/photos/intelfreepress/10477292993/

Morris worm

- An early example: Morris worm
  - November, 1988
  - Robert Morris, gradua[illegible]nt @Cornell

http://www.flickr.com/photos/intelfreepress/10477292993/

How Big is the DDoS Problem

https://horizon.netscout.com/

Who is Behind the Attacks

- Cyber-criminal
  - Motivation: financia

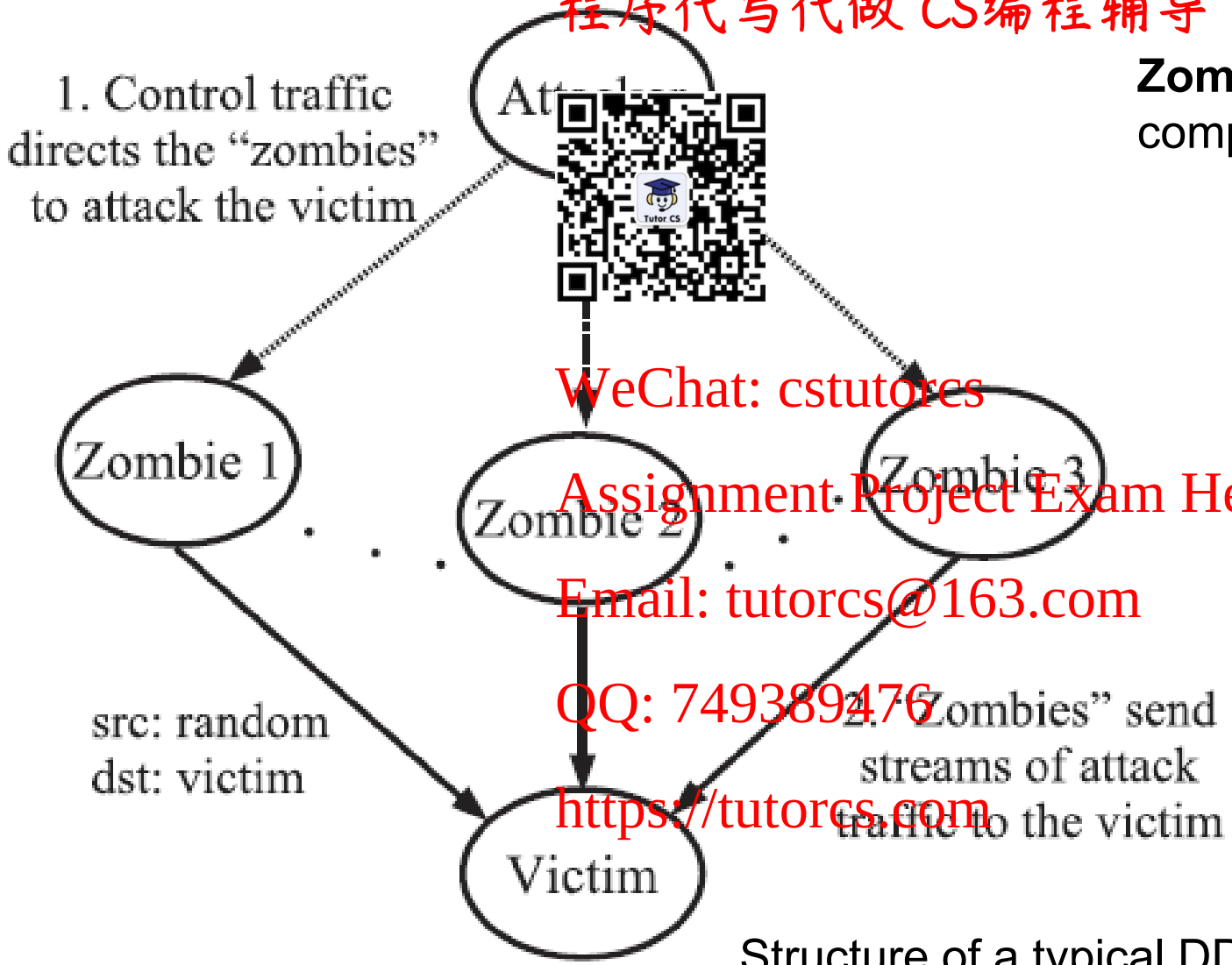
- Hacktivist
  - Motivation: political or ideologically driven

- Thrill & status seekers
  - Motivation: having done something disruptive

- Angry and disgruntled users
  - Motivation: seeking revenge

What DDoS Looks Like

Zombie: Internet connected compromised computers



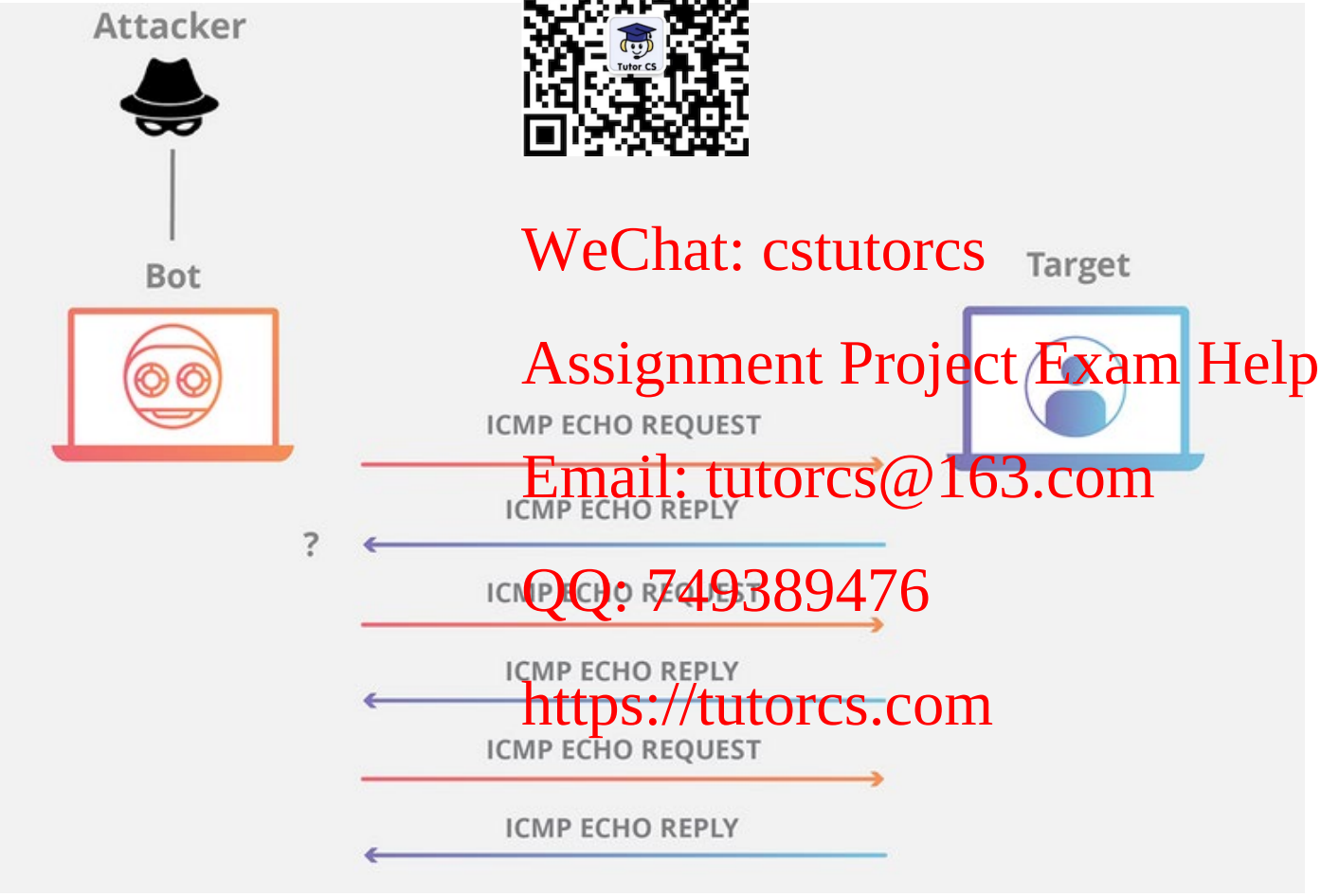
Structure of a typical DDoS attack (Source: [2])

Common Types of DDoS Attacks

- Volumetric Floods
  - Goal: to saturate th dth of the targeted site
  - Measurement: bits nd (bps)
- Network Protocol Attacks
  - Goal: to consumes actual server resources, or intermediate network devices such as firewalls and load balancers
  - Measurement: packets per second (pps)
- Application Layer Attacks
  - Goal: to crash the targeted web server
  - Measurement: requests per second (rps)

Volumetric Floods – Examples

- Ping (ICMP) flood - an attacker takes down a victim's computer by overwhelming it with IC[redacted]requests



Source: www.cloudflare.com

Volumetric Floods – Examples

- UDP flood – an attacker overwhelms random ports on the targeted host with IP packets containing datagrams

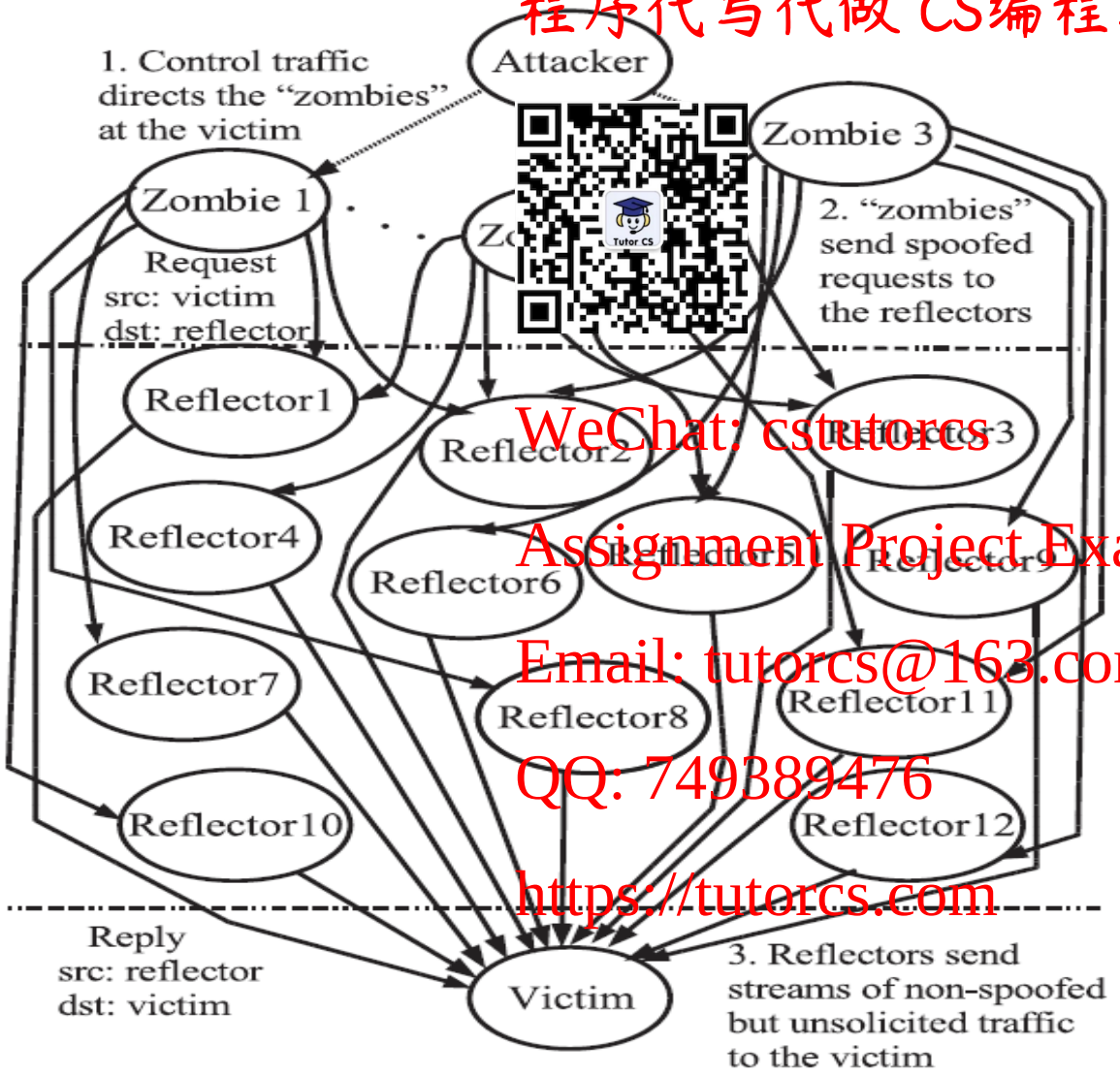
Source: www.cloudflare.com

Volumetric Floods – Examples

- Distributed reflector attacks: aims to obscure the sources of attack traffic by using third parties to launch attack traffic to the victim. These innocent third parties are also called *reflectors*

  - Stage 1, to compromise vulnerable systems that are available in the Internet and install attack tools in these compromised systems, i.e., turning the computers into "zombies"
  - Stage 2, the attacker instructs the "zombies" to send to the third parties spoofed traffic with the victim's IP address as the source IP address
  - Stage3, the third parties will then send the reply traffic to the victim, which constitutes a DDoS attack

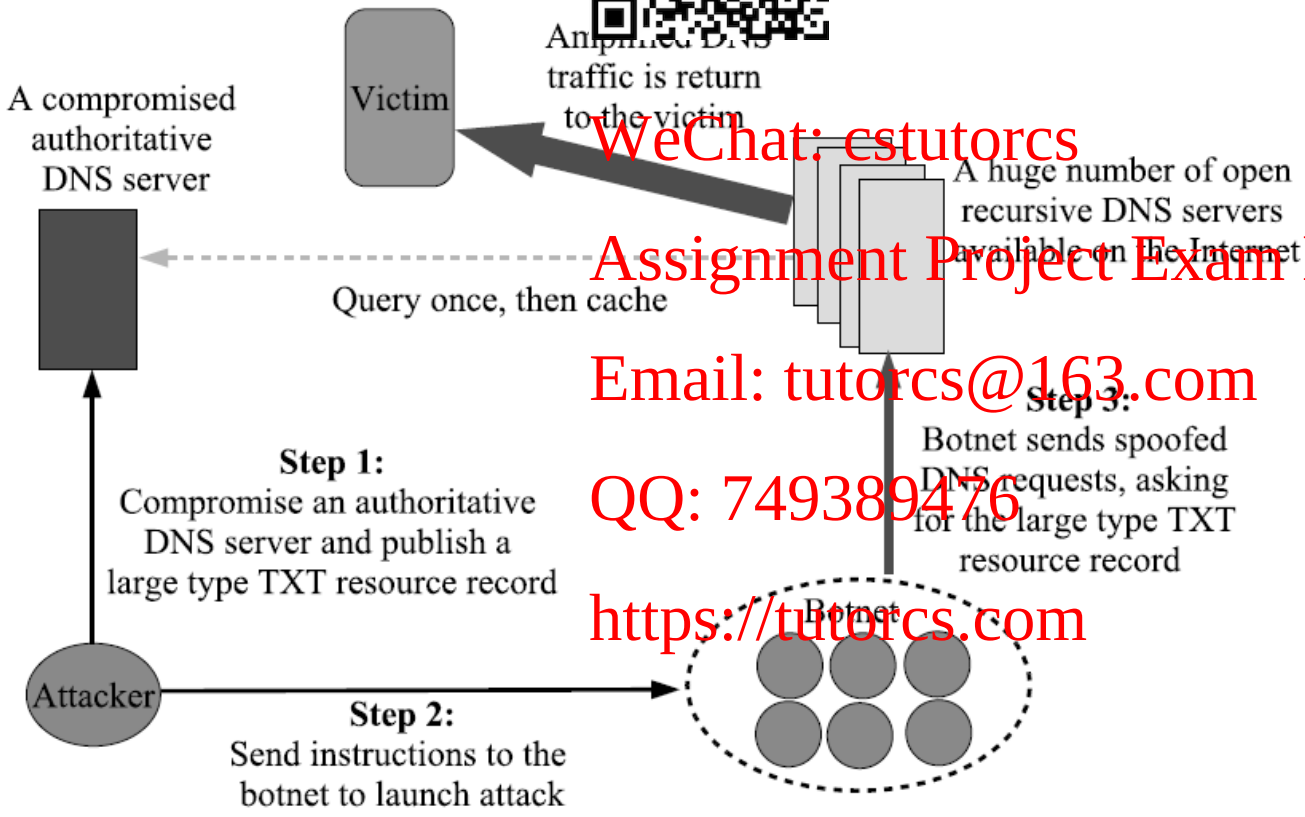
Volumetric Floods – Examples



Structure of a distributed reflector attacks (Source: [2])

Volumetric Floods – Examples

- DNS amplification attack, a reflection-based attack, an attacker leverages the functiona[illegible]en DNS resolvers in order to overwhelm a target with an amplifie[illegible]t of traffic



Steps of a DNS amplification attack (Source: [2])

Volumetric Floods – Examples

An example of DNS amplification attack (source: www.cloudflare.com)

Network Protocol Attacks – Examples

- SYN flood - an attack exploits part of the normal TCP three-way handshake to consume s on the targeted server and render it unresponsive

Progression of a SYN flood
(Source: www.imperva.com)

Network Protocol Attacks – Examples

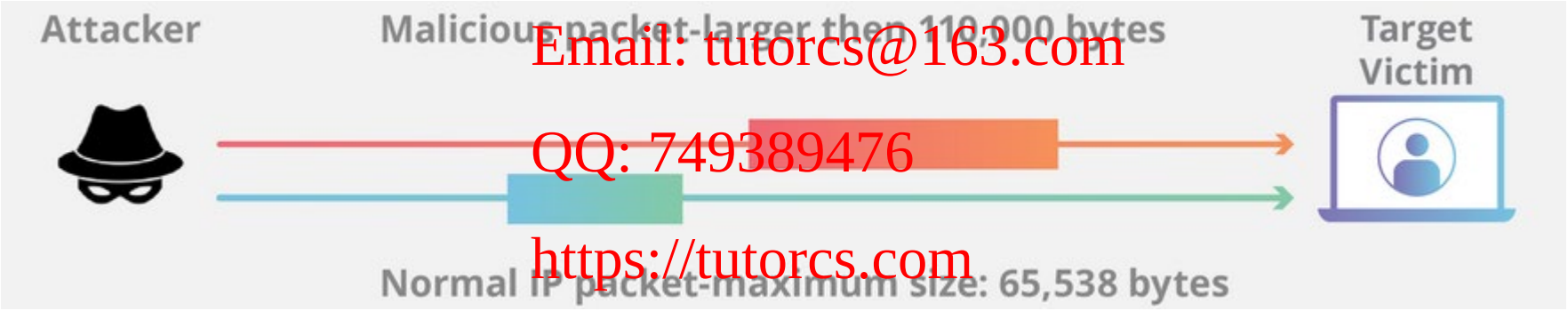
- SYN flood DoS attack e[illegible] client 10.131.87.112 is sending SYN packet continuously to [illegible].131.87.111 on port 80

No.	Time	Source	Destination	Protocol	Info
1	0.000000	10.131.87.112	10.131.87.111	TCP	14550 > http [SYN] Seq=0 Win=512 Len=0
2	0.000002	10.131.87.112	10.131.87.111	TCP	14551 > http [SYN] Seq=0 Win=512 Len=0
3	0.000003	10.131.87.112	10.131.87.111	TCP	14552 > http [SYN] Seq=0 Win=512 Len=0
4	0.000004	10.131.87.112	10.131.87.111	TCP	14553 > http [SYN] Seq=0 Win=512 Len=0
5	0.001894	10.131.87.112	10.131.87.111	TCP	14554 > http [SYN] Seq=0 Win=512 Len=0
6	0.001896	10.131.87.112	10.131.87.111	TCP	14555 > http [SYN] Seq=0 Win=512 Len=0
7	0.003709	10.131.87.112	10.131.87.111	TCP	14556 > http [SYN] Seq=0 Win=512 Len=0
8	0.004251	10.131.87.112	10.131.87.111	TCP	14557 > http [SYN] Seq=0 Win=512 Len=0
9	0.007647	10.131.87.112	10.131.87.111	TCP	14558 > http [SYN] Seq=0 Win=512 Len=0
10	0.007648	10.131.87.112	10.131.87.111	TCP	14559 > http [SYN] Seq=0 Win=512 Len=0

Wireshark screenshot (Source: vlab.amrita.edu)

Network Protocol Attacks – Examples

- Ping of death attack – a [illegible] attempts to crash, destabilize, or freeze the targeted computer or service by sending malformed or oversized packets using a simple ping command



Source: www.cloudflare.com

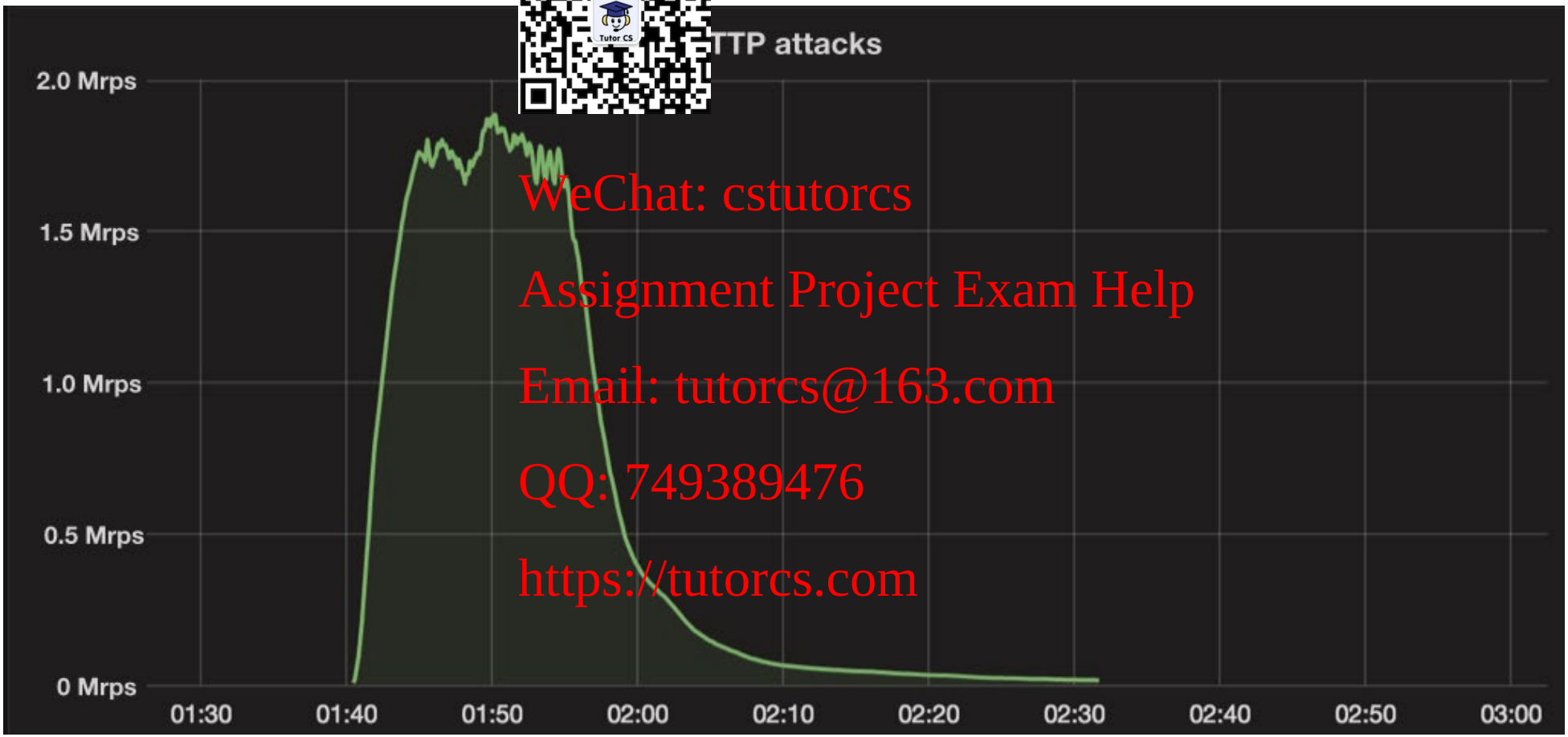
Application Layer Attacks – Examples

- HTTP flood attack - an attacker takes down a victim's web server by overwhelming it with HTTP requests

Source: www.cloudflare.com

Application Layer Attacks – Examples

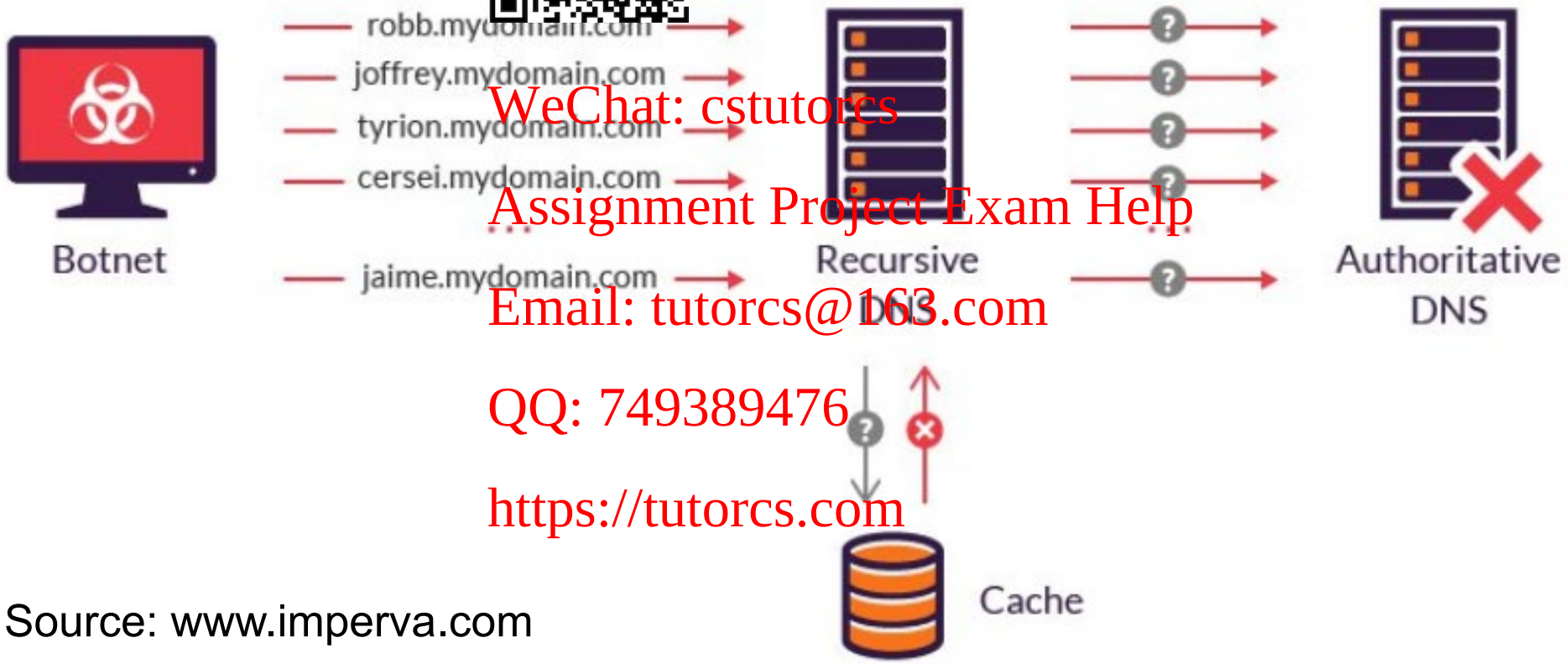
- Http flood example - a massive DDoS attacks coming from IoT cameras in 2016



Source: www.cloudflare.com

Application Layer Attacks – Examples

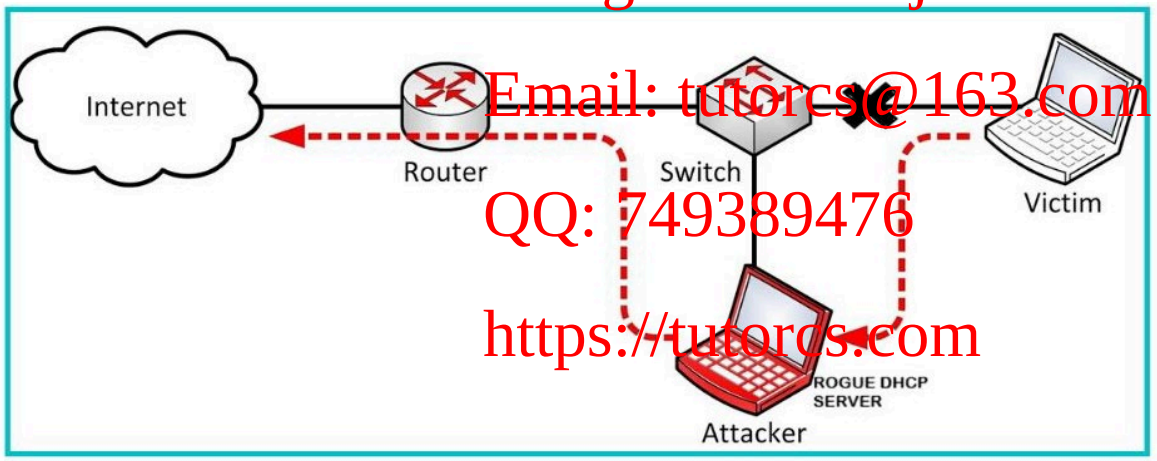
- DNS query flood – a symmetrical DDoS attack that attempts to exhaust server-side assets with [illegible] UDP requests, generated by scripts running on several com[illegible] botnet machines



Source: www.imperva.com

Application Layer Attacks – Examples

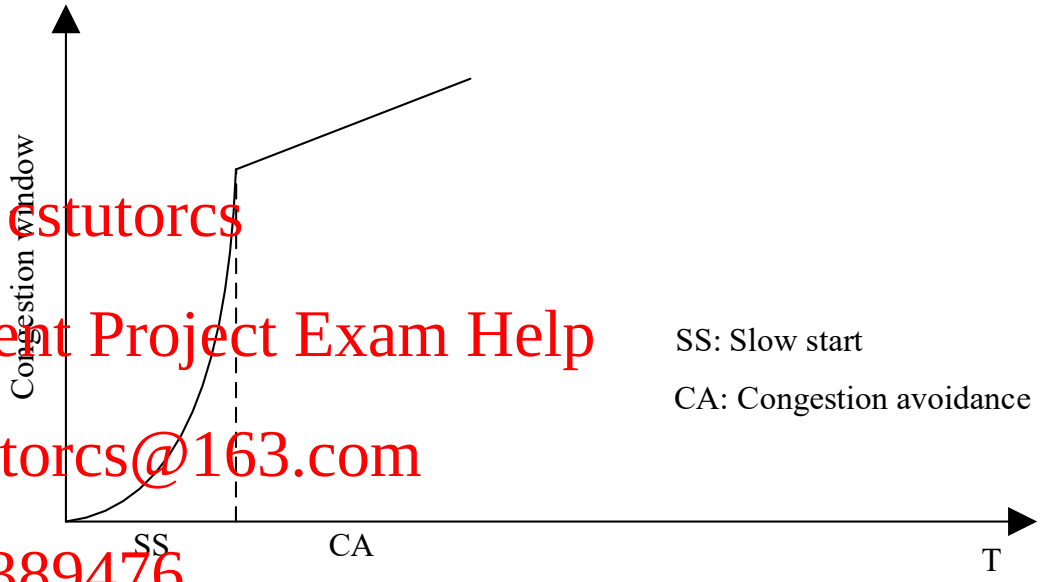
- DHCP-based DoS
  - DHCP starvation: the attacker floods the DHCP server by sending a large number of DHCP requests and uses all of the available IP addresses that the DHCP server can issue
  - Rogue DHCP server attack: the attacker creates a rogue DHCP server to offer IP addresses. The rogue server can intercept and disrupt the network access for all its clients, causing DoS.



https://info-savvy.com/rogue-dhcp-server-attack/

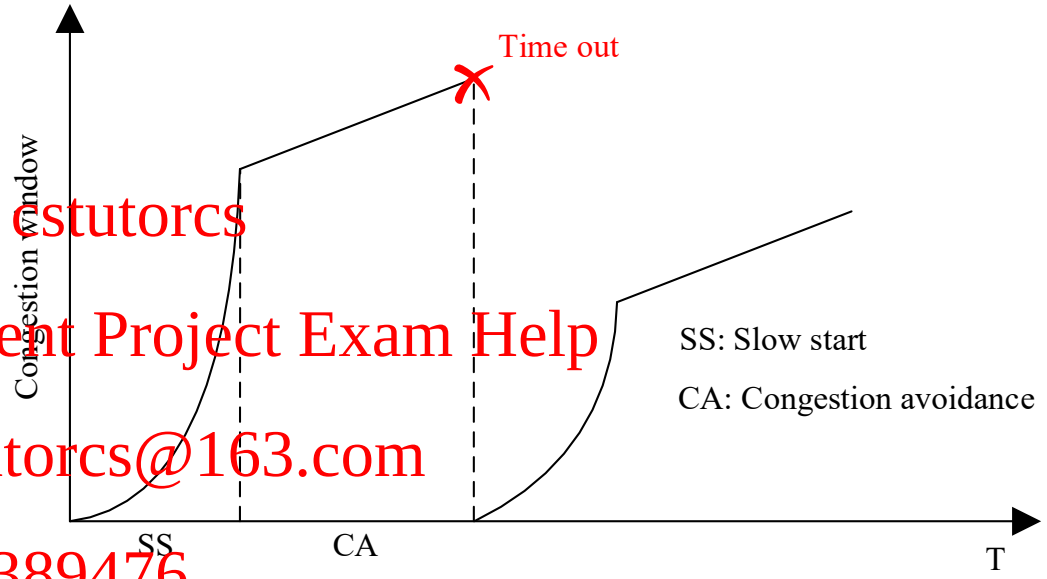
Low-rate DoS Attack

- Low-rate DoS attack
  - TCP congestion control mechanism
    - Slow start
    - Congestion avoidance
    - Fast retransmit
    - …



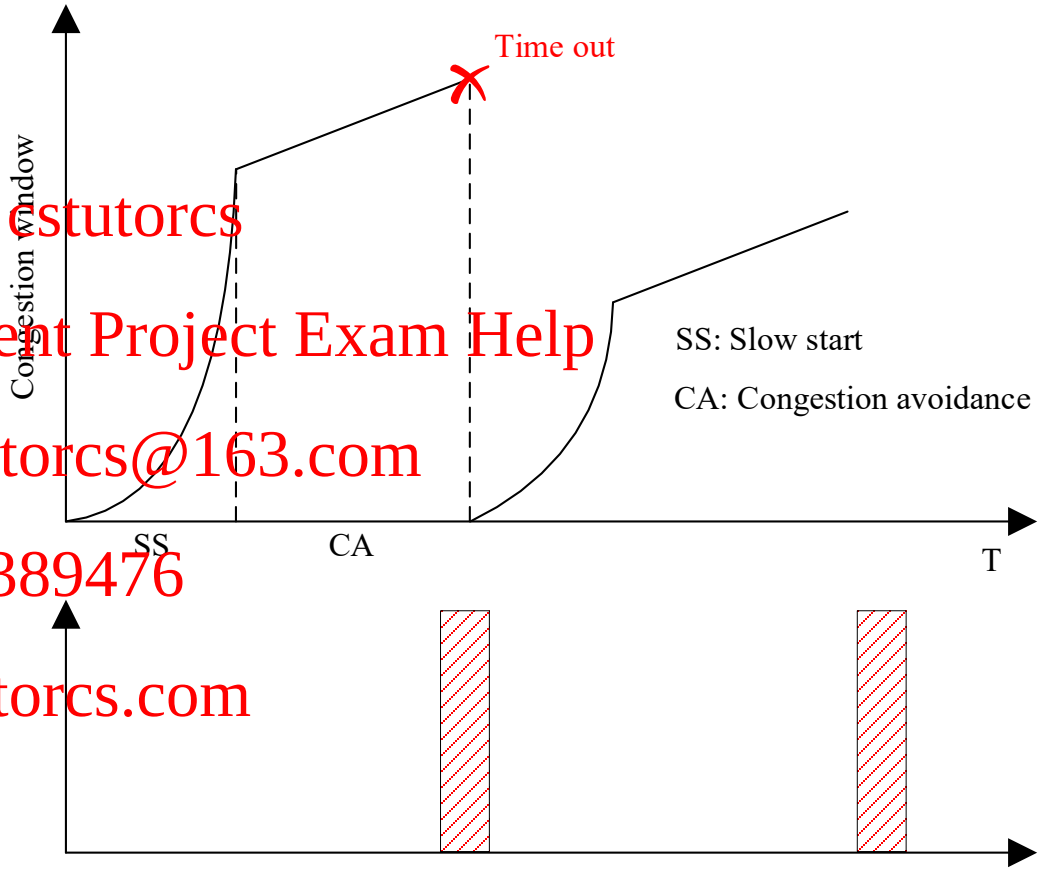
Low-rate DoS Attack

- Low-rate DoS attack
  - TCP congestion control mechanism
    - Slow start
    - Congestion avoidance
    - Fast retransmit
    - …



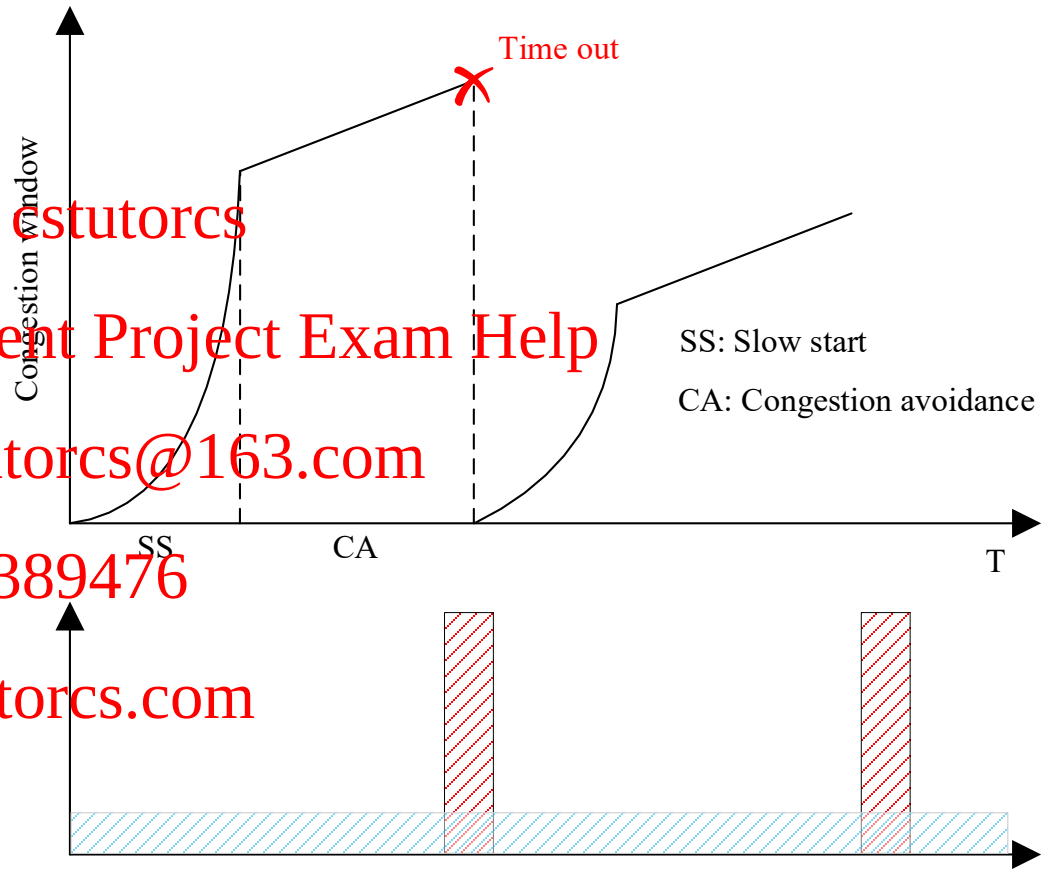
Low-rate DoS Attack

- Low-rate DoS attack
  - TCP congestion control mechanism
    - Slow start
    - Congestion avoidance
    - Fast retransmit
    - …



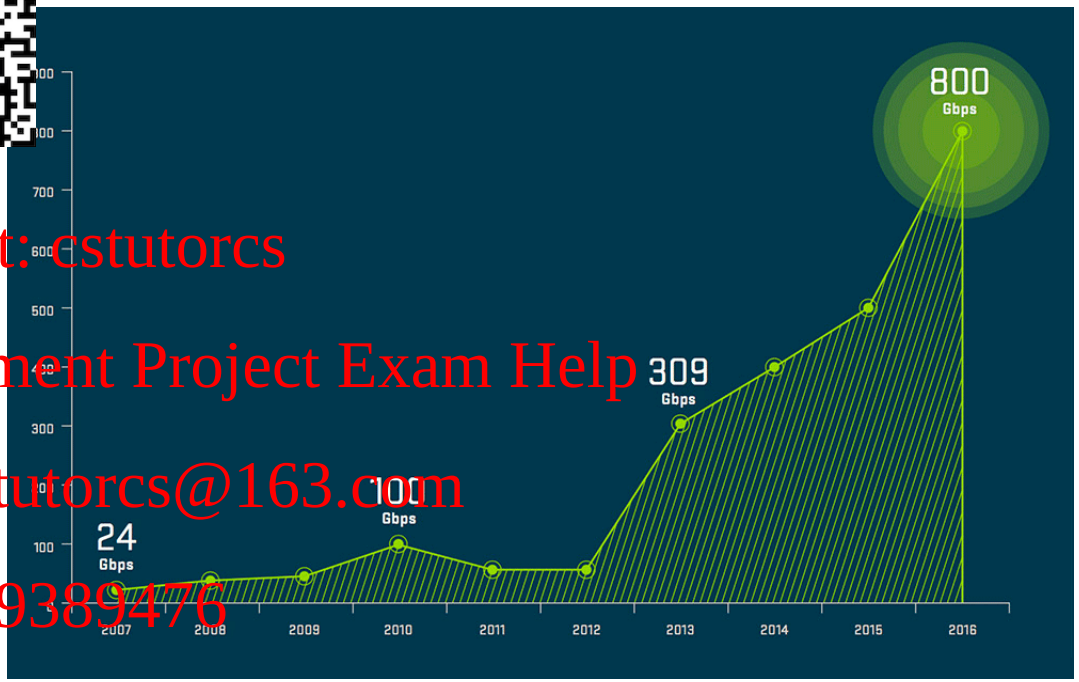
Low-rate DoS Attack

- Low-rate DoS attack
  - TCP congestion control mechanism
    - Slow start
    - Congestion avoidance
    - Fast retransmit
    - …



New Trends of DDoS Attack

- New trends of DDoS attack
  - Increase in quantity a ty
  - Application-layer atta
  - Internet-of-Things
  - 5G

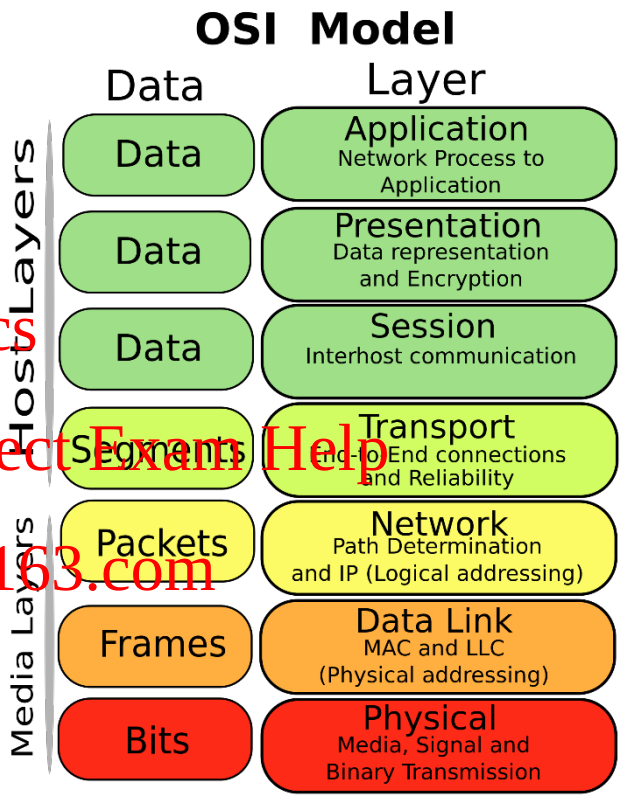


Trend in maximum DDoS attack rate

[Source: Arbor 12th Annual World Infrastructure Security Report, 2017]

New Trends of DDoS Attack

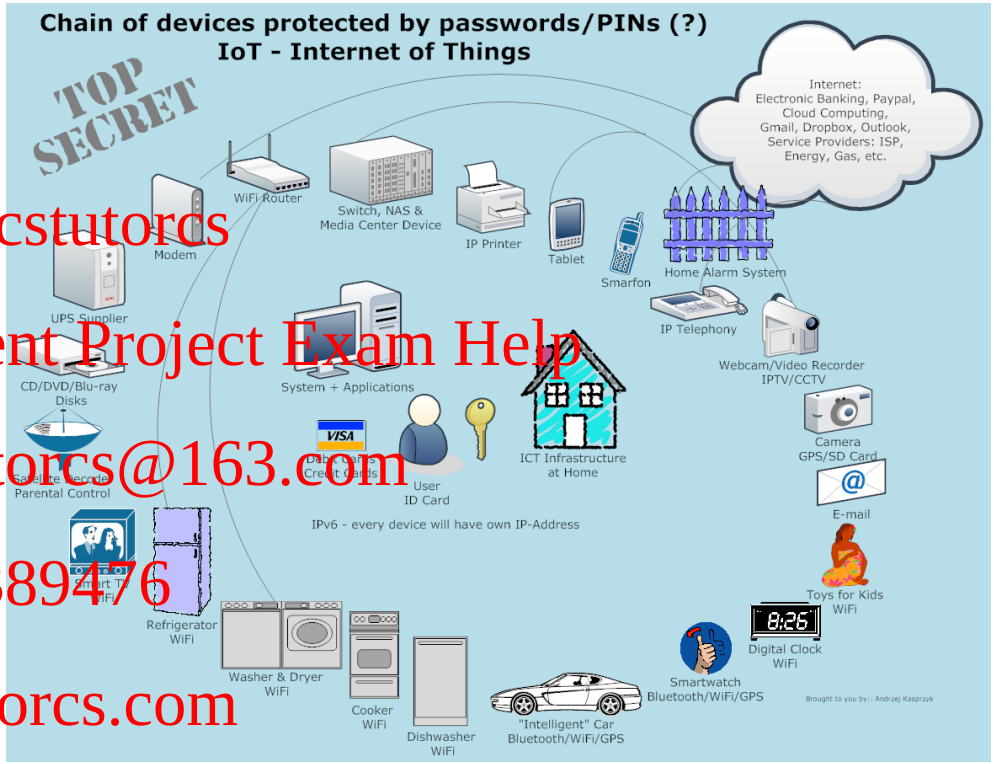
- New trends of DDoS attack
  - Increase in quantity a ty
  - Application-layer atta
  - Internet-of-Things
  - 5G



https://commons.wikimedia.org/wiki/File:Osi-model-jb.svg

New Trends of DDoS Attack

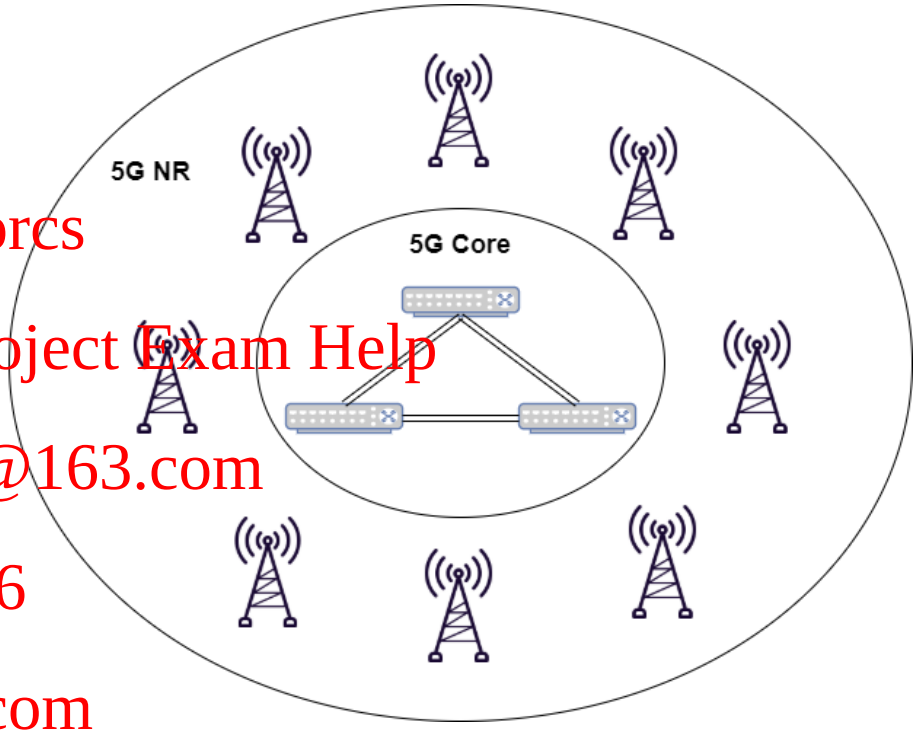
- New trends of DDoS attack
  - Increase in quantity a ty
  - Application-layer atta
  - Internet-of-Things
  - 5G



https://commons.wikimedia.org/wiki/File:Chain_of_home_devices_(including_IoT)_with_passwords_or_pin.png

New Trends of DDoS Attack

- New trends of DDoS attack
  - Increase in quantity a ty
  - Application-layer atta
  - Internet-of-Things
  - 5G



https://commons.wikimedia.org/wiki/File:5G_Architecture.png

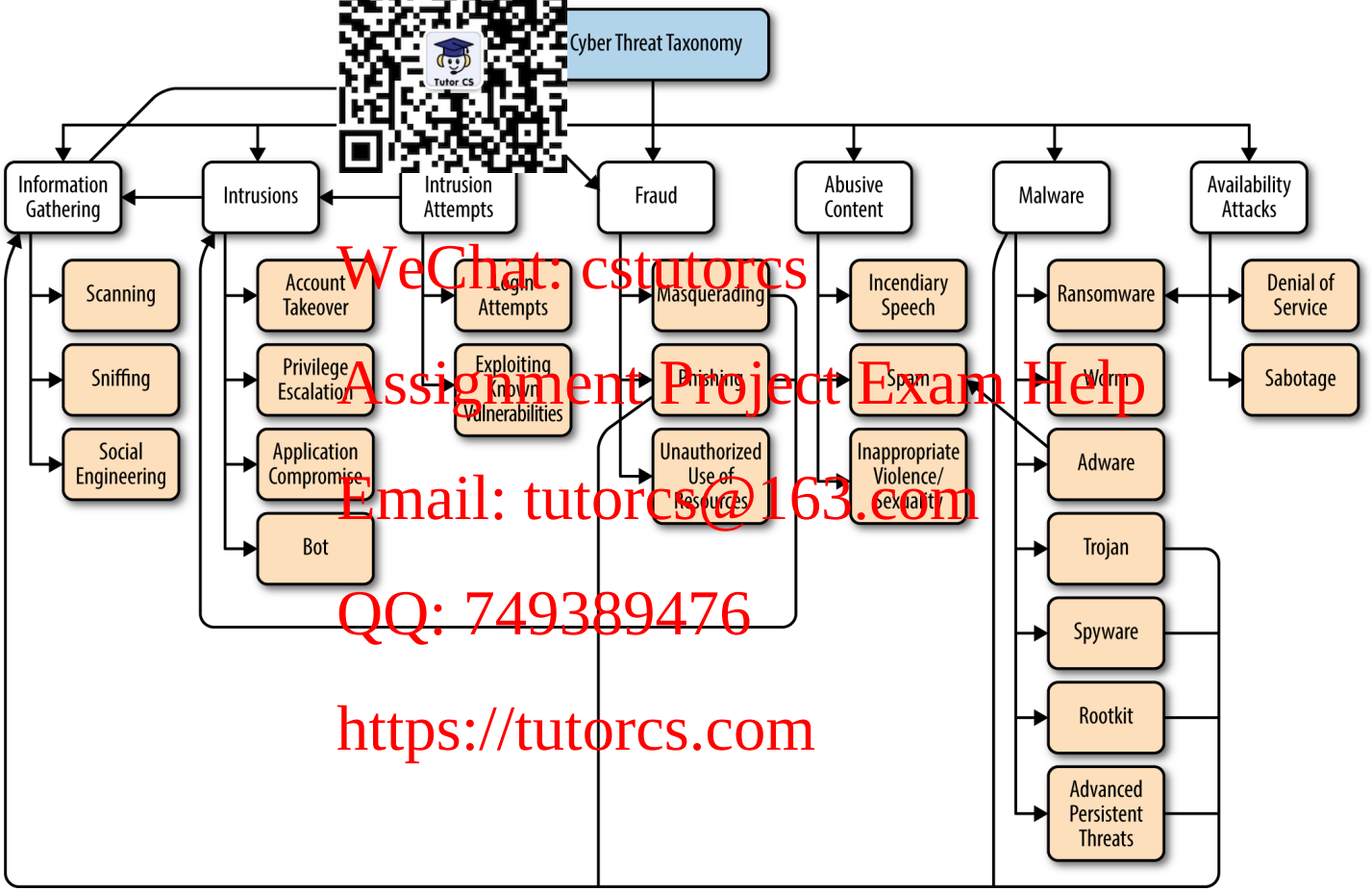
Summary

- Botnet Deep Dive
  - Botnet Architectures
    - Describe three di net topologies and their pros and cons
  - Botnet Lifecycle
    - Explain phases o cycle
  - Botnet Propagation
    - Compare the difference between push and pull based methods

- DDoS Deep Dive
  - Common Types of DDoS Attacks
    - Compare three types of DDoS attacks
    - Explain how the following DDoS attacks work, and how to detect
      - Ping flood, UDP flood, Distributed reflector attacks, DNS amplification attack
      - SYN flood
      - HTTP flood, DNS query flood, DHCP-based
  - Low-rate DoS Attacks

Summary

- Clarence Chio & David Freeman, 2018, Machine Learning and Security, Chapter 1, O'Reilly



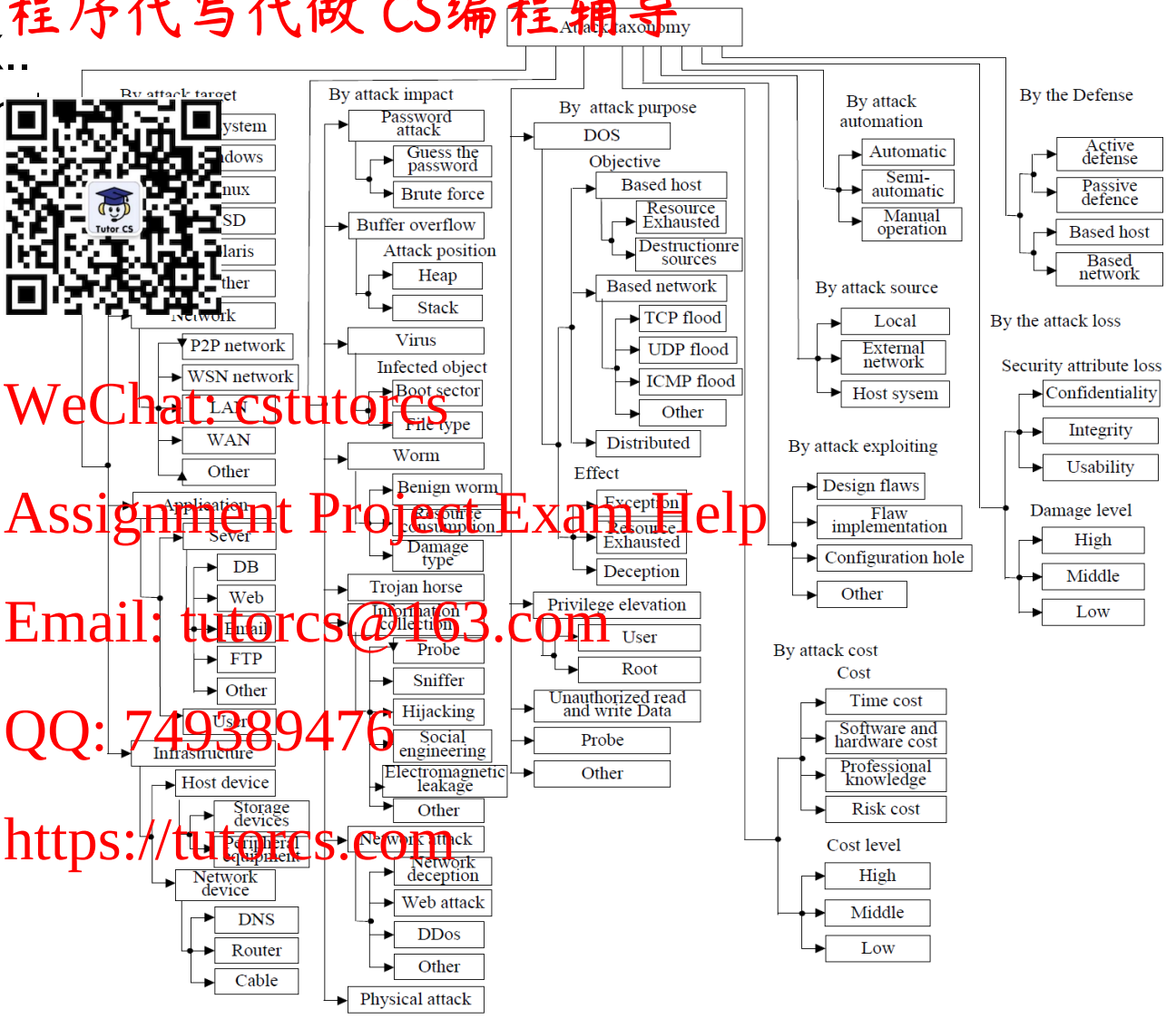
Summary

- Omar Santos, et al., 2017, CCNA Cyber Ops SECFND #210-250 Official Cert Guide (Cer[illegible]Guide), Chapter 13, Cisco Press

  - Reconnaissance At[illegible]
  - Social Engineering
  - Privilege Escalation Attacks
  - Backdoors
  - Code Execution
  - Man-in-the Middle Attacks
  - Denial-of-Service Attacks
  - Data Exfiltration
  - ARP Cache Poisoning
  - Spoofing Attacks
  - Route Manipulation Attacks
  - Password Attacks
  - Wireless Attacks

Summary

- Jiang, W., Tian, Z., Cui, X.. DMAT: A New Network ar Computer Attack Classification. Journal of Engineering Science and Technology Review, 6, 101-106, 2013



Summary

- Simmons, C.B., Ellis, C., Shiva, S., Dasgupta, D., Wu, Q. AVOIDIT: A Cyber Attack Taxonomy. CTIT technical reports series, 2009.

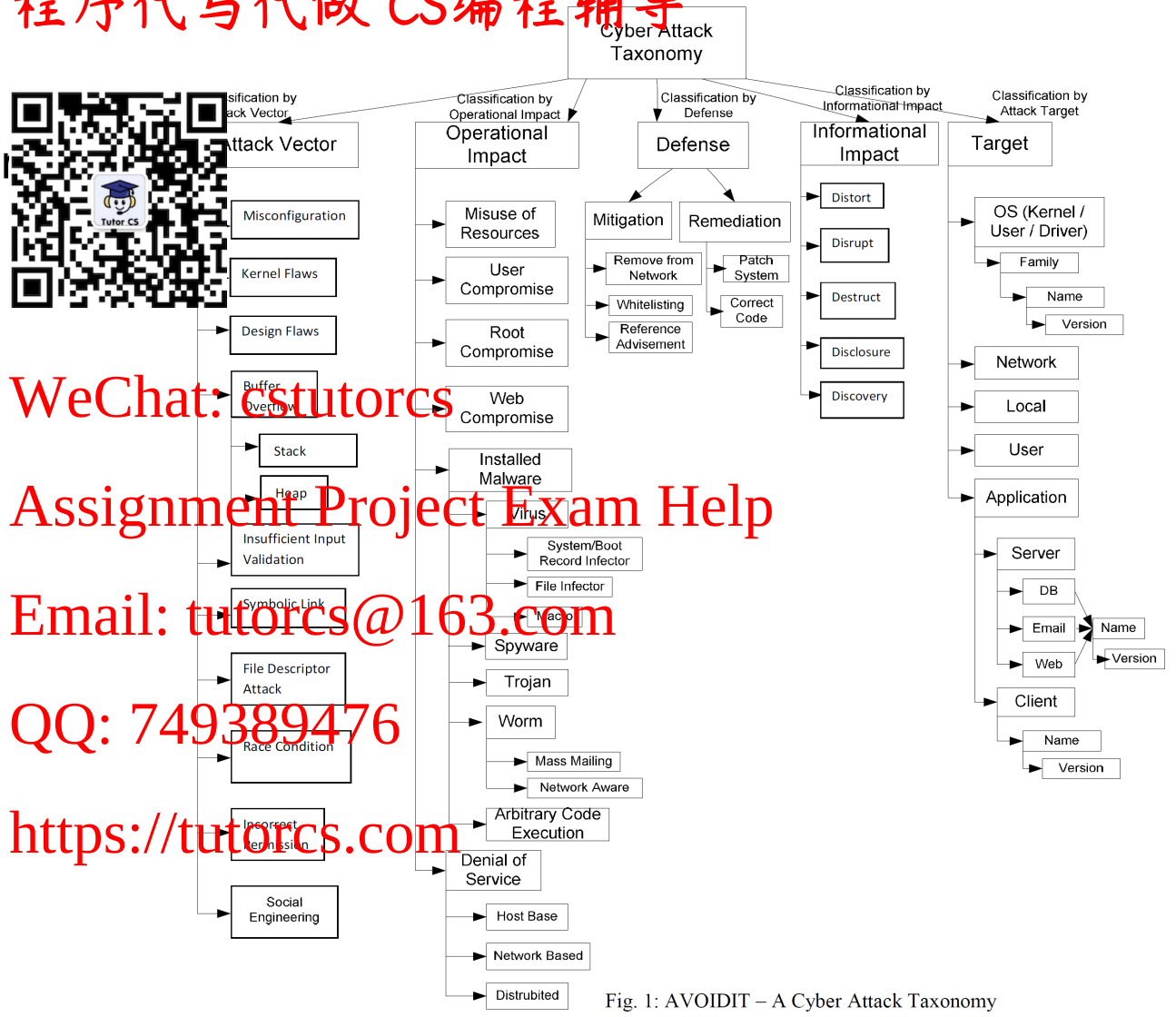


Fig. 1: AVOIDIT – A Cyber Attack Taxonomy

Reference

- [1] Eric Chou and Rich Groves, 2016, *Distributed Denial of Service*, O'Reilly Media, Inc.
- [2] Tao Peng, Chris Lec[illegible] Katagiri Ramamohanorao, *Survey of Network-Based Defens[illegible]nisms Countering the DoS and DDoS Problems*, ACM Computing Surveys