DDoS Trends

Soo Jung Bae, Michael Mierzwa, and Richmond Truong

Definition

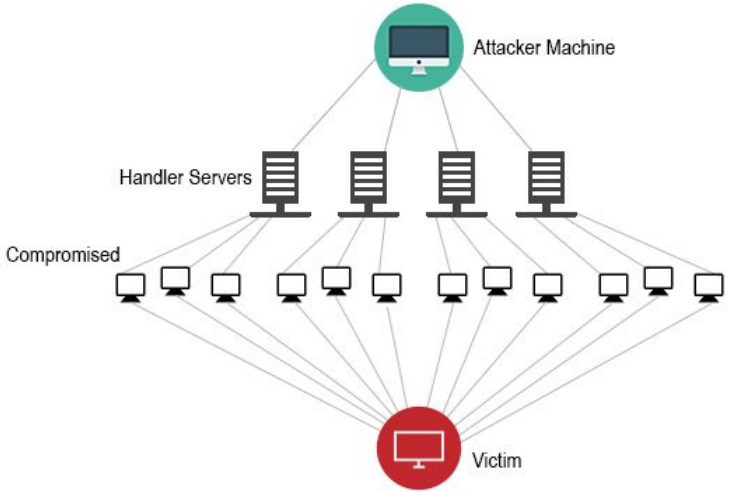
...

What is a DDoS attack?
What types of DDoS attacks are there?

What is a DDoS attack?

Distributed Denial of Service

An attempt to make an **online** service unavailable by **overwhelming** it with traffic from **multiple sources**



Reasons for DDoS attacks

What do attackers gain?
What is the purpose of the attack?

- Money
- Weapon
- Express anger/criticism
- Distraction from other attacks

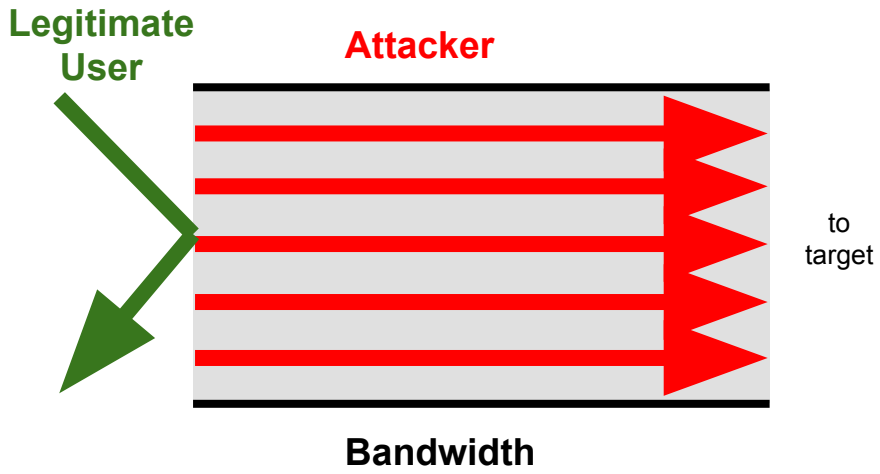
Types of DDoS attacks

•••

Which area of the network infrastructure is the attack focused on?

Volumetric Attacks

Overwhelms bandwidth



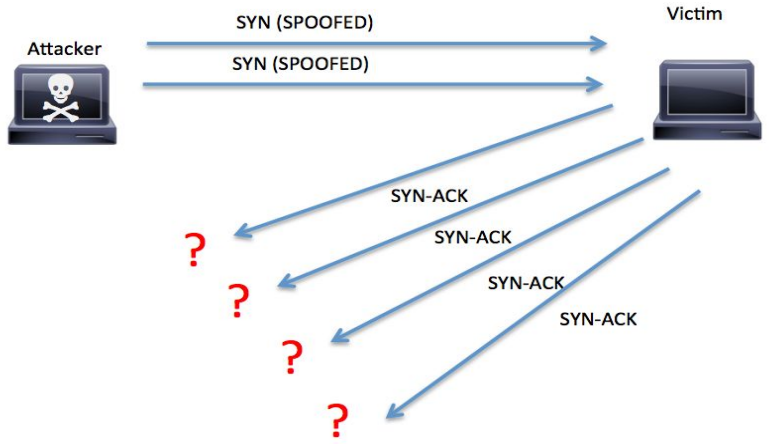
- **Unit:** Measured in bps
- **Examples:**
  - ICMP flood
  - UDP flood
  - Smurf flood

Protocol Attacks

Overwhelms resources

- Server
- Intermediate devices

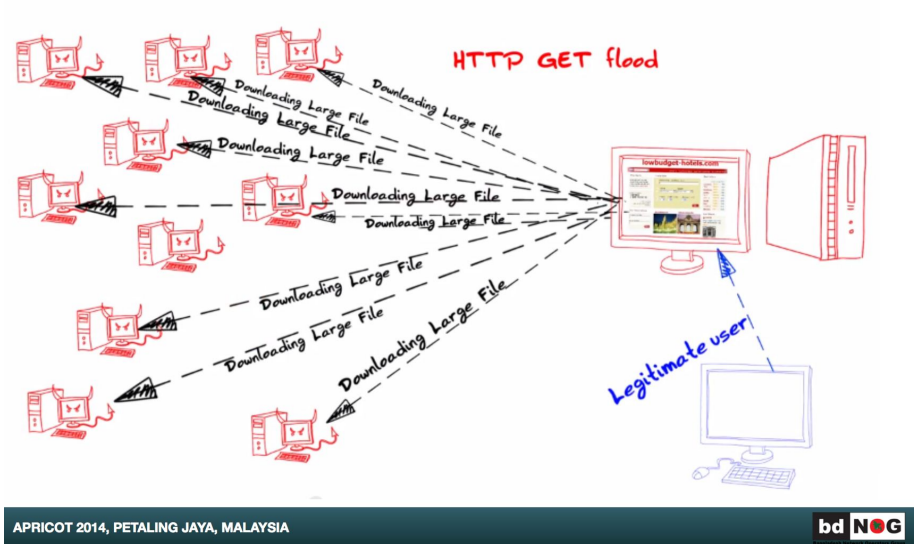
SYN flood attack:



- **Unit:** Measured in packets / sec
- **Examples:**
  - SYN flood
  - Pings of Death

Application Layer Attacks

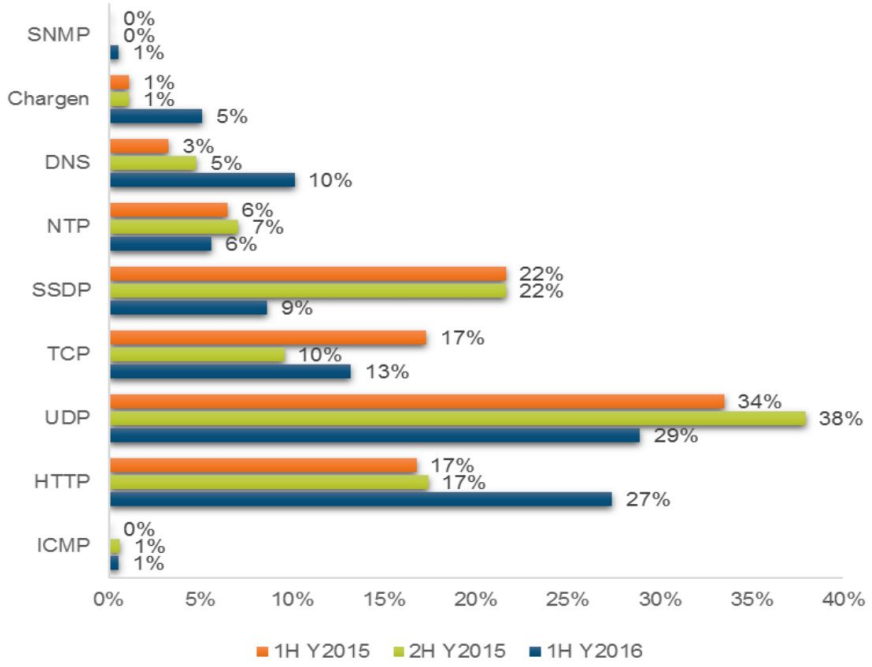
Monopolizes processes and transactions



- **Unit:** Measured in requests / sec
- **Examples:**
  - HTTP flood (GET/POST flood)
  - Slowloris

DDoS attack type analysis

- UDP flood occurs the most
  - Volumetric attack
- Rising trend of HTTP floods
  - Application layer attack



https://emea.cdnetworks.com/resources/cdnetworks_2016_1sthalf_ddosattacktrendreport_final.pdf

How an attack begins

...

What is needed for an attack?
How does someone start an attack?

How attacks happen

Attacks start with an IP

- A common way of obtaining someone's IP is Skype.
- Skype previously displayed your IP publicly.
- Even now there is such a thing as Skype Resolvers

When your IP is found

Large scale attacks.

- Purchasable DDoS attacks
- Cost for attack can be anywhere from 2-5 USD per hour
- Booter Shells

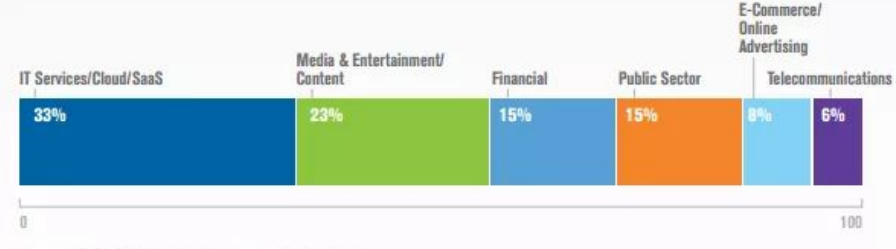


Figure 3: Q4 2014 Mitigations by Vertical

Internet of things

...

What is IOT?
How can it do a DDoS attack?

What is the internet of things?

Routers, baby monitors, CCTV
Printers, Smart TVs, Smart Watch,
Wifi repeaters, etc.

How it works

- 15% of routers are unsecure
- Default login information.
- Miria Malware

Attacks by the internet of things

Akamai

KrebsonSecurity
In-depth security news and investigation

- 620+ Gbps
- 100,00 logical attempts from 1,800 IP's

OVH.com

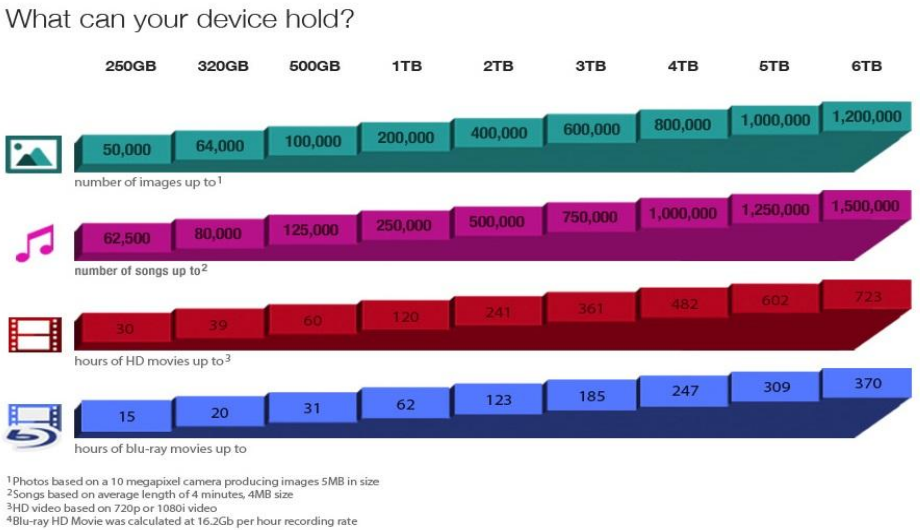
- 1 Tbps
- 145607 cameras/dvr

Biggest attack in recent history

- Took down: twitter, reddit, GitHub
- Attacked Dyn's DNS infrastructure
- 1.2 Tbs

How much bigger?

- 65 Gbs in 2012
- 18 times



Protection

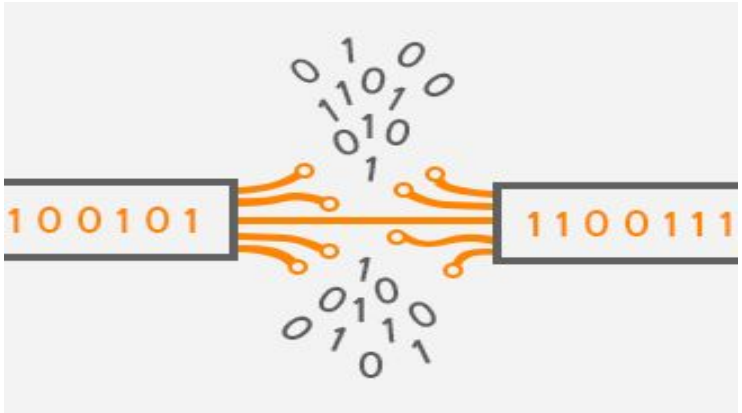
...

How do I protect myself?
How do businesses protect themselves?

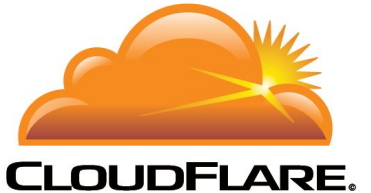
When you are being DDoSed

Try to ask your ISP

- The first fix is a change of IP.
- If it continues the request that your ISP drops the fake packets.
- Not all ISP's are willing to help.

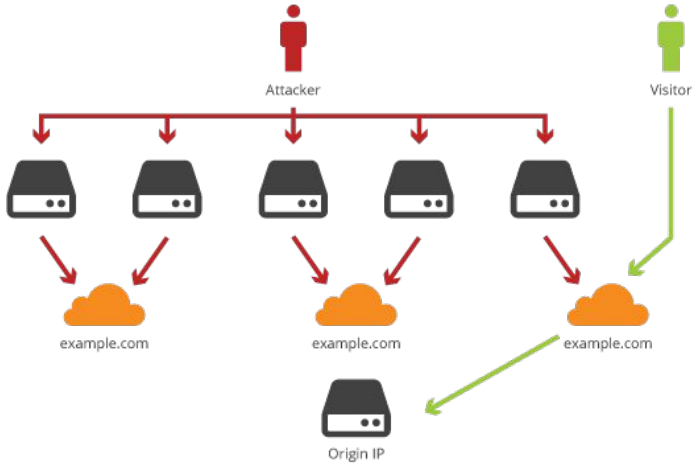


DDoS Protection & Mitigation Services



How DDoS mitigation works

- DNS redirecting
  - Over multiple countries
- Data Caching
  - Saves bandwidth
  - Faster load times



Conclusion

•••

We need to pay as much attention to the security of the IoT as we do to our websites or both will suffer.

FIN

Thanks for listening.

Review Questions

...

Q1: Which of these is NOT a property of application layer DDoS attacks?

A. It is measured in requests per second.

B. It is harder to detect compared to volumetric attacks.

C. It specifically targets the application layer of the OSI model.

D. It generates less traffic than protocol attacks.

E. It does not require a connection to be established prior to the attack.

Q2: Which of these is NOT a reason that DDoS is becoming more widely used?

A. Certain DDoS tools are designed with ease of use in mind.

B. Attacks can deal millions of dollars in damage

C. DDoS mitigation services are becoming weaker

D. DDoS attacks are taught in online forums

E. Internet of things allow for more attack opportunities.

Q3: What did the internet of things attack in its biggest attack?

A. No one knows.

B. DNS servers

C. Google

D. Microsoft

E. Routers

References

1. http://blogs.cisco.com/sp/latest-trends-on-ddos-attacks
2. http://www.cisco.com/c/en/us/about/security-center/guide-ddos-defense.html#35
3. https://www.tripwire.com/state-of-security/security-awareness/defending-your-network-against-ddos-attacks/
4. https://www.cyberscoop.com/mirai-botnet-for-sale-ddos-dark-web/
5. https://www.incapsula.com/ddos/ddos-attacks/
6. http://www.welivesecurity.com/2016/10/24/10-things-know-october-21-iot-ddos-attacks/
7. https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/q3-2016-state-of-the-internet-security-executive-summary.pdf
8. http://www.digitalattackmap.com/
9. https://securelist.com/analysis/quarterly-malware-reports/76464/kaspersky-ddos-intelligence-reportfor-q3-2016/
10. http://securityaffairs.co/wordpress/33916/cyber-crime/verisign-ddos-attacks-as-a-service.html
11. http://resources.infosecinstitute.com/dos-attacks-free-dos-attacking-tools/#gref
12. https://krebsonsecurity.com/2012/08/booter-shells-turn-web-sites-into-weapons/
13. https://blog.malwarebytes.com/threat-analysis/2016/02/gate-to-nuclear-ek-uses-fake-cloudflare-ddos-check/
14. https://blog.cloudflare.com/65gbps-ddos-no-problem/
15. http://www.esecurityplanet.com/network-security/5-tips-for-fighting-ddos-attacks.html
16. http://www.toptenreviews.com/business/internet/best-ddos-protection-services/
17. https://www.rt.com/viral/360989-ddos-attack-iot-hackers/