DDoS trends and defense issues

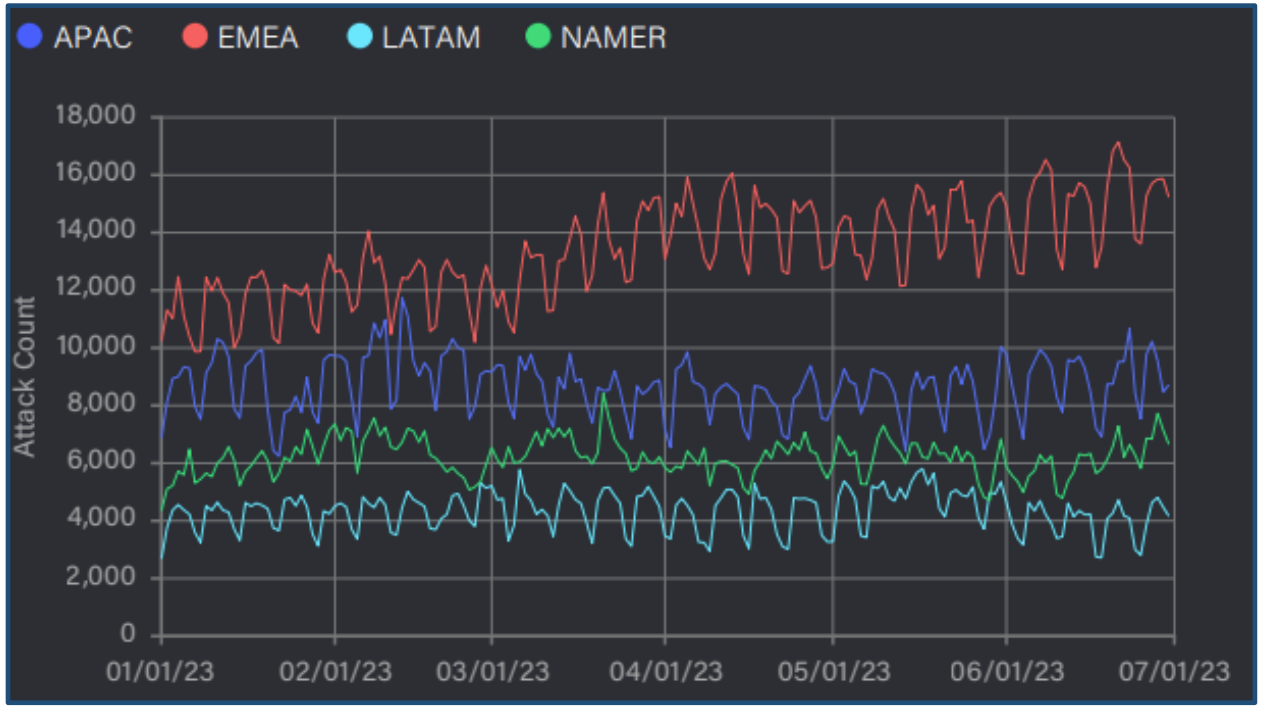
Linzhe Li

Beijing Zhongguancun Laboratory

March 17, 2024

DDoS Attack Trends and Problems

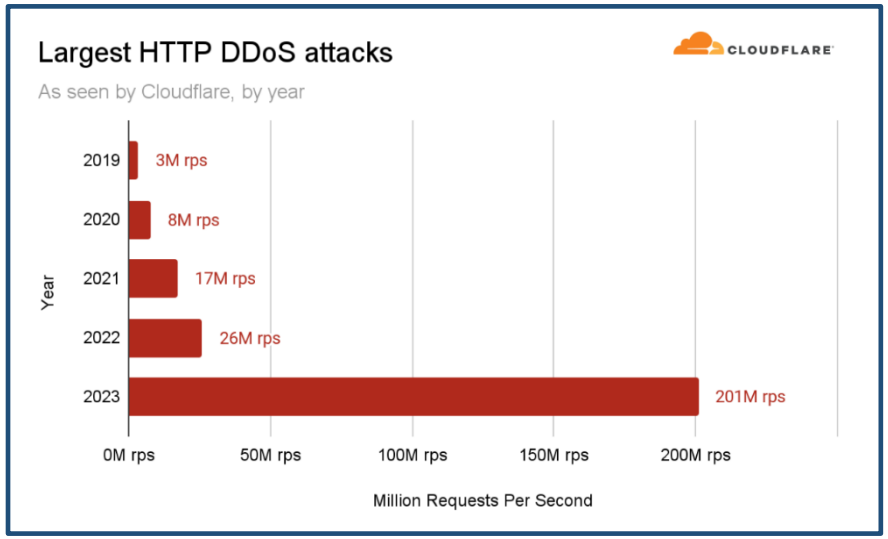
- **More frequent**
  - 7.9 million DDoS attacks happened in the first half year of 2023, 31% increase year over year.



DDoS Attack Trends and Problems

➢ Hyper-volumetric

- The largest attack in 2023 — 201M requests per second (rps), almost 8 times larger than 2022's.



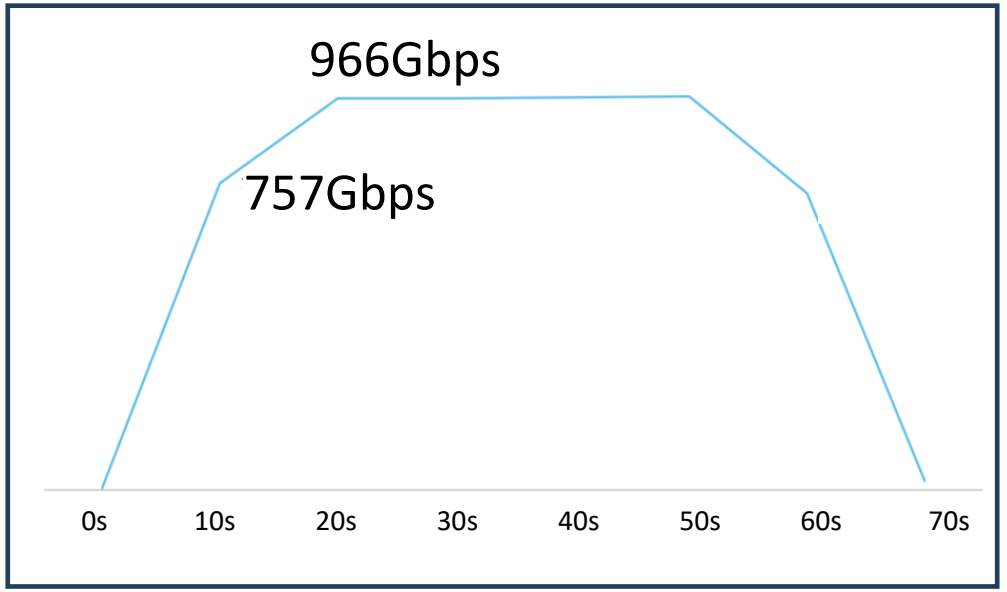
➢ High defense costs

- To counter randomly occurring DDoS attacks, long-term procurement and operation of large-scale DDoS defense resources come at a very high cost.

DDoS Attack Trends and Problems

➢ More Intelligent

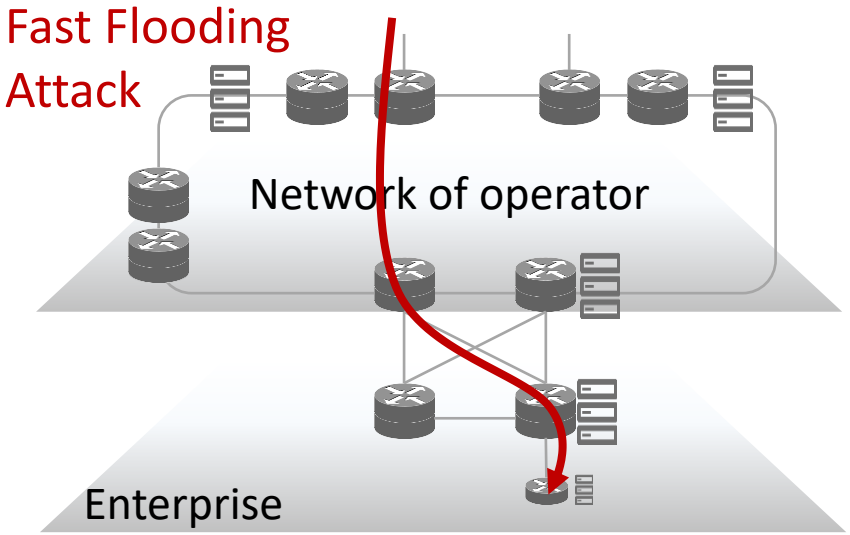
- 50% of DDoS use more than two vectors.
- "Fast Flooding" can suddenly spike to a high level for a short duration.
- New means using HTTP2.0, Coap, …



➢ Hard to detect

- For ISP, Sampling-based attack detection usually takes more than 1 minute.
- New types of attacks are emerging, and intelligent attacks occur more frequently, both are difficult to detect.

A Case



For operator：

- Detect attacks in minutes （sampling based）
- Have enough resources

For enterprise:

- Detect attacks in seconds
- Limited resources, can not mitigate Gbps-level attack traffic

The enterprise (DOTS Client)

1. Mitigation Request →

← 3. Collaborative Mitigation

The operator (DOTS Server)

2. Acknowledge the attack(in minutes) and develop mitigation strategies

Key elements of defense

Visibility → **scheduling strategy** → **Defense resources**

- Attack Features
- Network Telemetry Information
- DDoS Threat Intelligences

- Number and Types of Defense Devices
- Filtering Method

➢ Collaborative mitigation can help expand the visibility and increase available defense resources.

➢ DOTS(DDoS Open Threat Signaling) has defined the protocol and data model for collaborative mitigation during transfers, but there are still some shortcomings.

We are looking for cooperators!

We are building a collaborative defense architecture and signaling:

- Extended Yang data model of DDoS Open Threat Signaling
  - Alldispatch: IETF-Wide "Dispatch" Session
  - 8:30-11:30 Monday, Plaza Terrace Room
- SAV-based Anti-DDoS Architecture(SAV-D)

Please contact me: lilz@zgclab.edu.cn, Linzhe.

Thanks!