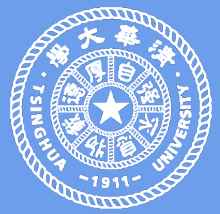
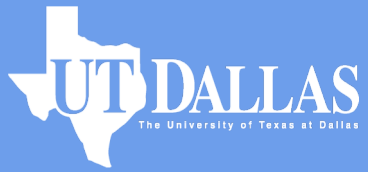
CDN Backfired: Amplification Attacks Based on HTTP Range Requests

Weizhong Li, Kaiwen Shen, Run Guo, Baojun Liu, Jia Zhang,
Haixin Duan, Shuang Hao, Xiarun Chen, Yao Wang (**Chaoyi Lu**)

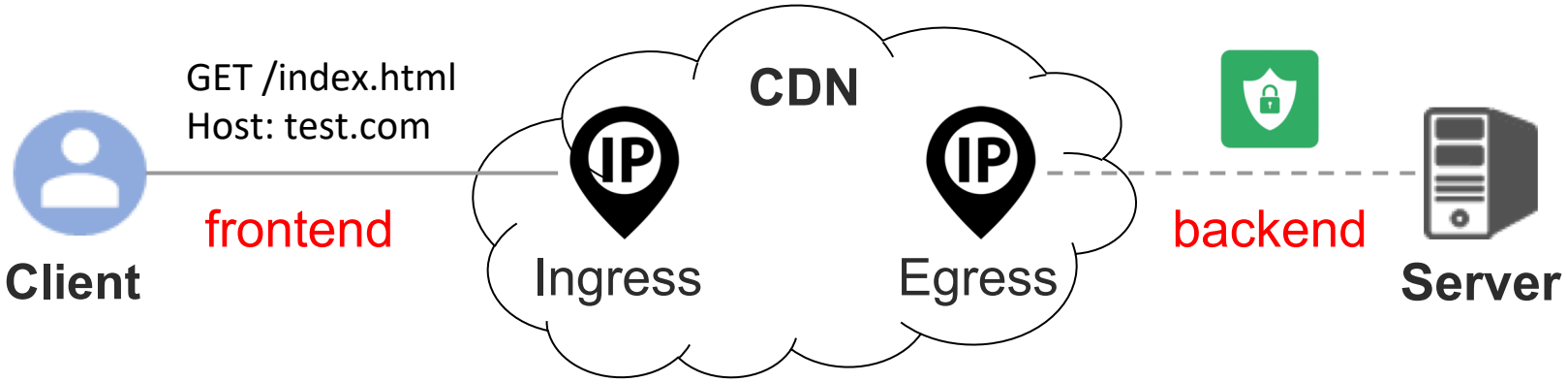




DSN 2020 - June 30, 2020

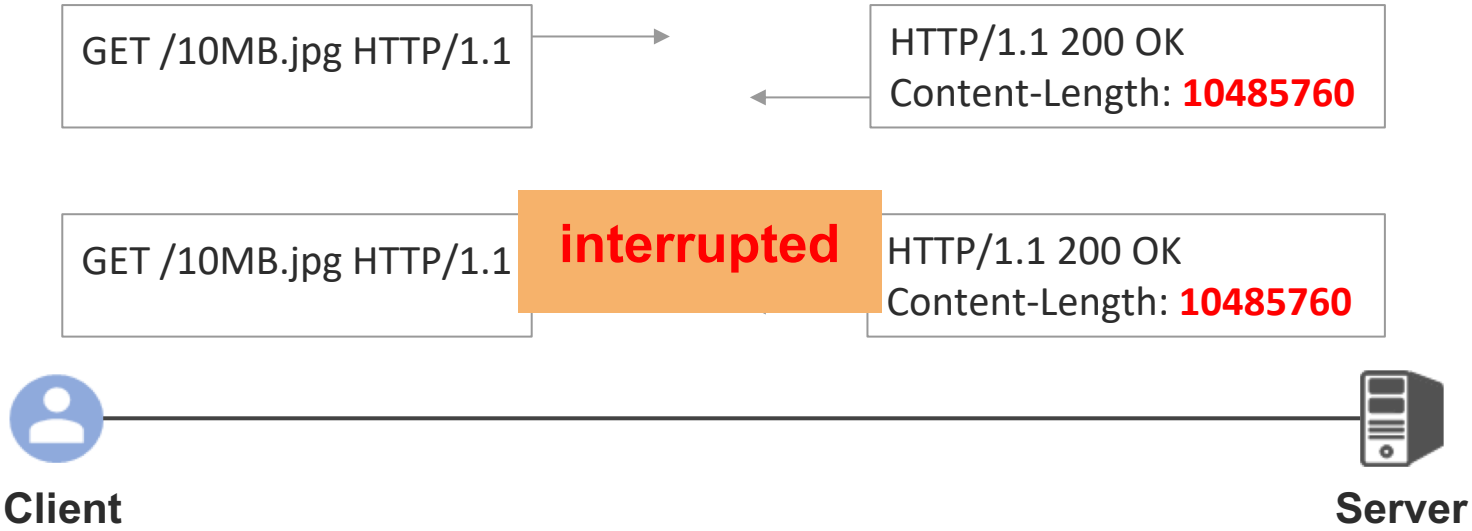
Content Delivery Network

- Infrastructure for performance and security.
  - Cache → Access acceleration.
  - DDoS defence.
- Adoption: 39.0% of Top 10K websites.



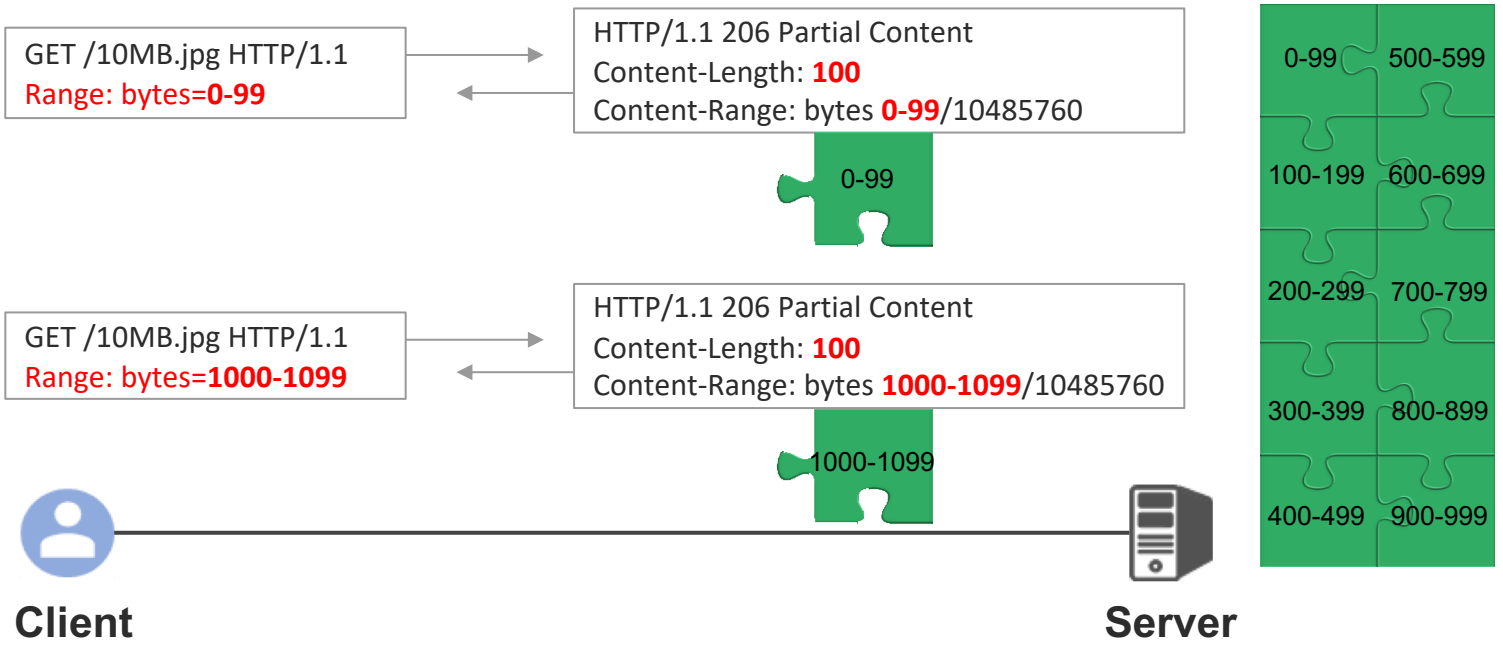
HTTP Range Request Mechanism

- HTTP is a stateless application protocol.
  - Interrupted transfer → Re-obtain the entire file.



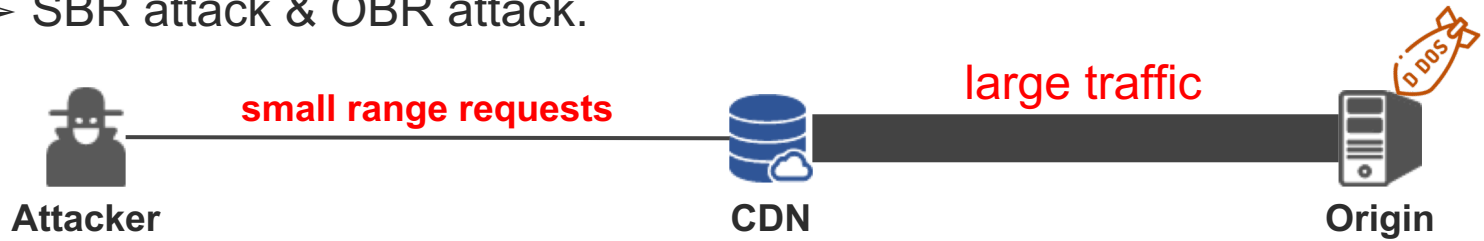
HTTP Range Request Mechanism

- To reduce unnecessary network transmission.
- Resuming from breakpoint & multi-thread transfers.



Our Work

- Range-based Amplification (**RangeAmp**) Attacks.
  - CDN turns into an amplifier when meeting range requests.
  - SBR attack & OBR attack.



(1) Small Byte Range (**SBR**) Attack

(2) Overlapping Byte Ranges (**OBR**) Attack

Measurement and Evaluation in the Wild

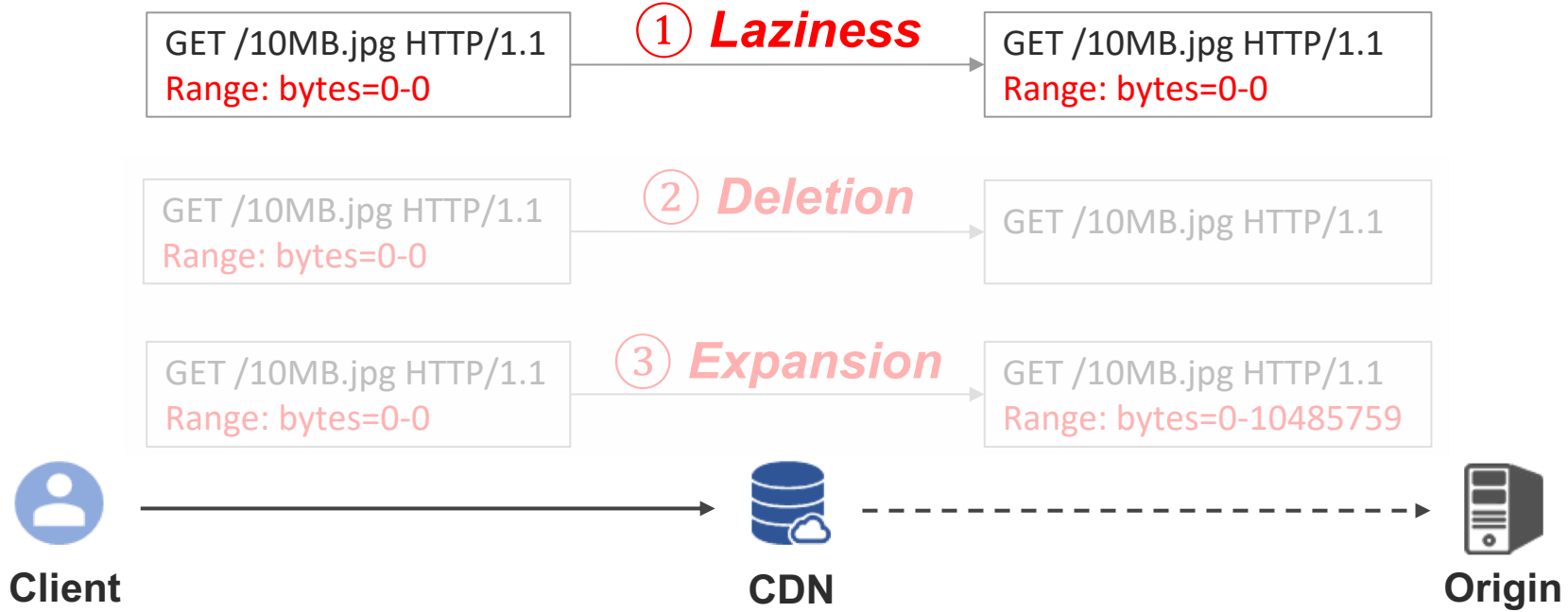
- **13 popular CDN vendors** we tested were vulnerable.
- The amplification factor far exceeds most traditional attack methods.

Attack-1

Small Byte Range (SBR) Attack

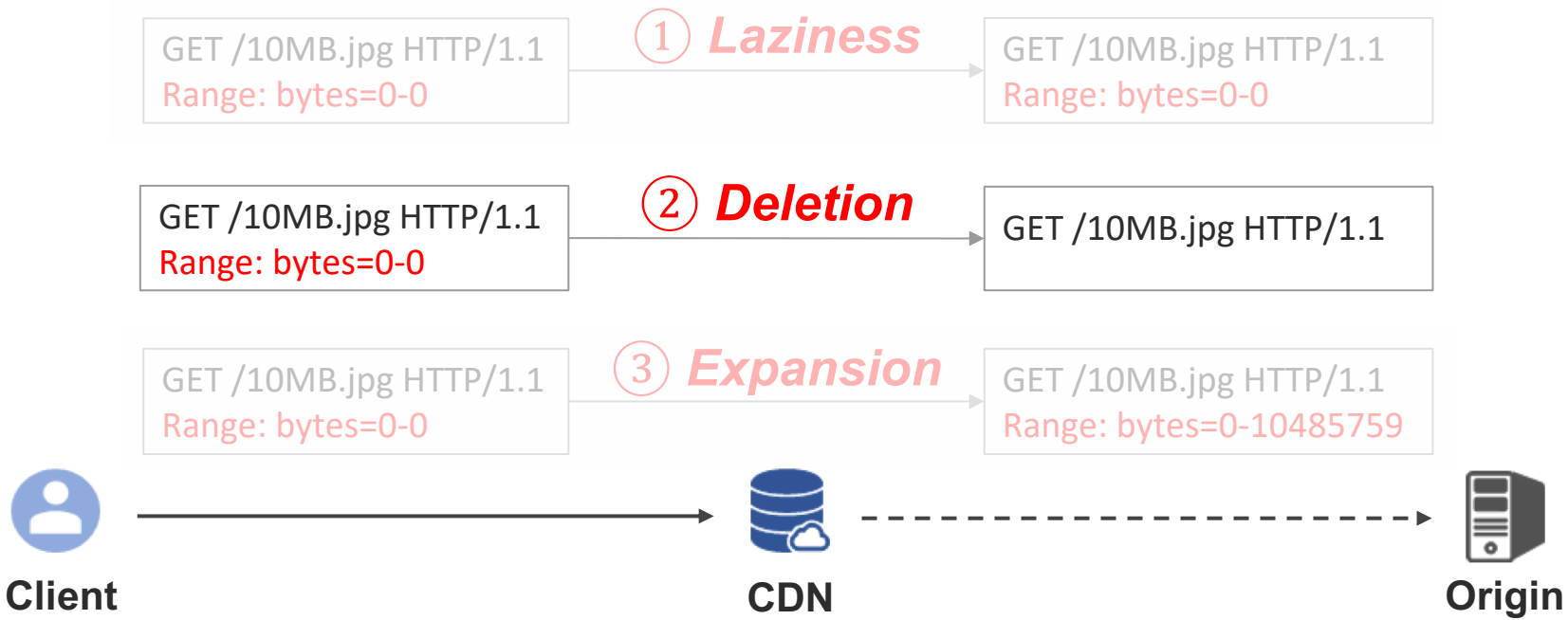
CDN's Range Forwarding Policies

- Different policies for malformed Range header.
  - ***Laziness***, *Deletion*, *Expansion*.



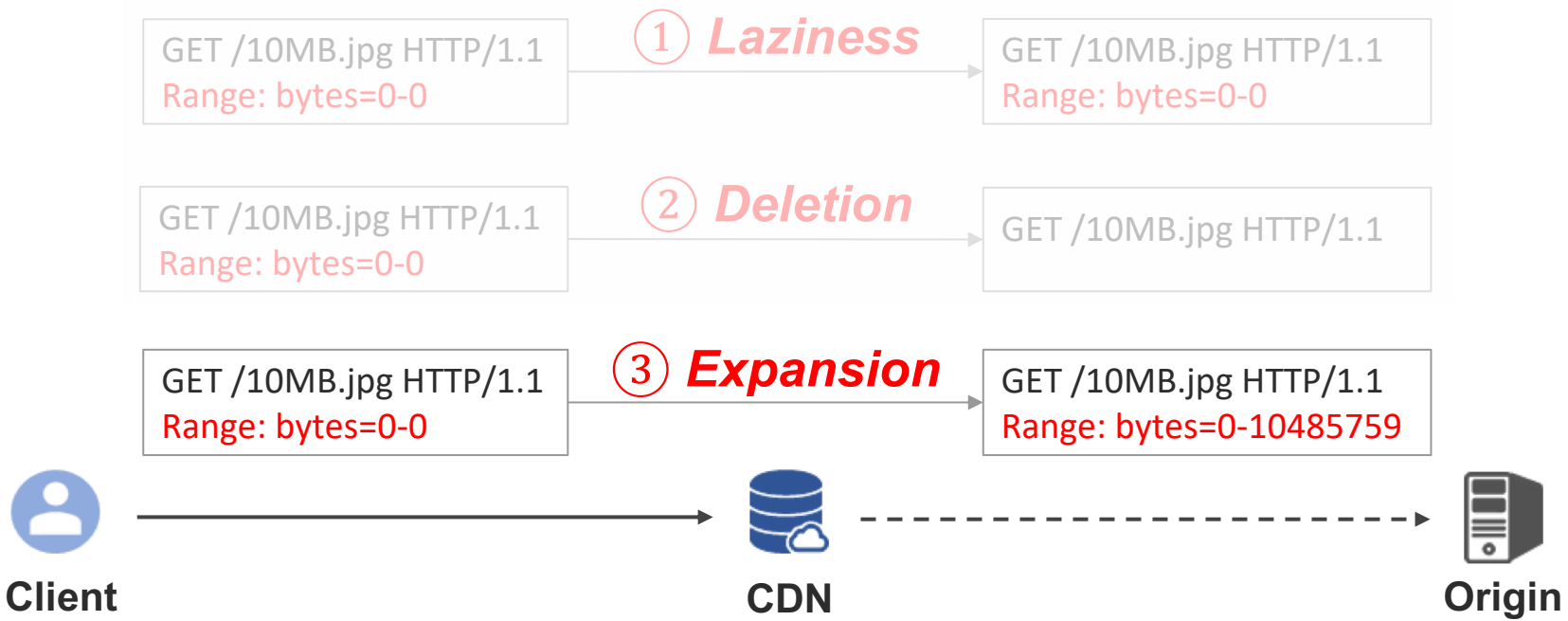
CDN's Range Forwarding Policies

- Different policies for malformed Range header.
  - *Laziness*, ***Deletion***, *Expansion*.



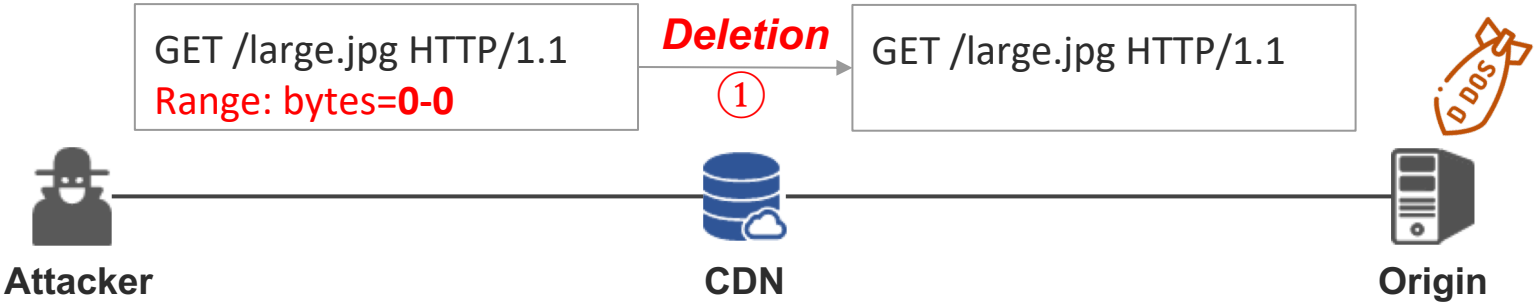
CDN's Range Forwarding Policies

- Different policies for malformed Range header.
  - ➢ *Laziness*, *Deletion*, ***Expansion***.



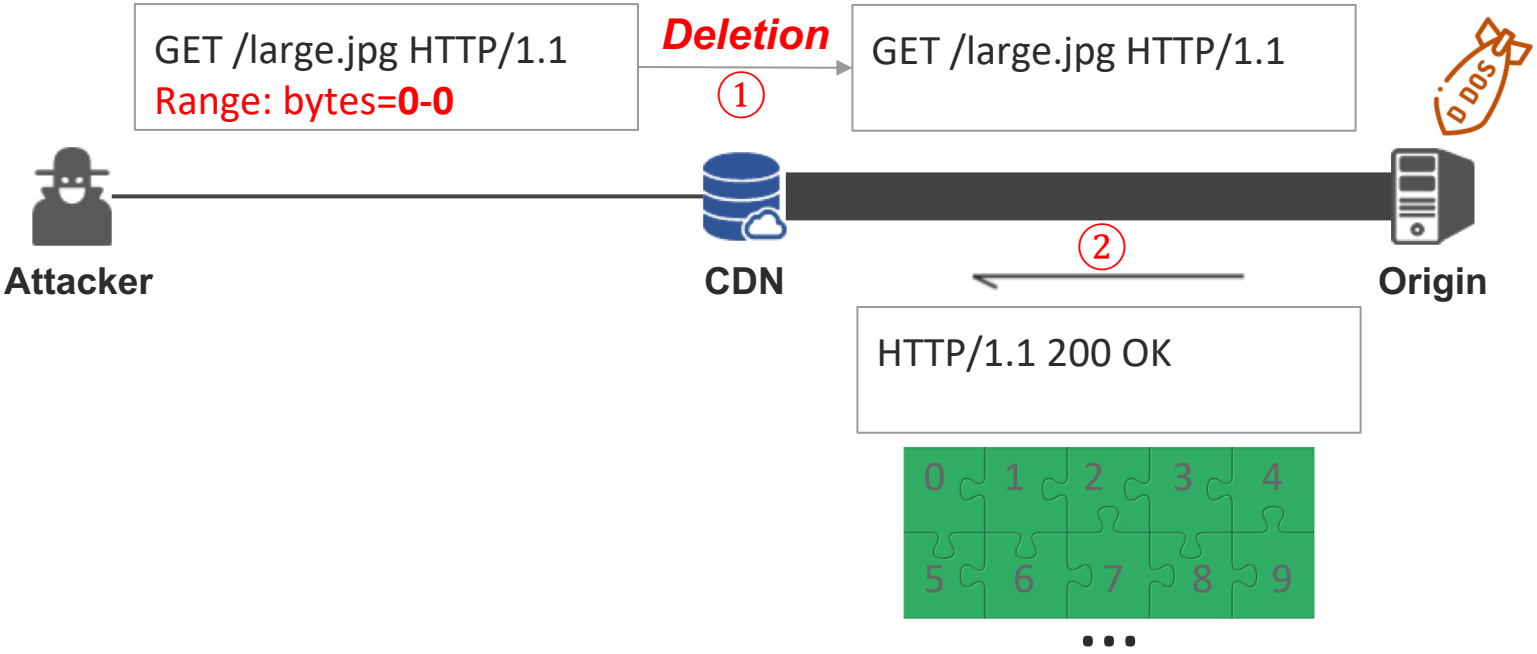
Small Byte Range (SBR) Attack

- The ***Deletion*** and ***Expansion*** policies will cause SBR attack.
  - Increasing bytes requested from the origin server.



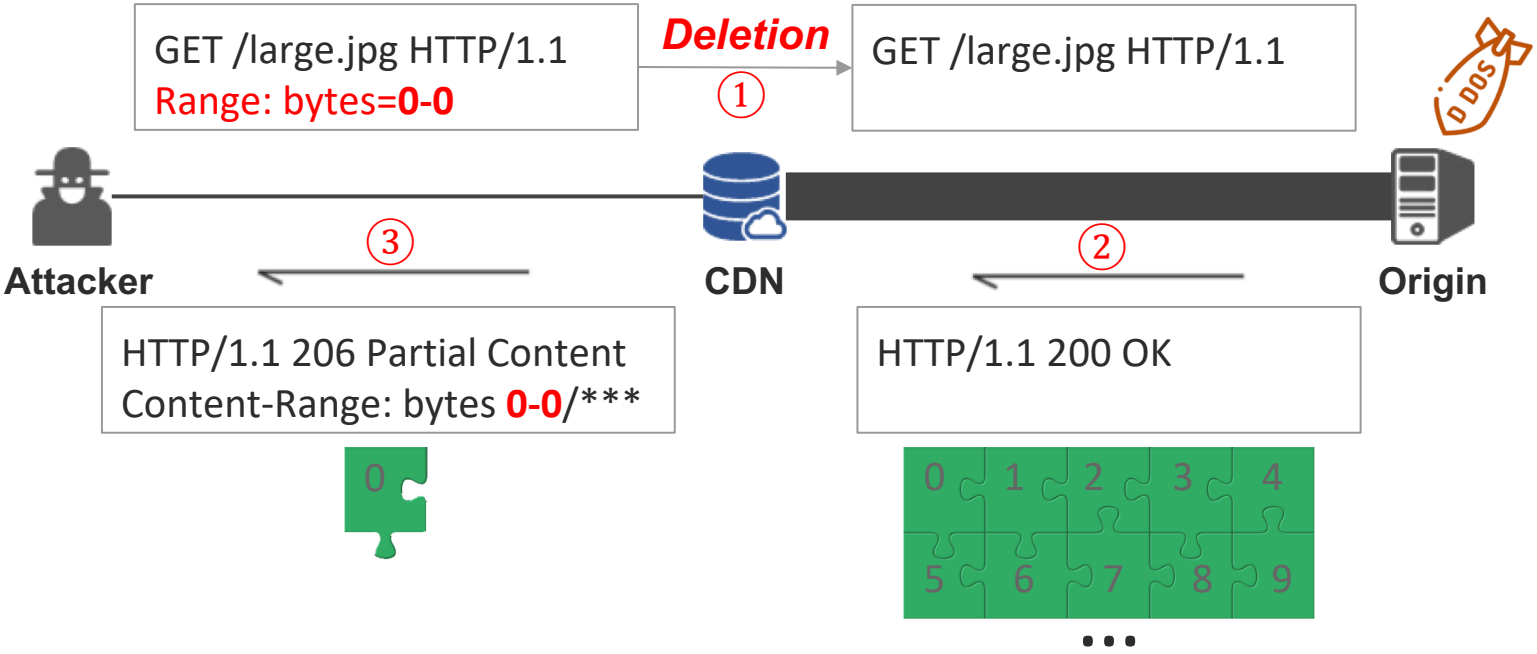
Small Byte Range (SBR) Attack

- The ***Deletion*** and ***Expansion*** policies will cause SBR attack.
  - Increasing bytes requested from the origin server.



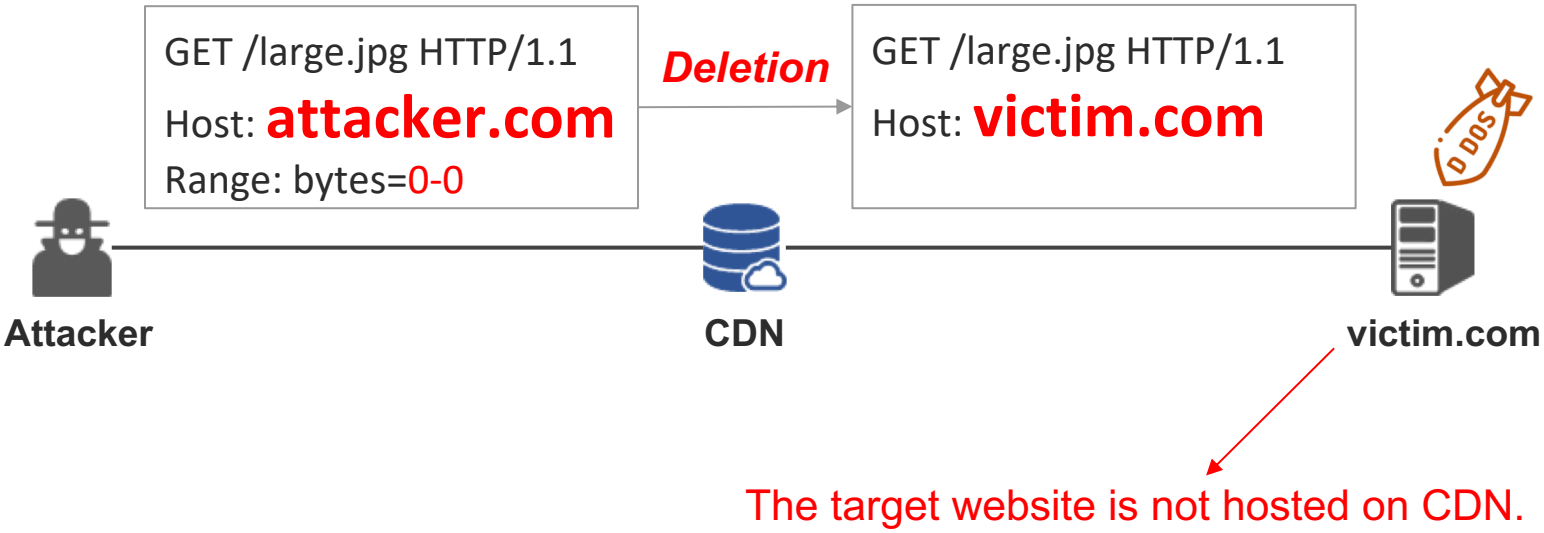
Small Byte Range (SBR) Attack

- The ***Deletion*** and ***Expansion*** policies will cause SBR attack.
  - Increasing bytes requested from the origin server.



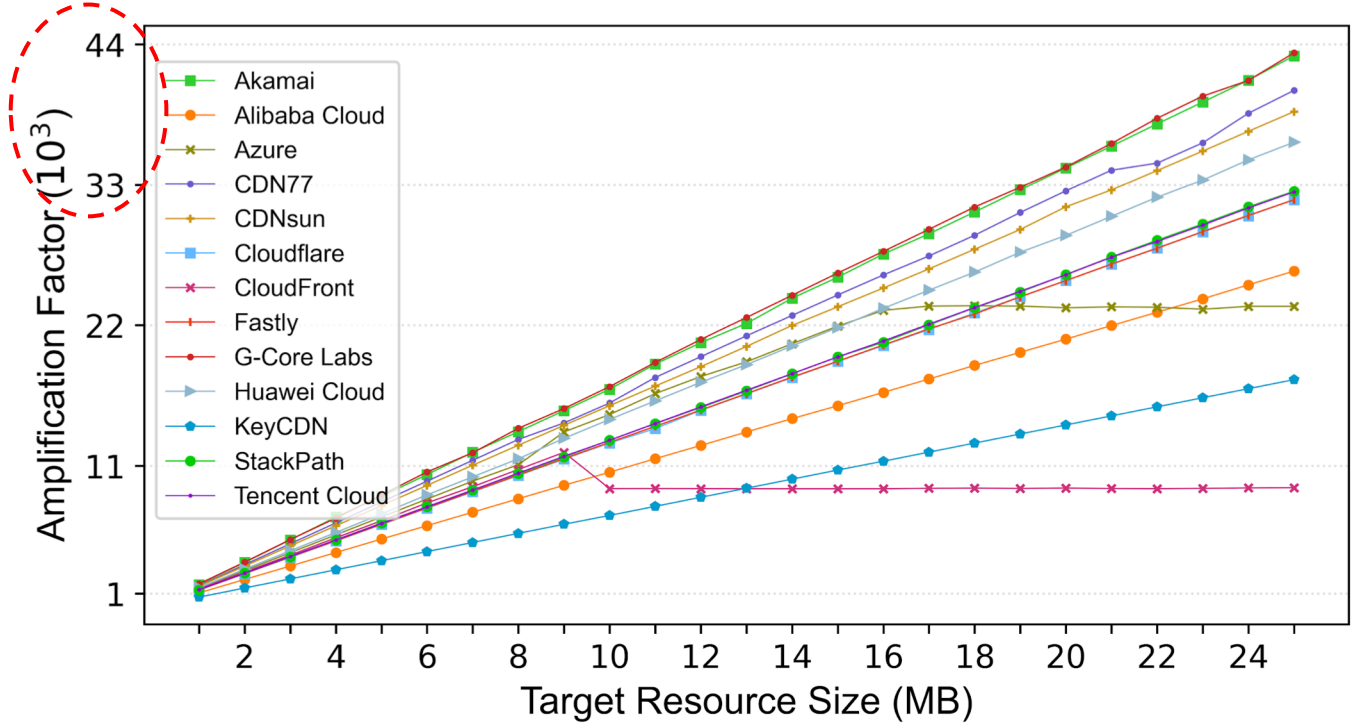
Victims Include Websites Not Hosted on CDN

- Most CDN vendors do not validate the origin servers.
  - Almost all websites are potentially affected.



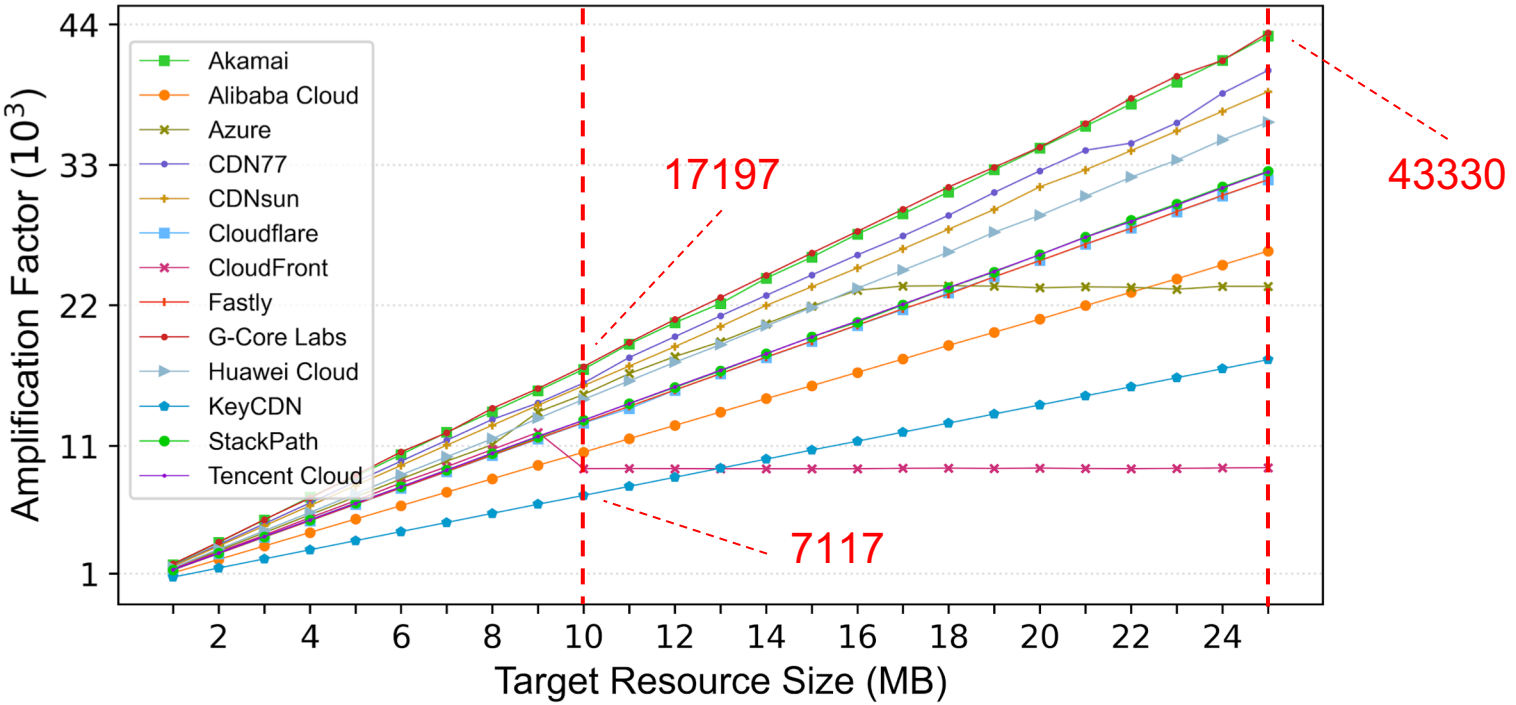
Evaluation of SBR Attack

- 13 popular CDN vendors we tested were vulnerable.
  - The amplification factor exceeds most traditional attack methods.



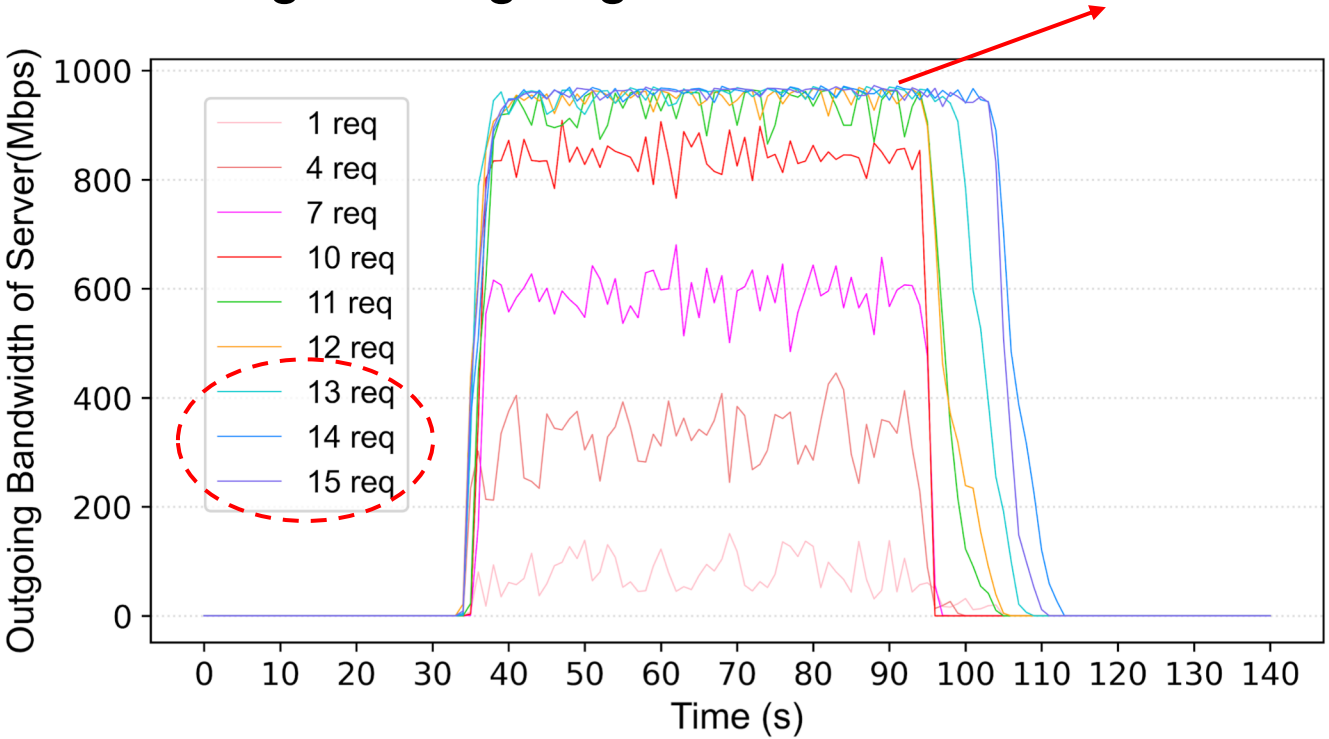
Evaluation of SBR Attack

- 13 popular CDN vendors we tested were vulnerable.
  - The amplification factor exceeds most traditional attack methods.



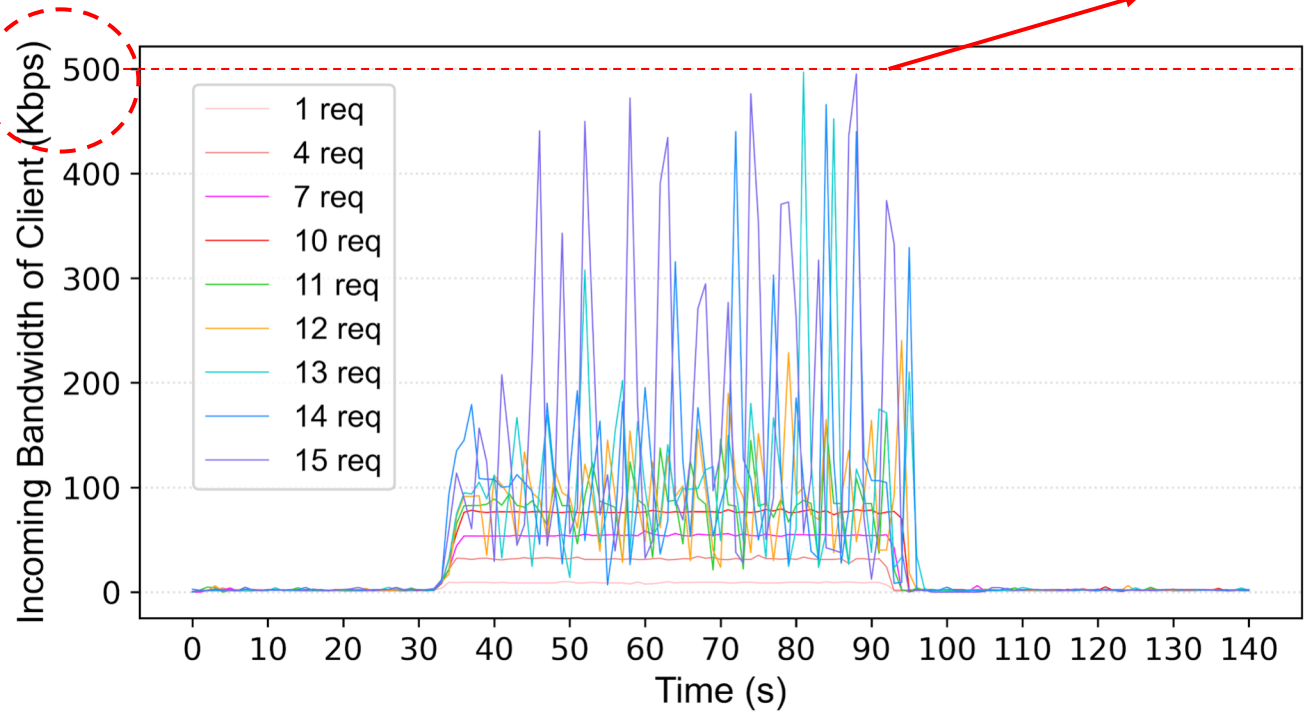
Demo of SBR Attack

- Experiment setup: bandwidth (1000Mbps), target file (10MB).
- Result: The origin's outgoing bandwidth was exhausted.



Demo of SBR Attack

- All CDNs raised no alert under the default configuration.
- The Client's incoming bandwidth consumption < 500Kbps

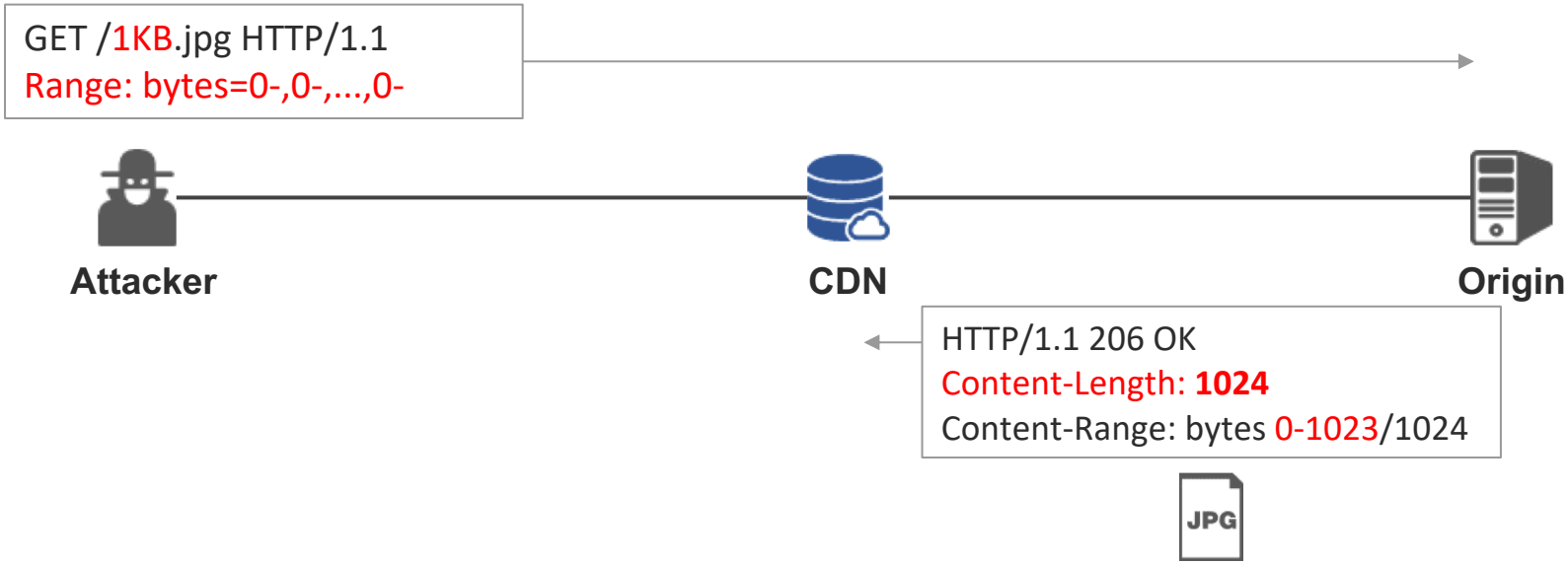


Attack-2

Overlapping Byte Ranges (OBR) Attack

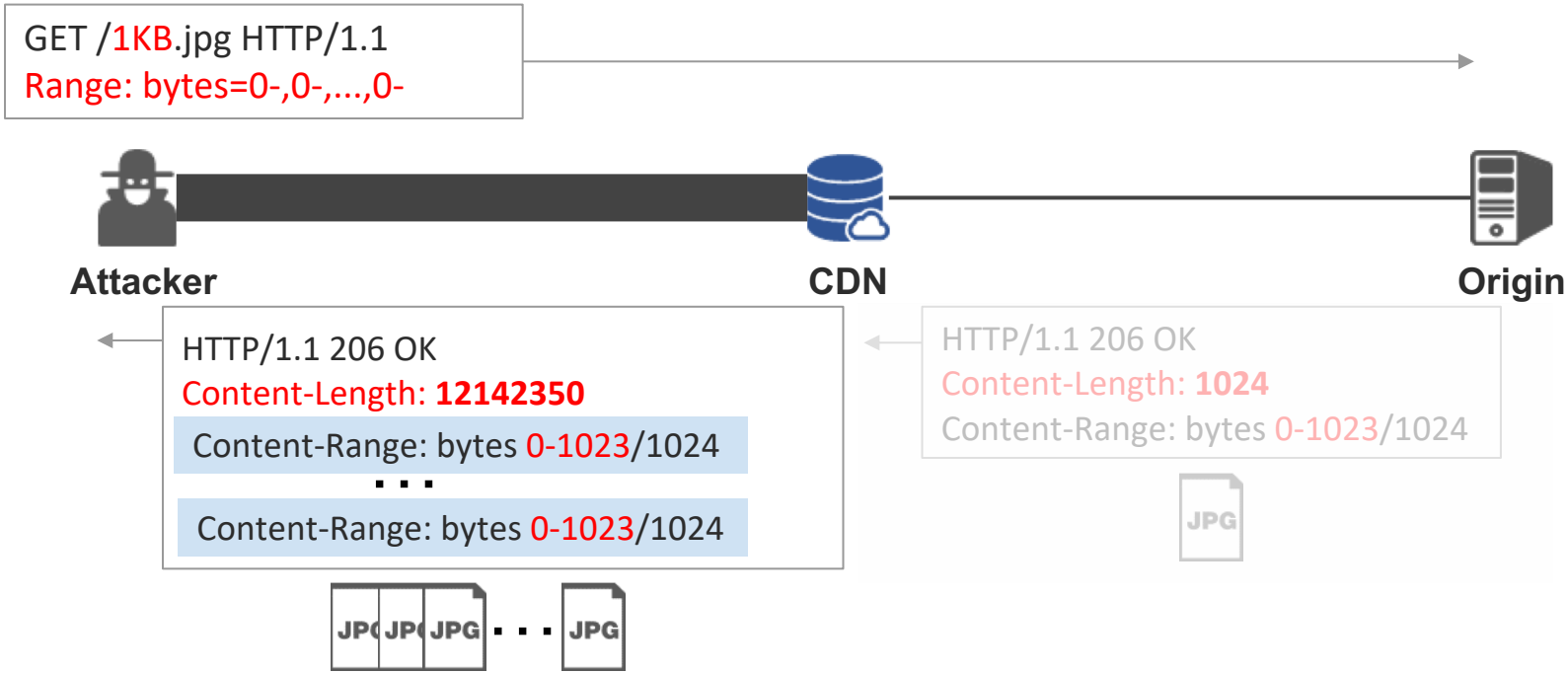
Overlapping Multi-range Requests

- RFC7233 suggests to **coalesce** overlapping multi-range requests.



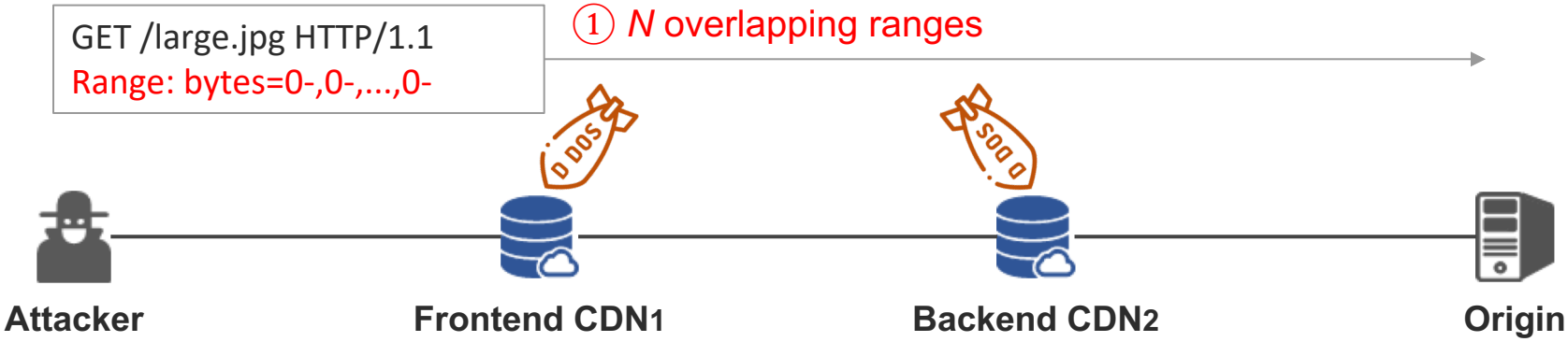
Overlapping Multi-range Requests

- RFC7233 suggests to **coalesce** overlapping multi-range requests.
  - Some CDN vendors ignore this security suggestion.



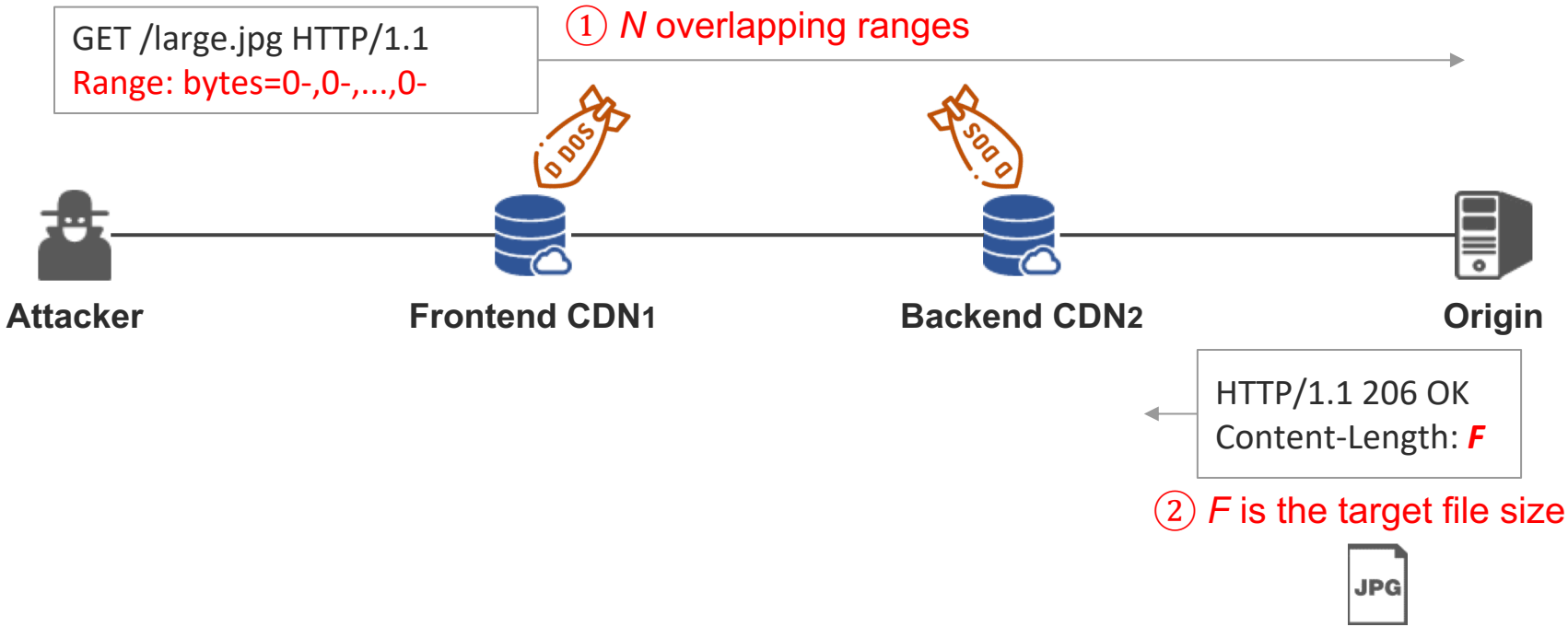
Overlapping Byte Ranges (OBR) Attack

- Two CDNs can be cascaded together.
- The Backend CDN returns overlapping multi-part responses.



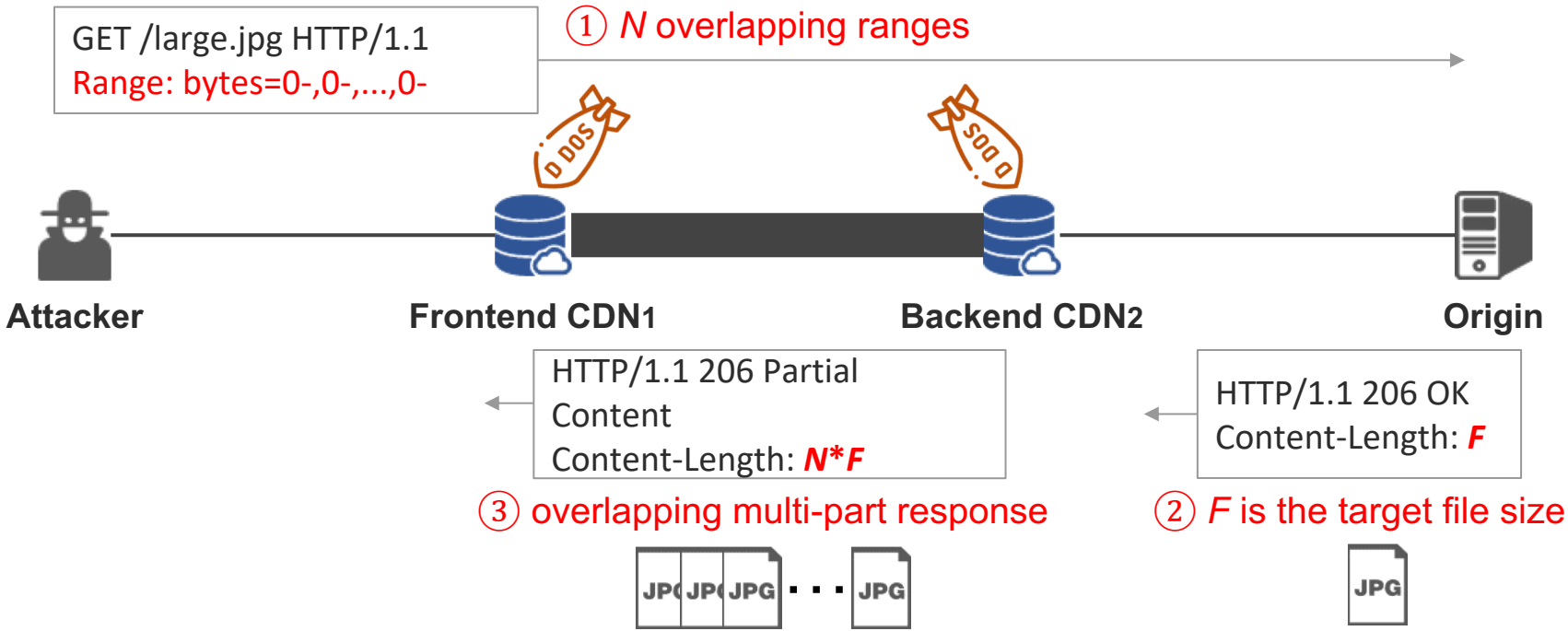
Overlapping Byte Ranges (OBR) Attack

- Two CDNs can be cascaded together.
- The Backend CDN returns overlapping multi-part responses.



Overlapping Byte Ranges (OBR) Attack

- Two CDNs can be cascaded together.
- The Backend CDN returns overlapping multi-part responses.



Evaluation of OBR Attack

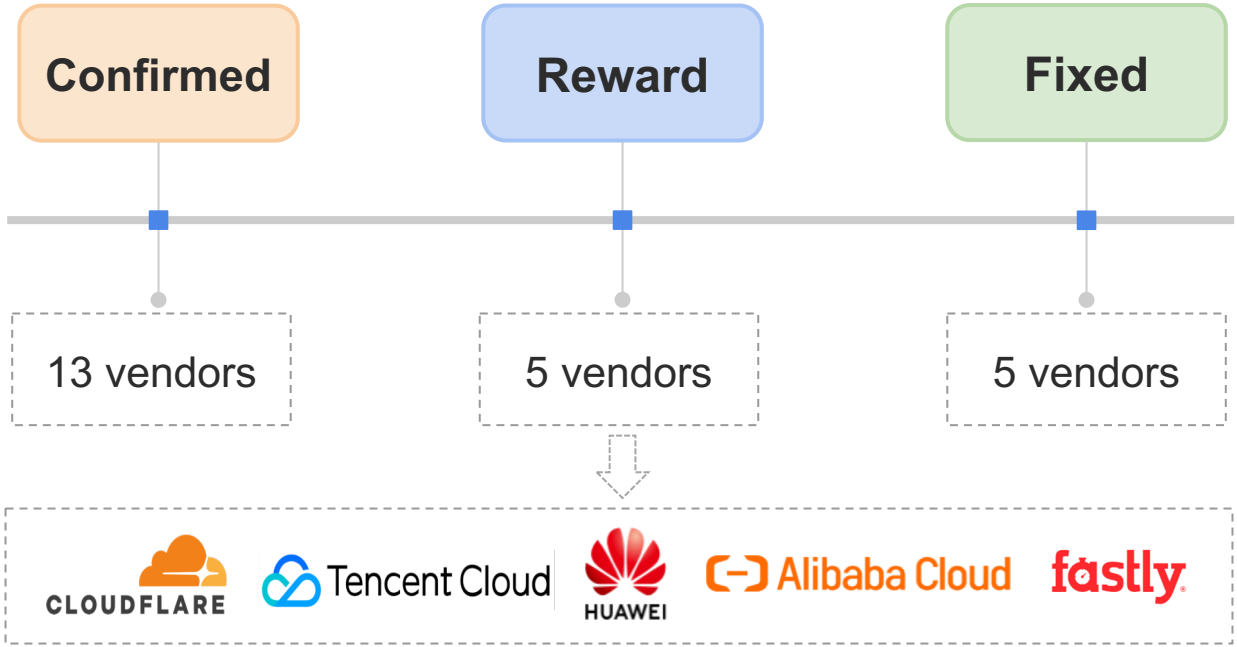
- Totally 11 combinations of cascaded CDNs are affected.
  - The amplification factor far exceeds traditional attack methods.

FCDN	BCDN	Traffic from Orign to Backend CDN	Traffic from Backend CDN to Frontend CDN	Amplification Factor
CDN77	Akamai	1676B	6350944B	**3789.35**
Cloudflare	Akamai	1676B	12456915B	**7432.53**
StackPath	Akamai	1676B	12522091B	**7471.41**
CDN77	StackPath	1808B	6413097B	**3547.07**
...	...	...	...	**...**
Traditional NTP reflection attack				**4670**

Discussion & Summary

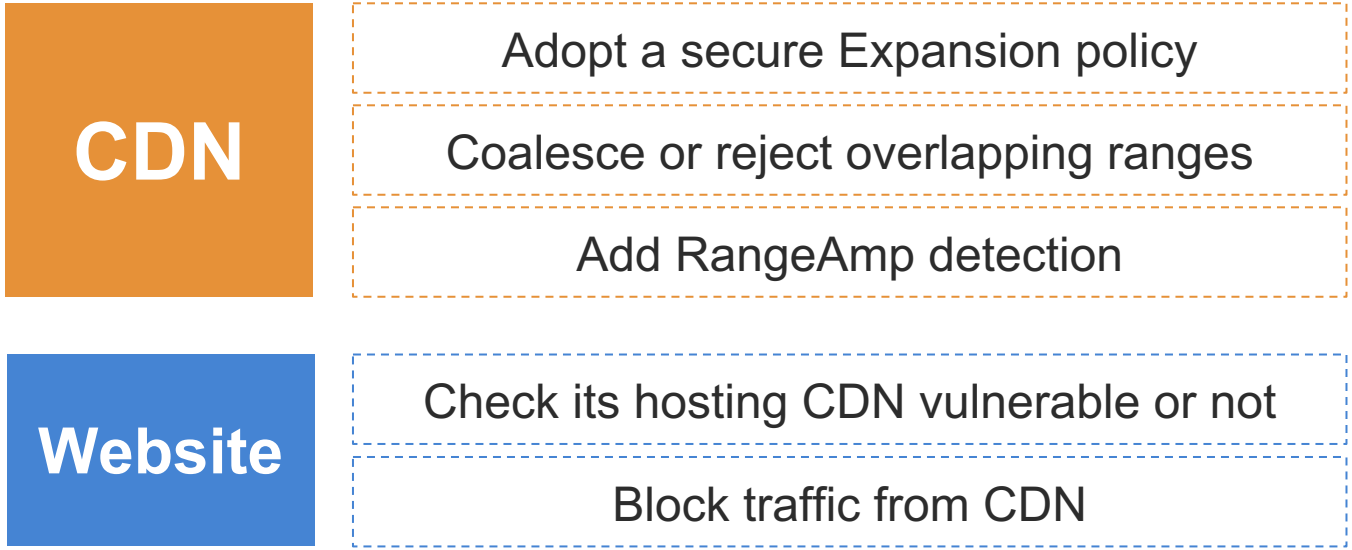
Responsible Disclosure

- Helping CDN vendors eliminate the detected threats.
  - Vendors have 7 months to mitigate it before this paper is published.



Mitigation and Solution

- Proposing mitigation and solution at different levels.



Media Coverage

- ZDNet, iTnews, GovCERT.HK, DOSarrest, SecNews, …

Summary

RangeAmp Attacks (SBR & OBR)

- Turn CDN into a DDoS cannon
- No botnet needed, just a laptop
- Affect most CDNs and websites
- Nullify CDN's DDoS protection