

CDN Backfired: Amplification Attacks Based on HTTP Range Requests

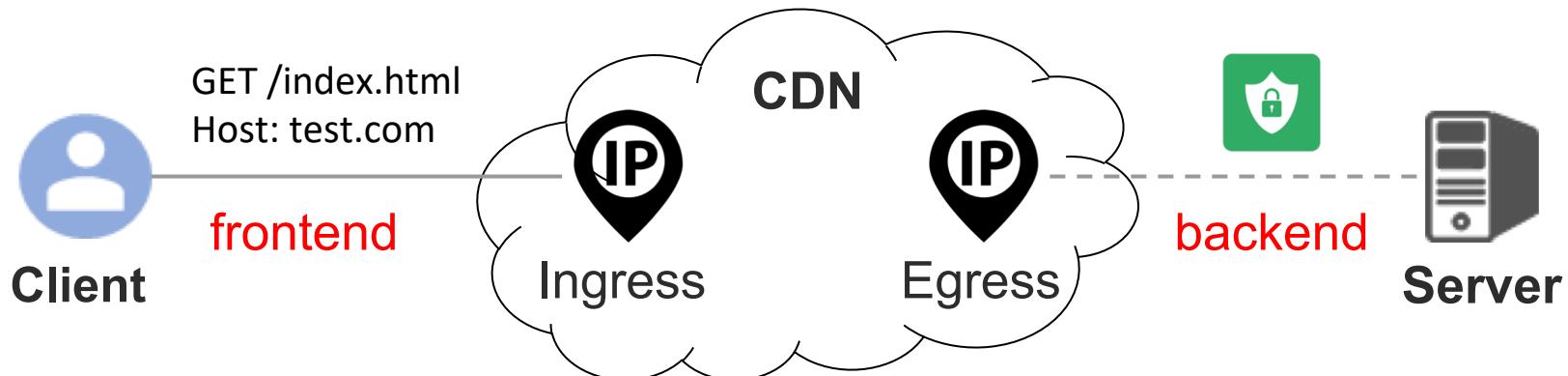
Weizhong Li, Kaiwen Shen, Run Guo, Baojun Liu, Jia Zhang,
Haixin Duan, Shuang Hao, Xiarun Chen, Yao Wang (Chaoyi Lu)



DSN 2020 - June 30, 2020

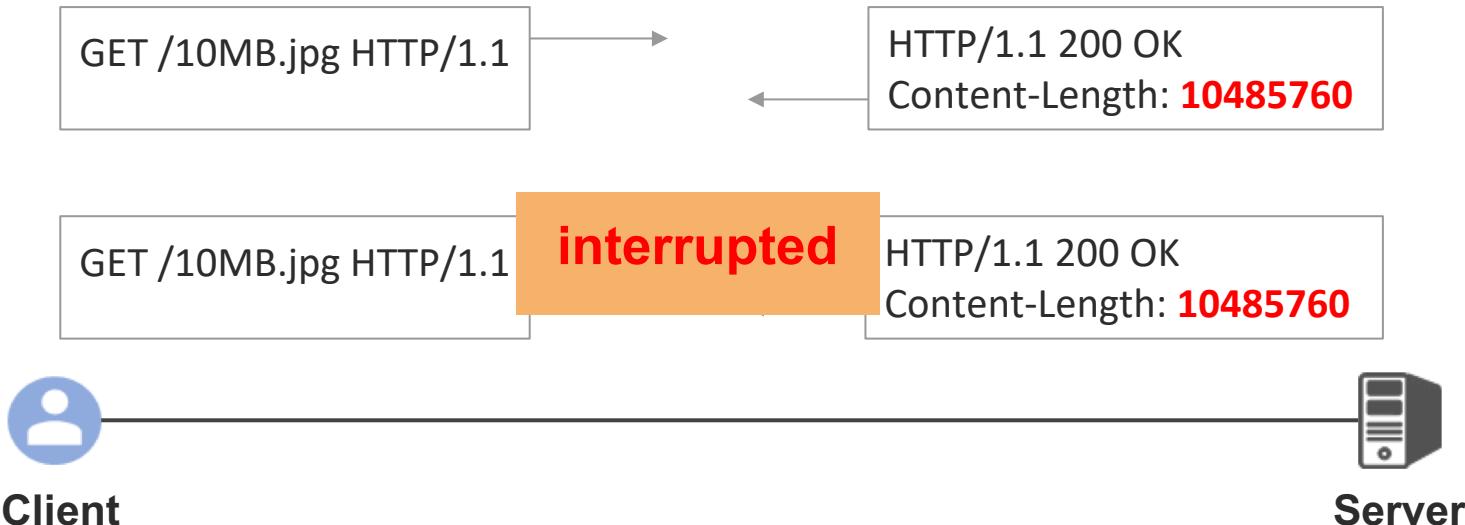
Content Delivery Network

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



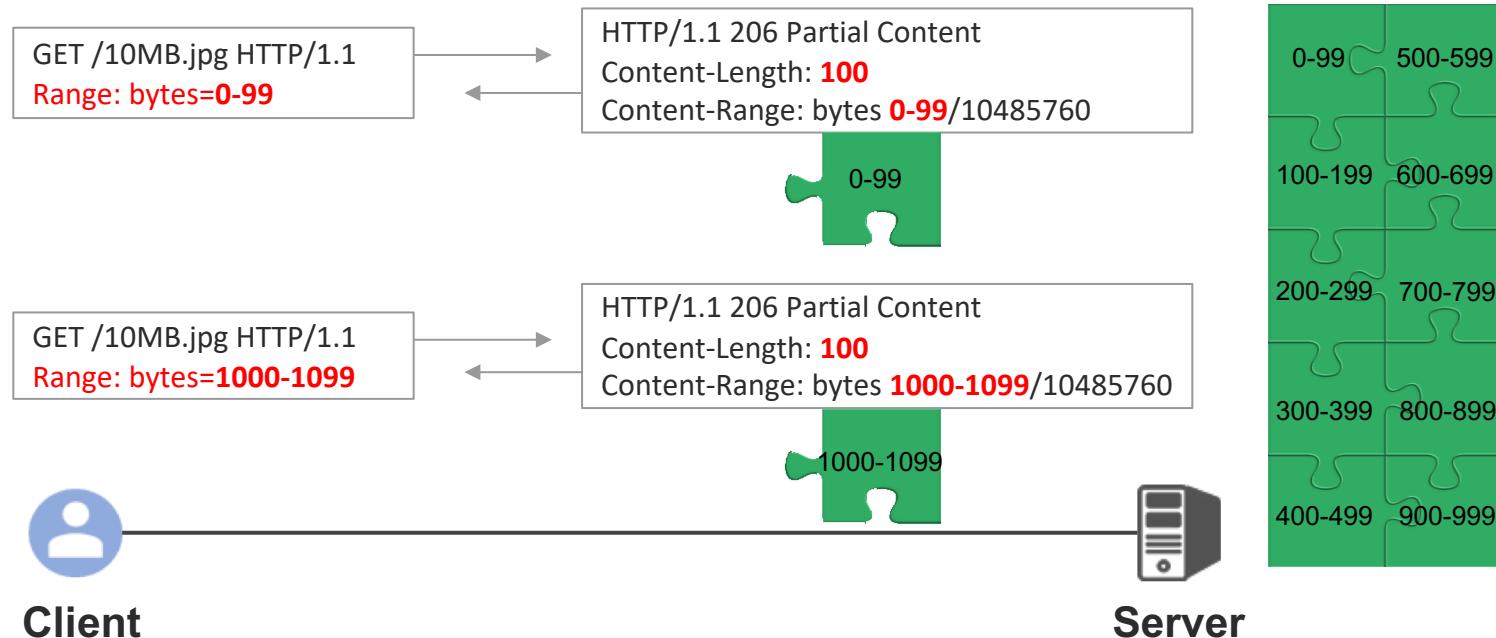
HTTP Range Request Mechanism

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



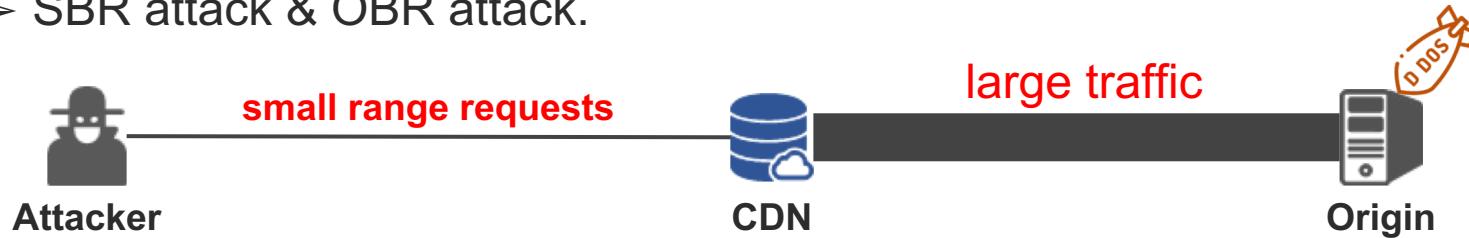
HTTP Range Request Mechanism

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

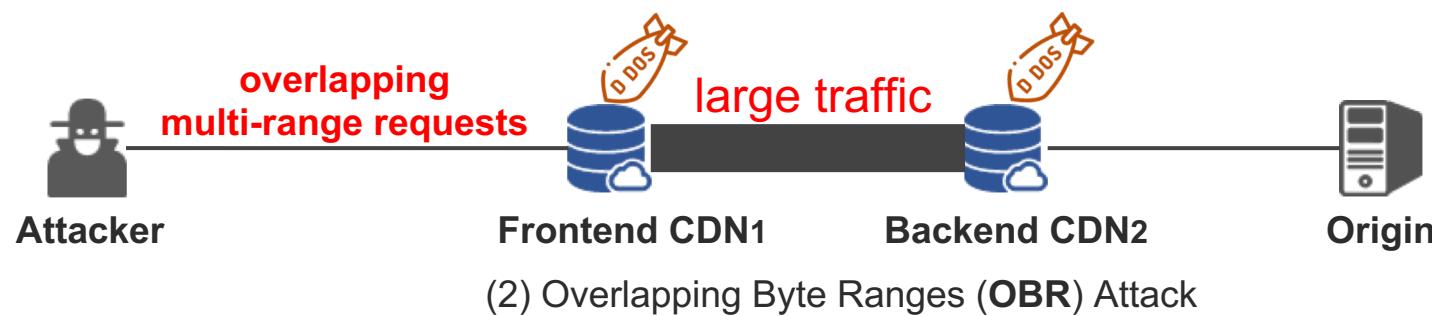


Our Work

- ❖ 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.



Alibaba Cloud



fastly



G-CORE LABS



SP//



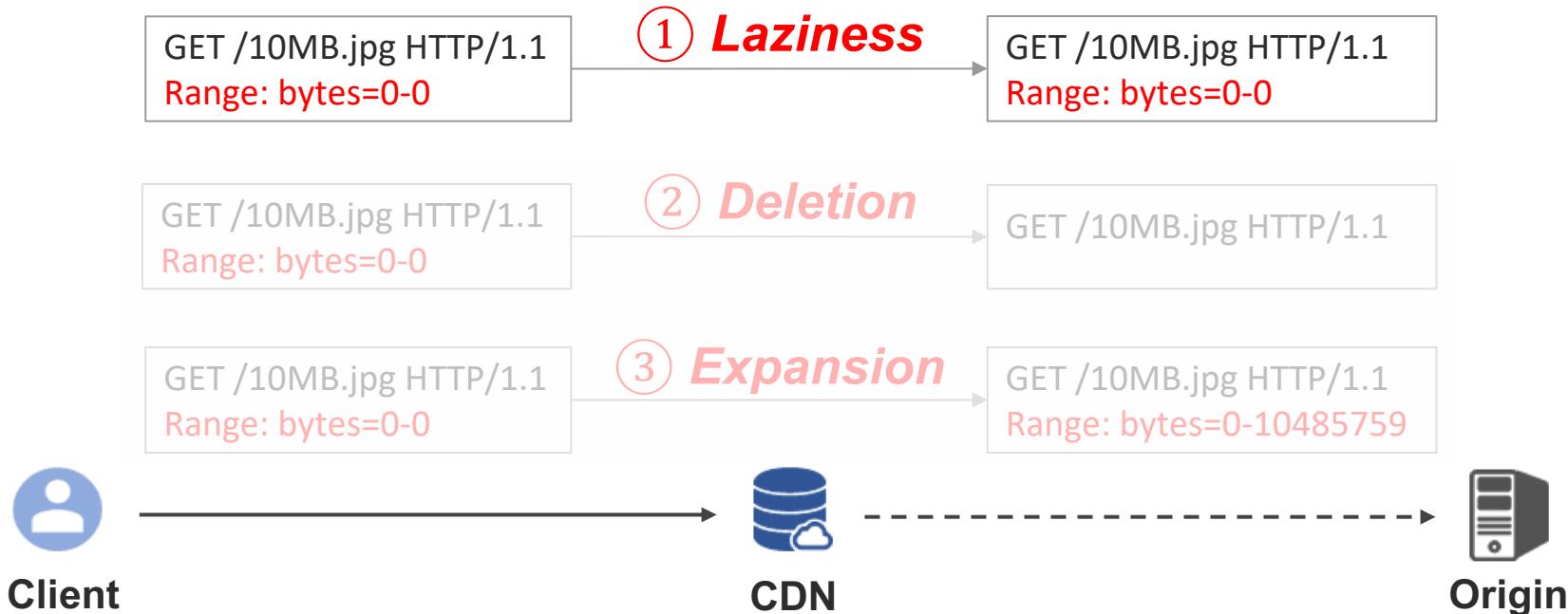
Tencent Cloud

Attack-1

Small Byte Range (SBR) Attack

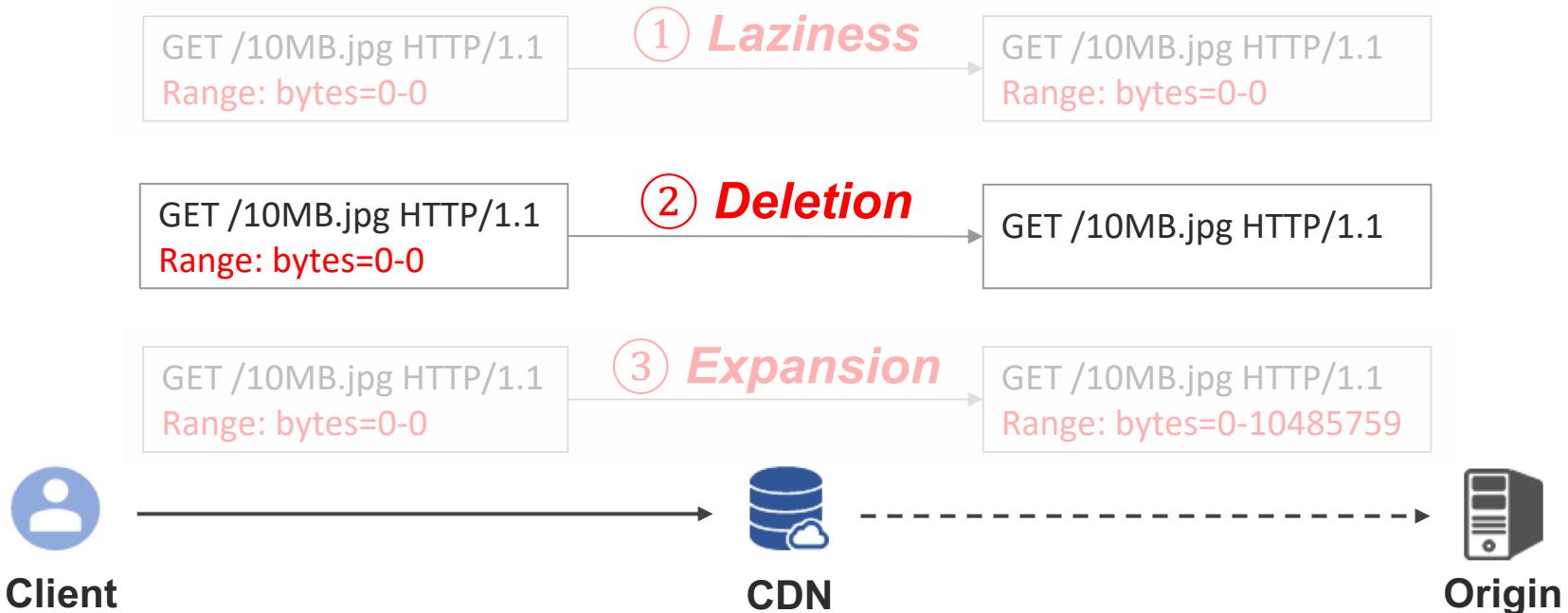
CDN's Range Forwarding Policies

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



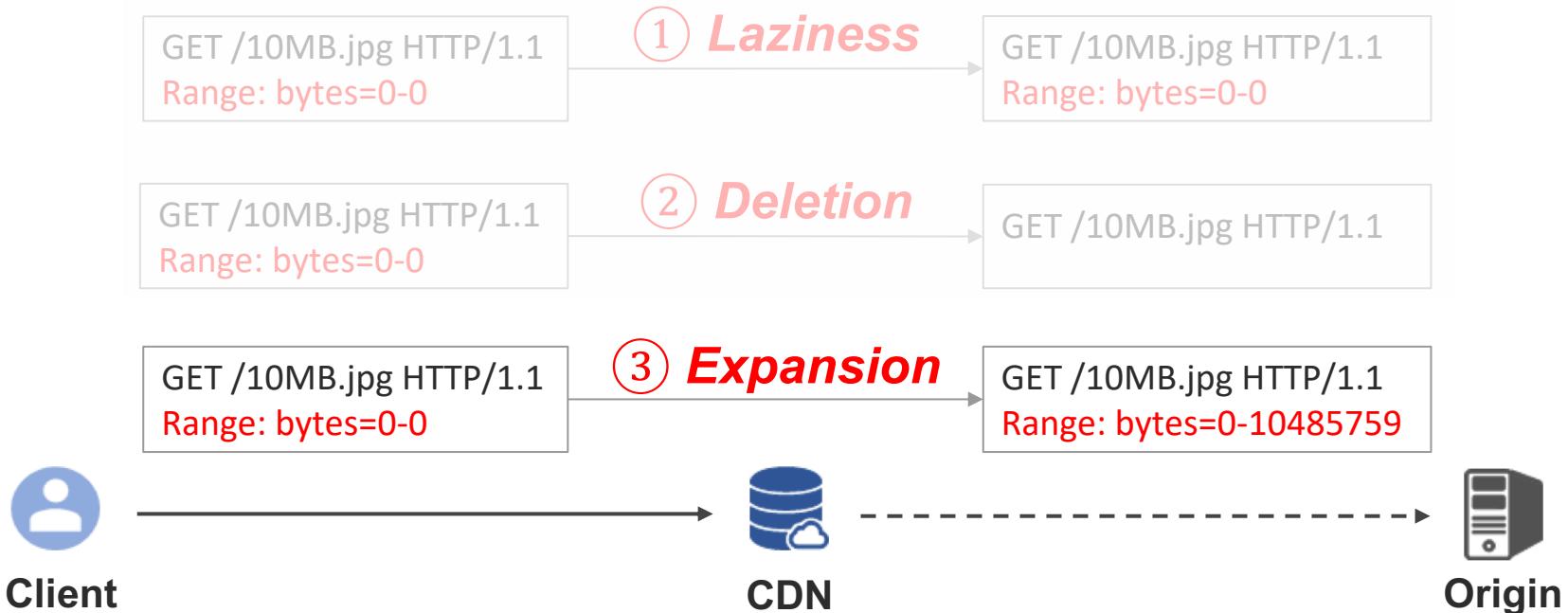
CDN's Range Forwarding Policies

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



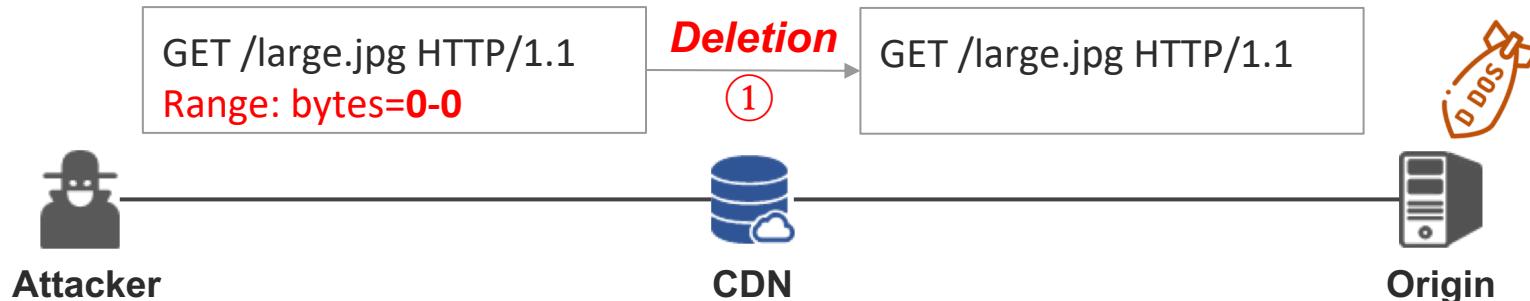
CDN's Range Forwarding Policies

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



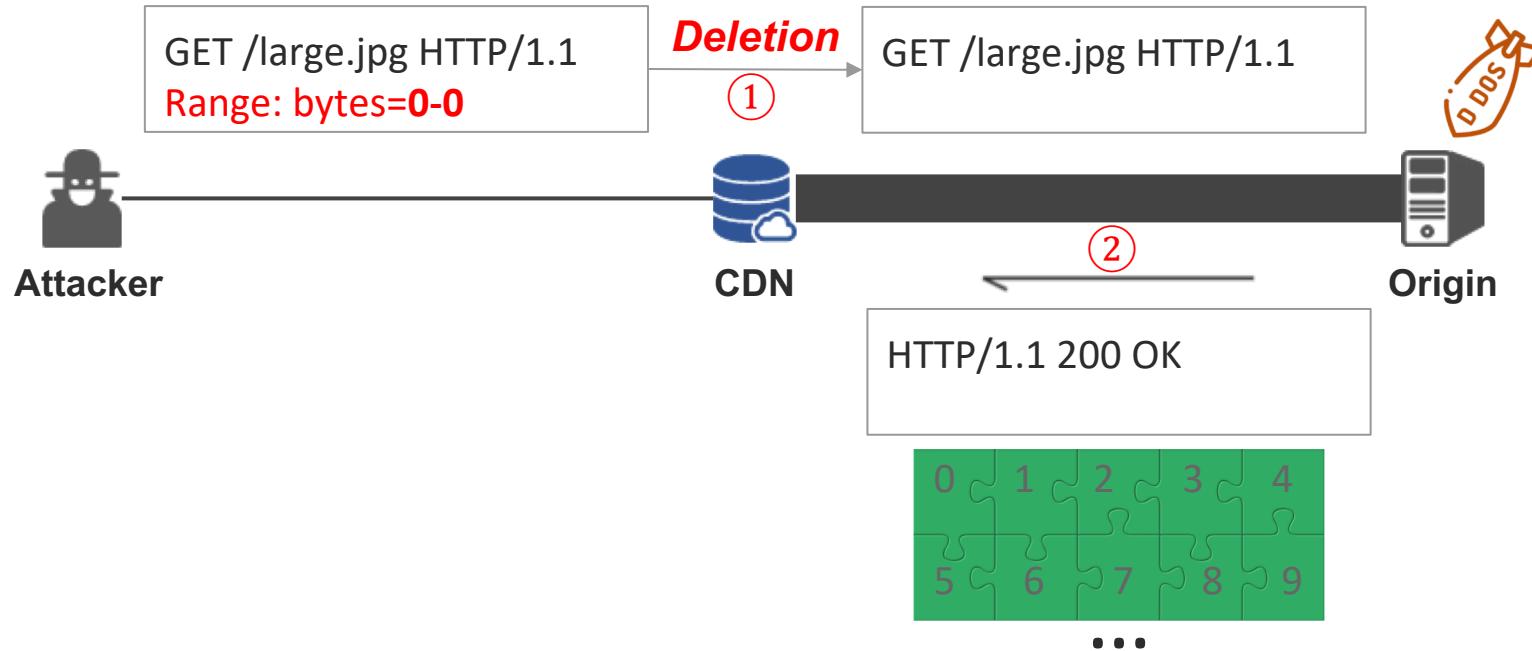
Small Byte Range (SBR) Attack

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



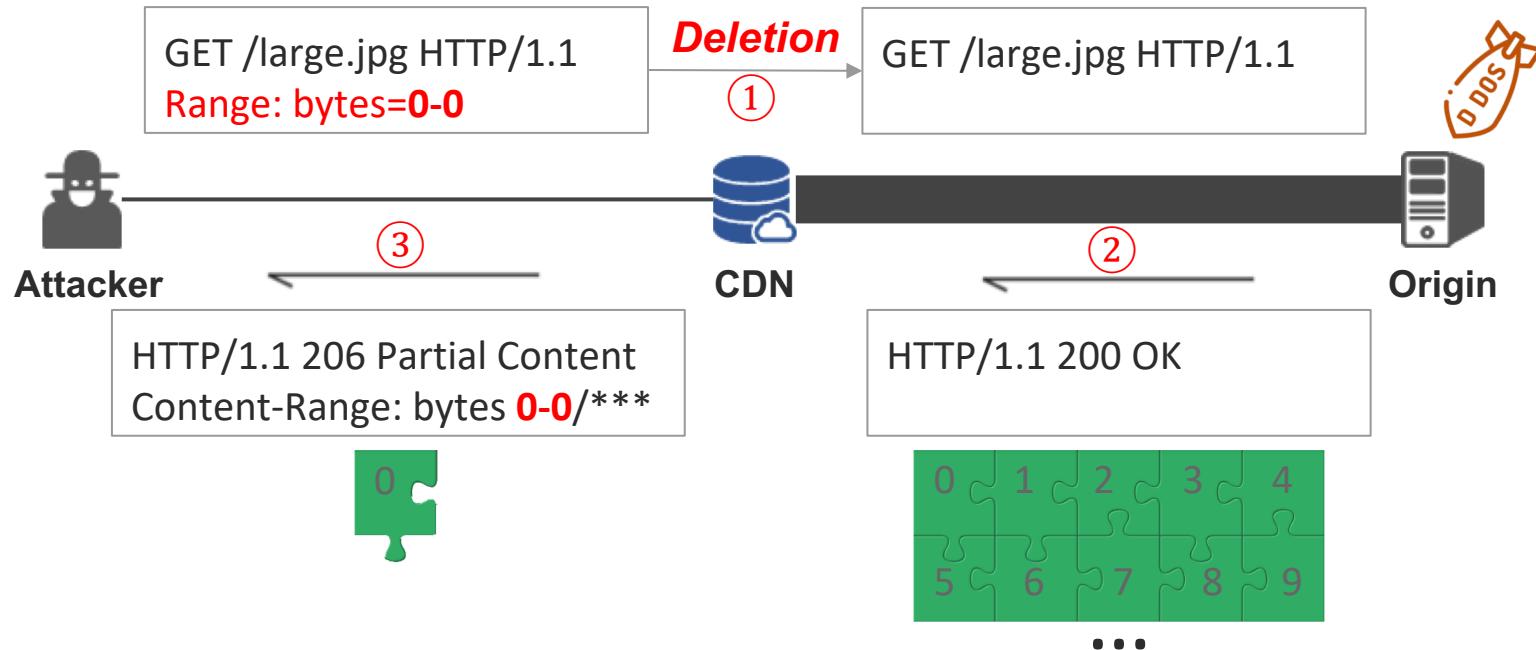
Small Byte Range (SBR) Attack

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



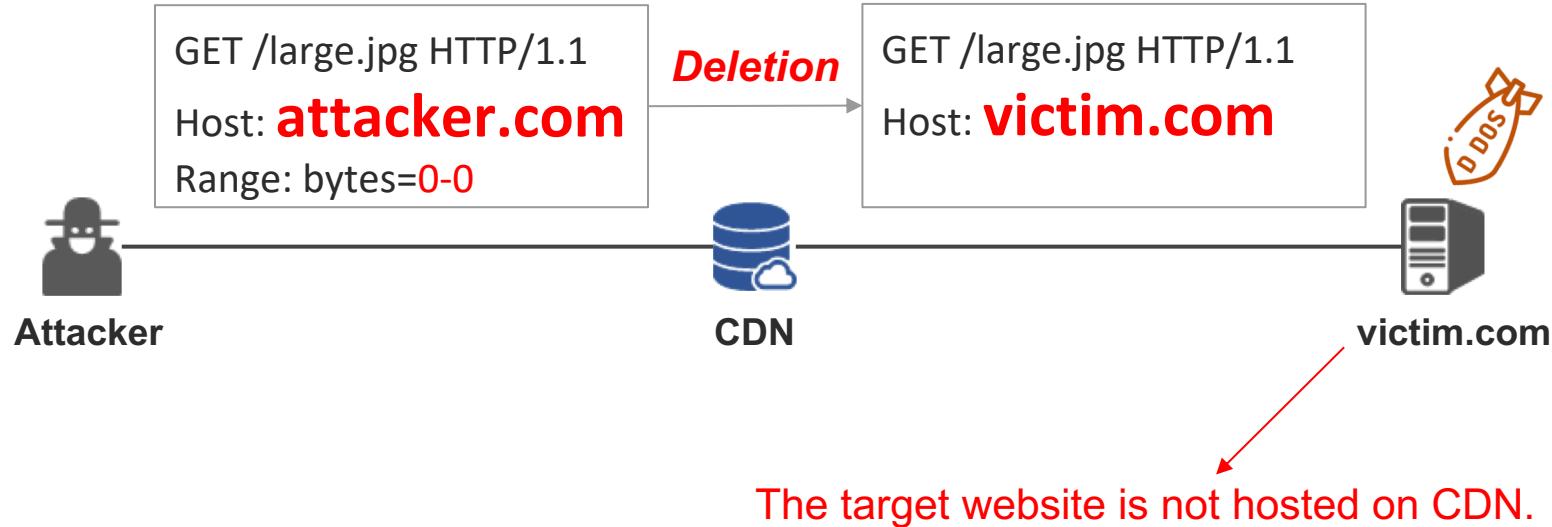
Small Byte Range (SBR) Attack

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



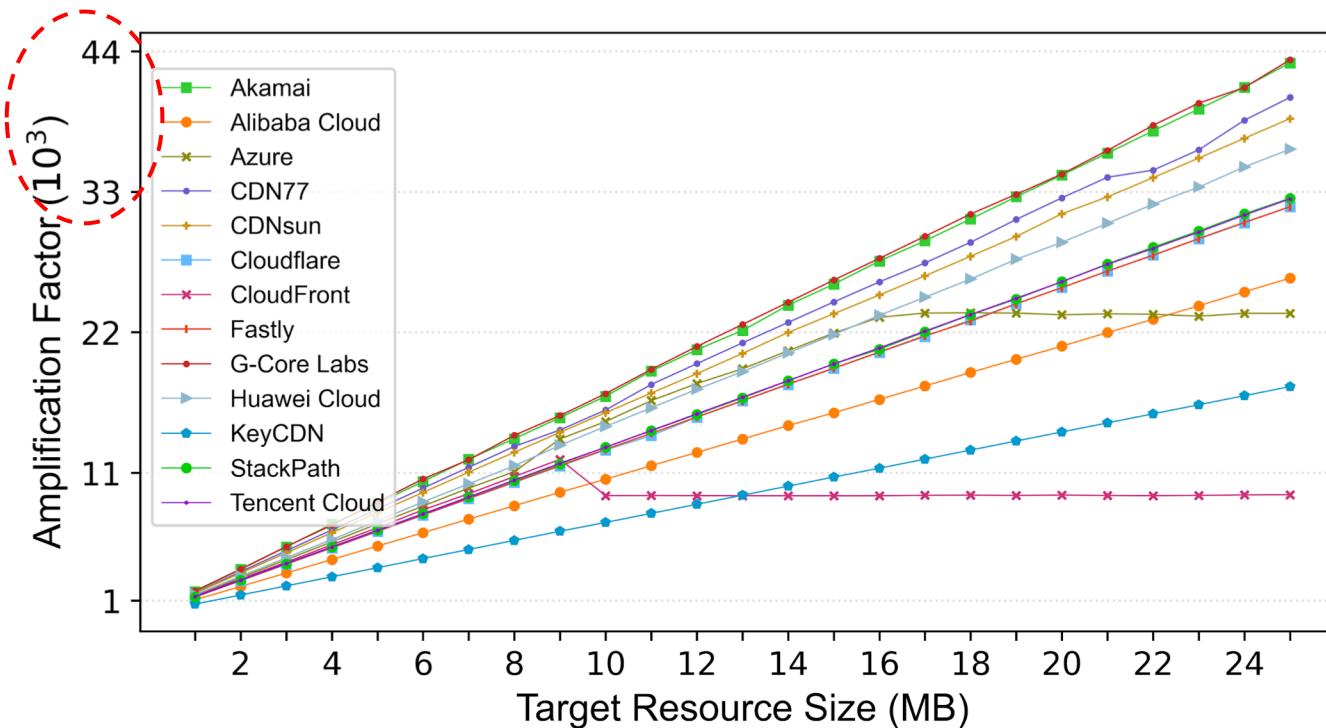
Victims Include Websites Not Hosted on CDN

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



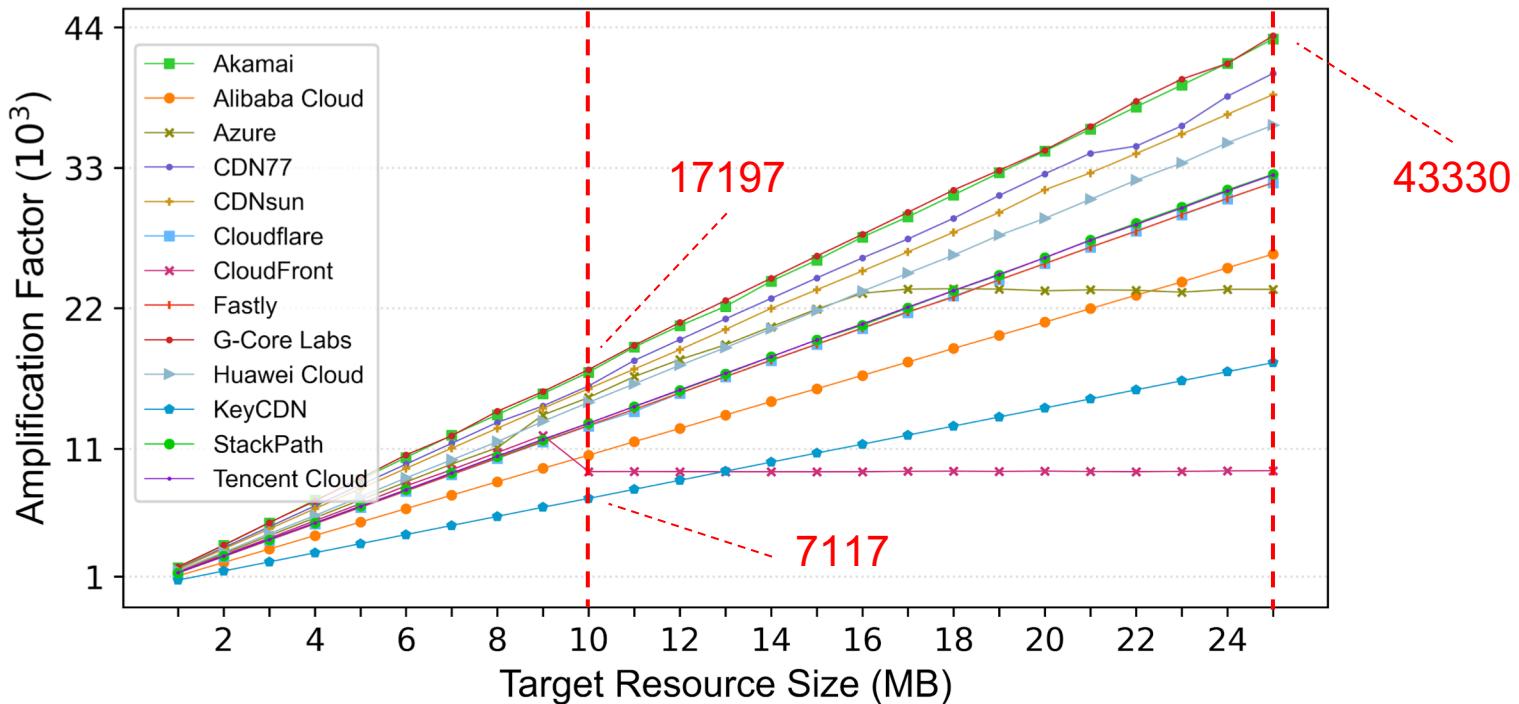
Evaluation of SBR Attack

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



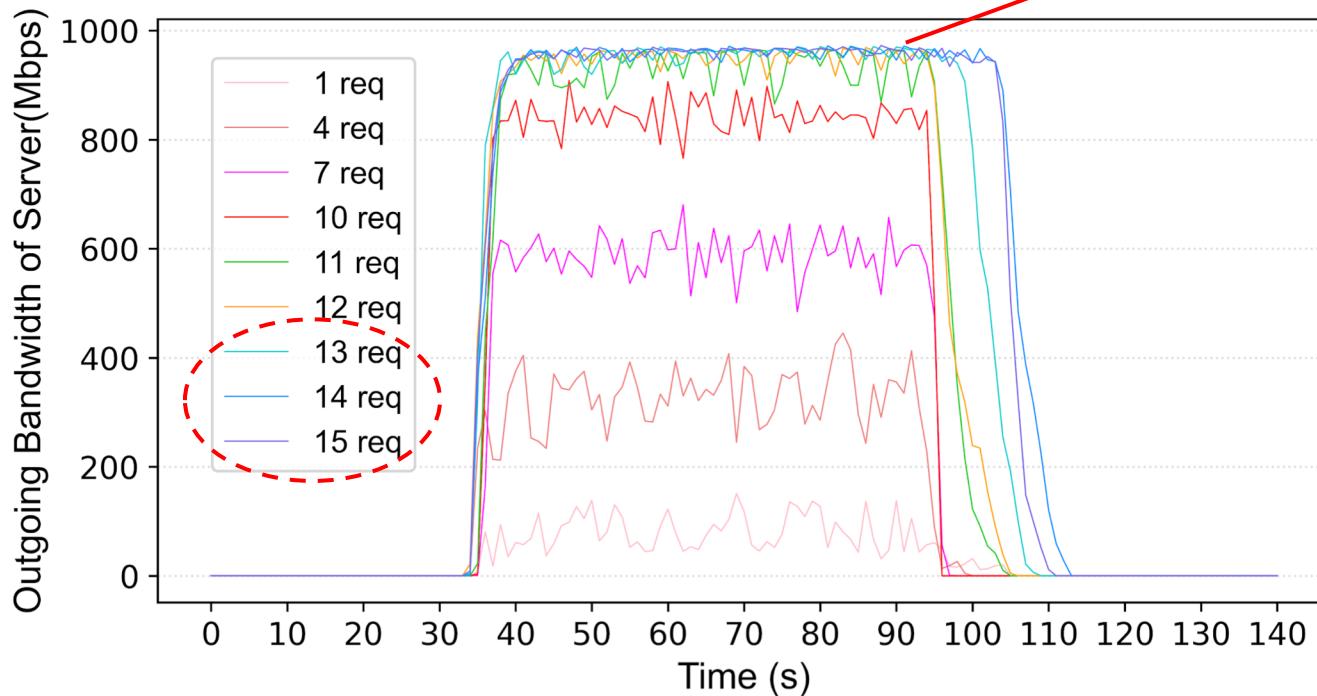
Evaluation of SBR Attack

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



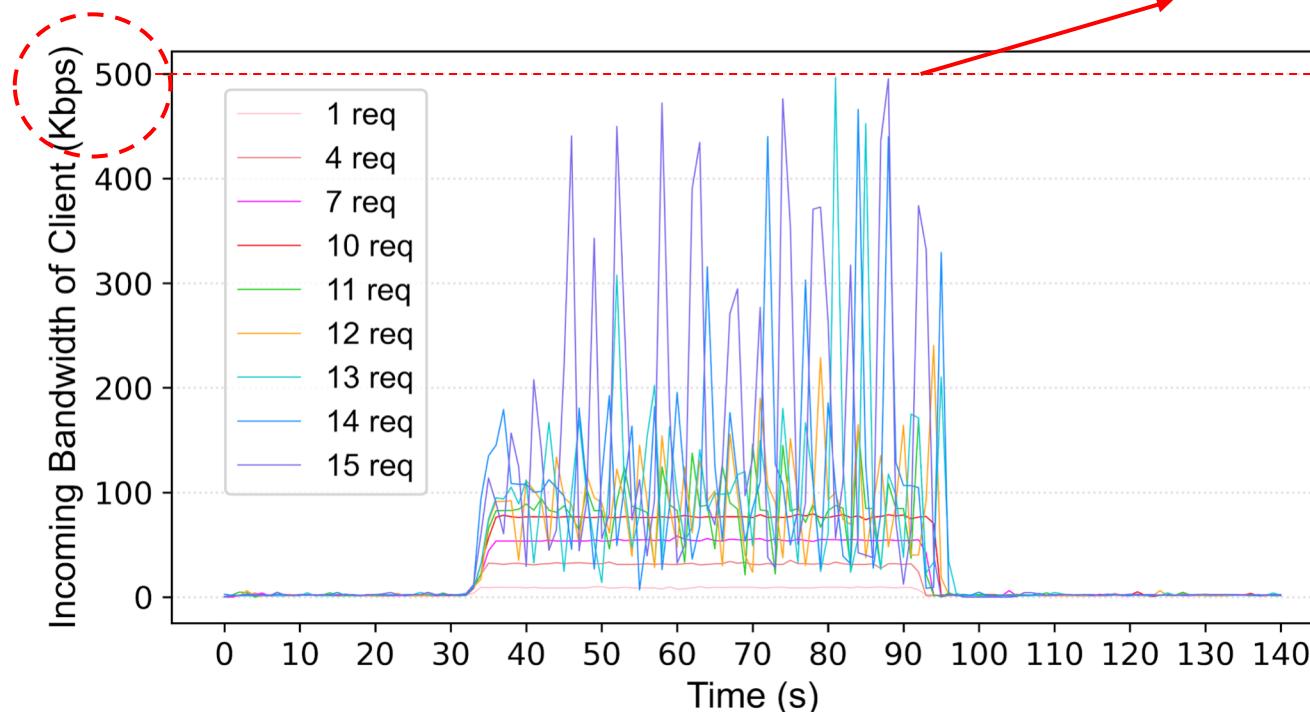
Demo of SBR Attack

- ❖ 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**

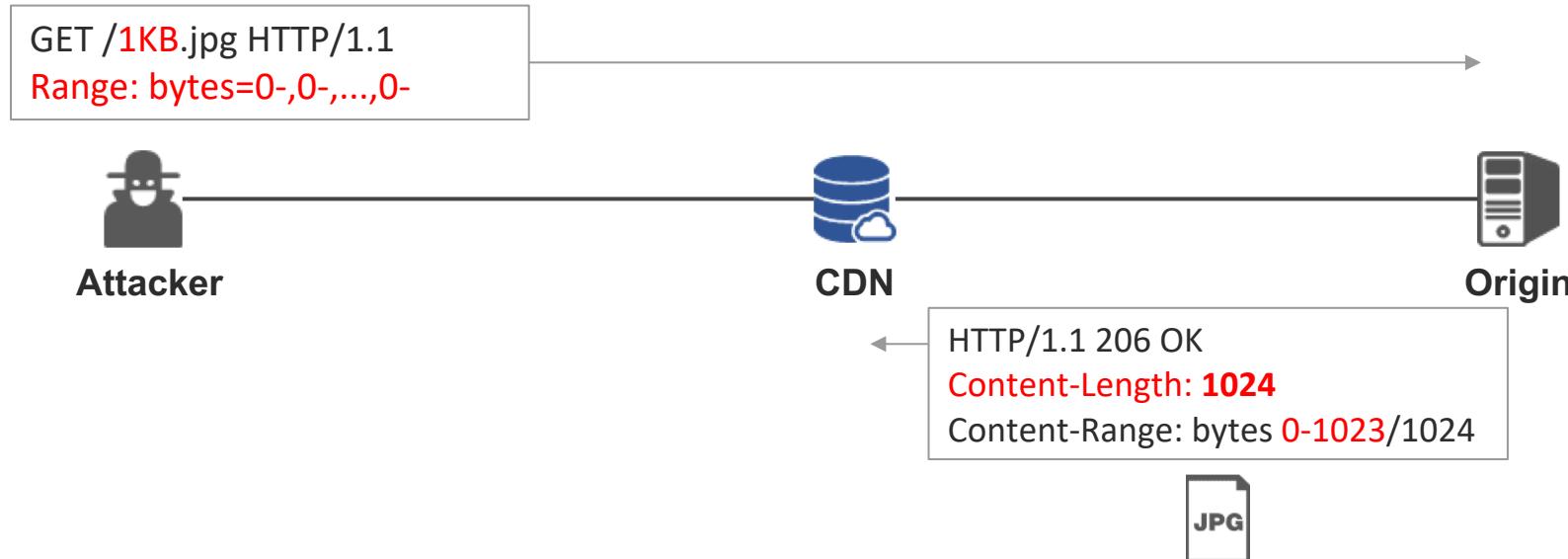


Attack-2

Overlapping Byte Ranges (OBR) Attack

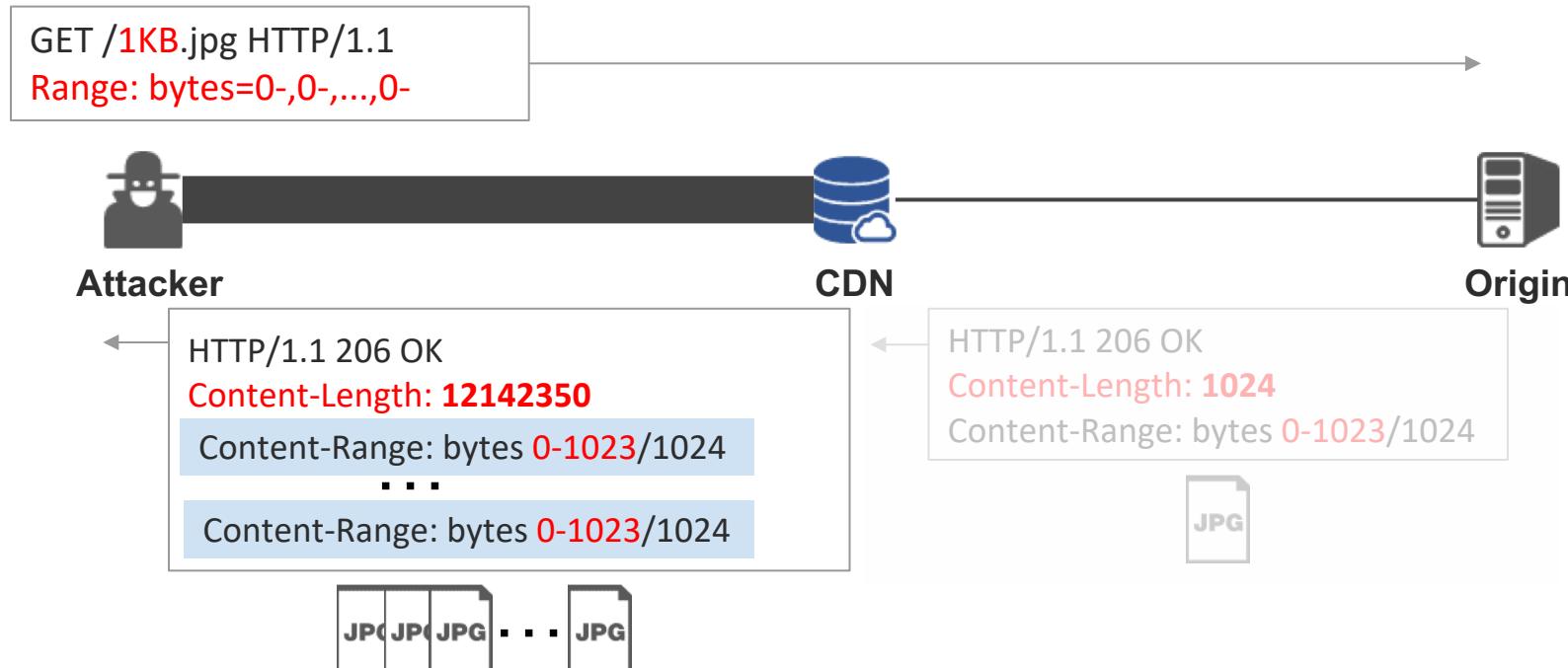
Overlapping Multi-range Requests

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



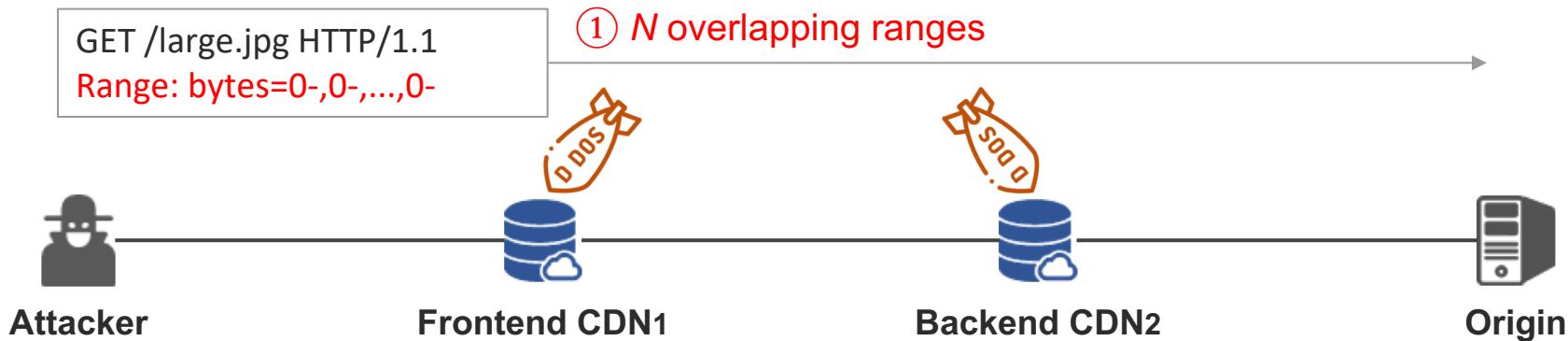
Overlapping Multi-range Requests

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



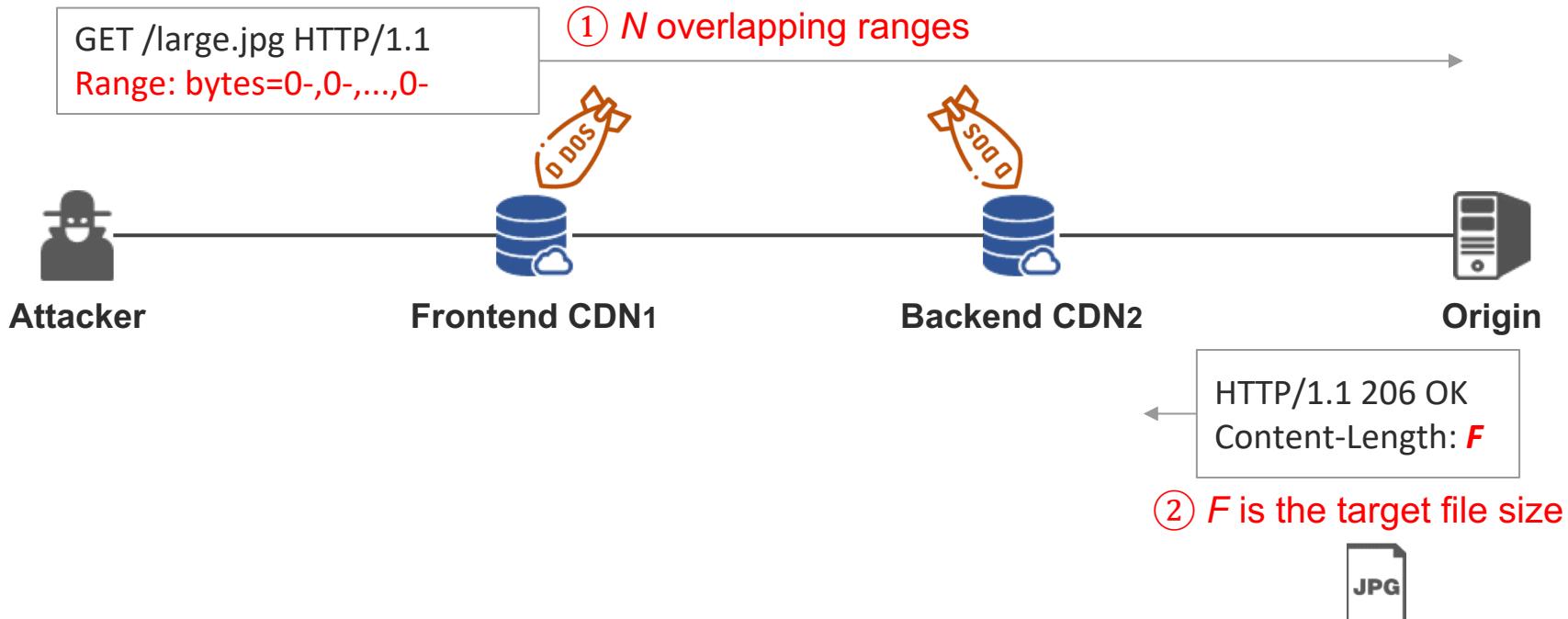
Overlapping Byte Ranges (OBR) Attack

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



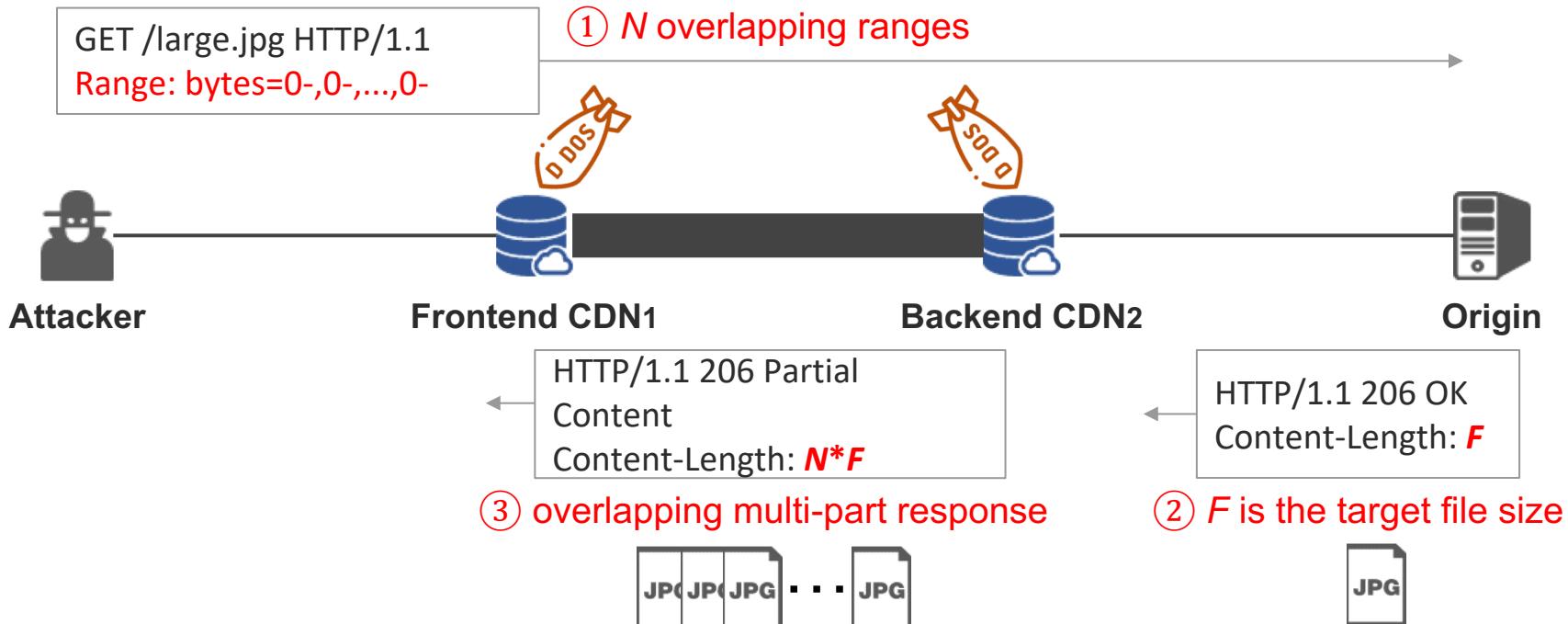
Overlapping Byte Ranges (OBR) Attack

- ❖ 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

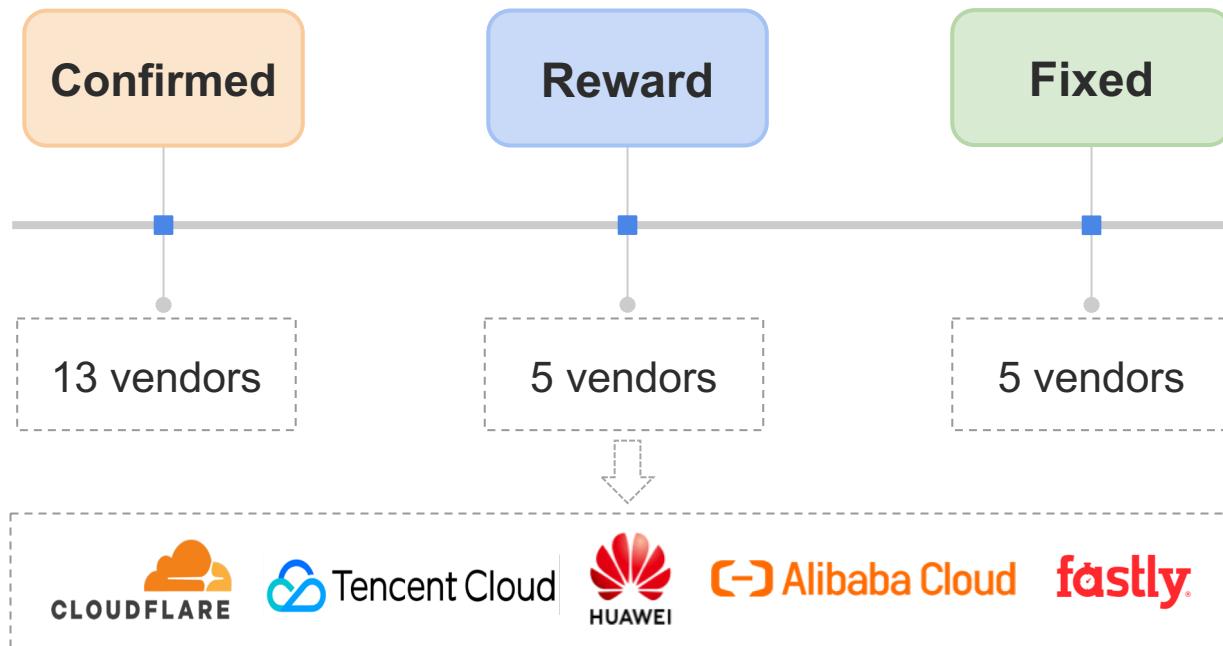
- ❖ Totally 11 combinations of cascaded CDNs are affected.
 - The amplification factor far exceeds traditional attack methods.

FCDN	BCDN	Traffic from Origin 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.

CDN

Adopt a secure Expansion policy

Coalesce or reject overlapping ranges

Add RangeAmp detection

Website

Check its hosting CDN vulnerable or not

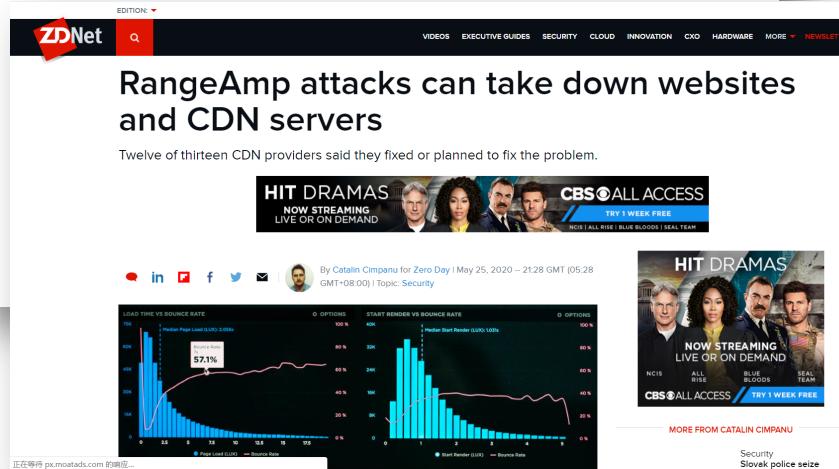
Block traffic from CDN

Media Coverage

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



GovCERT.HK
Weekly IT Security News Bulletin, 2020-W22
25 May – 31 May 2020



RangeAmp attacks can take down websites and CDN servers

Twelve of thirteen CDN providers said they fixed or planned to fix the problem.

HIT DRAMAS NOW STREAMING LIVE OR ON DEMAND CBS ALL ACCESS TRY 1 WEEK FREE

By Catalin Cimpanu for Zero Day | May 25, 2020 – 21:28 GMT (05:28 GMT+08:00) | Topic: Security

LOAD TIME VS SOURCE RATE

START RENDER VS BOUNCE RATE

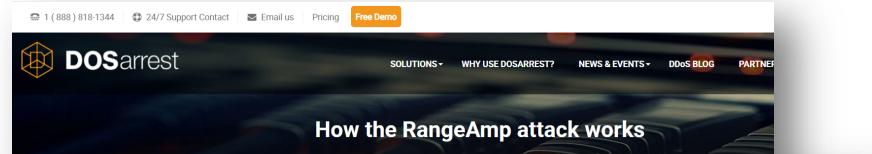
57.1%

NOCIS ALL RISE BLUE BLOODS SEAL TEAM

MORE FROM CATALIN CIMPANU

Security Slovak police seize

正在等待 px.moatads.com 的响应...



1 (888) 818-1344 24/7 Support Contact Email us Pricing Free Demo

DOSarrest

SOLUTIONS WHY USE DOSARREST? NEWS & EVENTS DDOS BLOG PARTNER

How the RangeAmp attack works



LATEST NEWS RBA to build 'data bunker' to safeguard payments system from outages Fisher & Paykel Appliances struck by Neftilm ransomware Lion accidentally directs milk orders to Sydney IT security consultancy Flinders Uni taps Worldpay in HR overhaul TSMC says unable to say

RangeAmp attacks turn CDNs into giant DoS cannons

By Juha Saarinen May 26 2020 10:14PM

No botnet needed, just a laptop.

RangeAmp attacks turn CDNs into giant DoS cannons

Chinese researchers have outlined a way to abuse small requests to web servers hosted through content delivery networks that allows attackers to generate DDoS attacks.

Named RangeAmp [pdf] the attack exploits the hyper text transfer protocol (HTTP) Range Requests attribute to ask for a random, small amount of data from a large file on a server, like a byte out of gigabyte and terabyte sized resources.

Since a CDN is unlikely to have the small amount of data cached, it will have to request the entire large file from the origin server it is stored on, just to serve up a byte of it.

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

