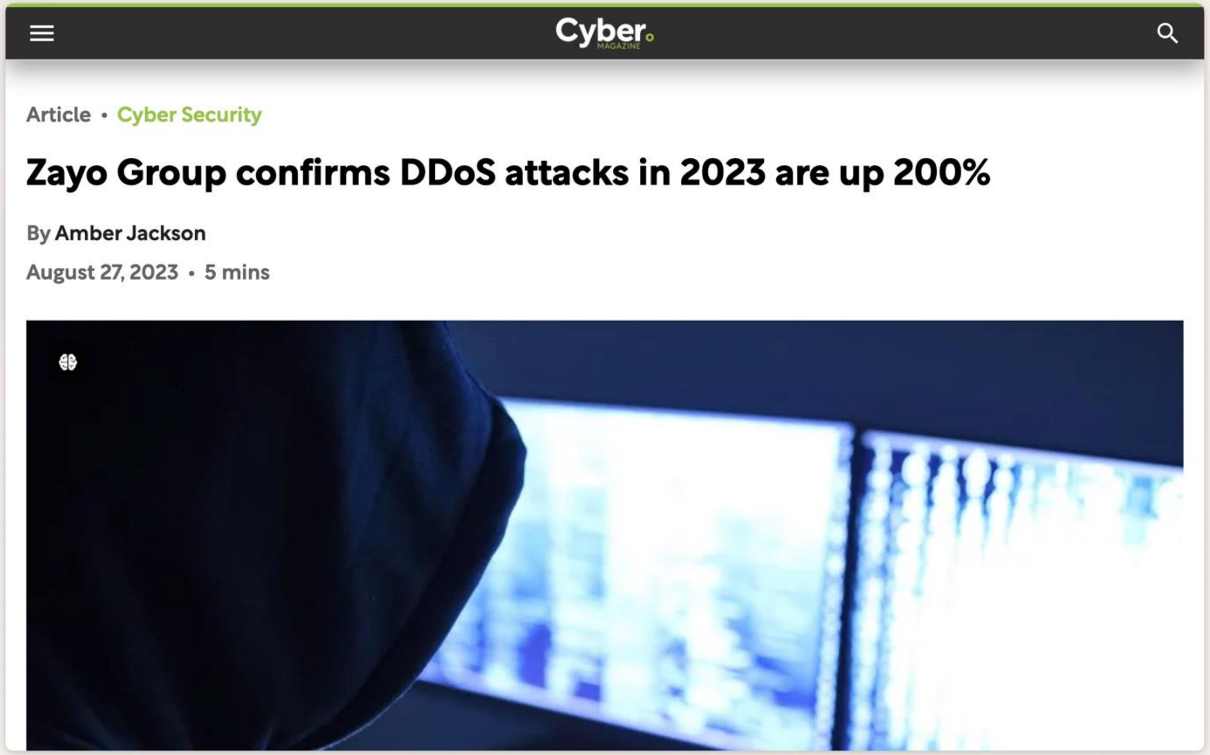
# CDN Cannon: Exploiting CDN Back-to-Origin Strategies for Amplification Attacks

**Ziyu Lin**, Zhiwei Lin, Ximeng Liu,
Jianjun Chen, Run Guo, Cheng Chen
Shaodong Xiao

福州大学 FUZHOU UNIVERSITY 四川大學 SICHUAN UNIVERSITY 清華大學 Tsinghua University

# Increased Risk of DDoS Attacks

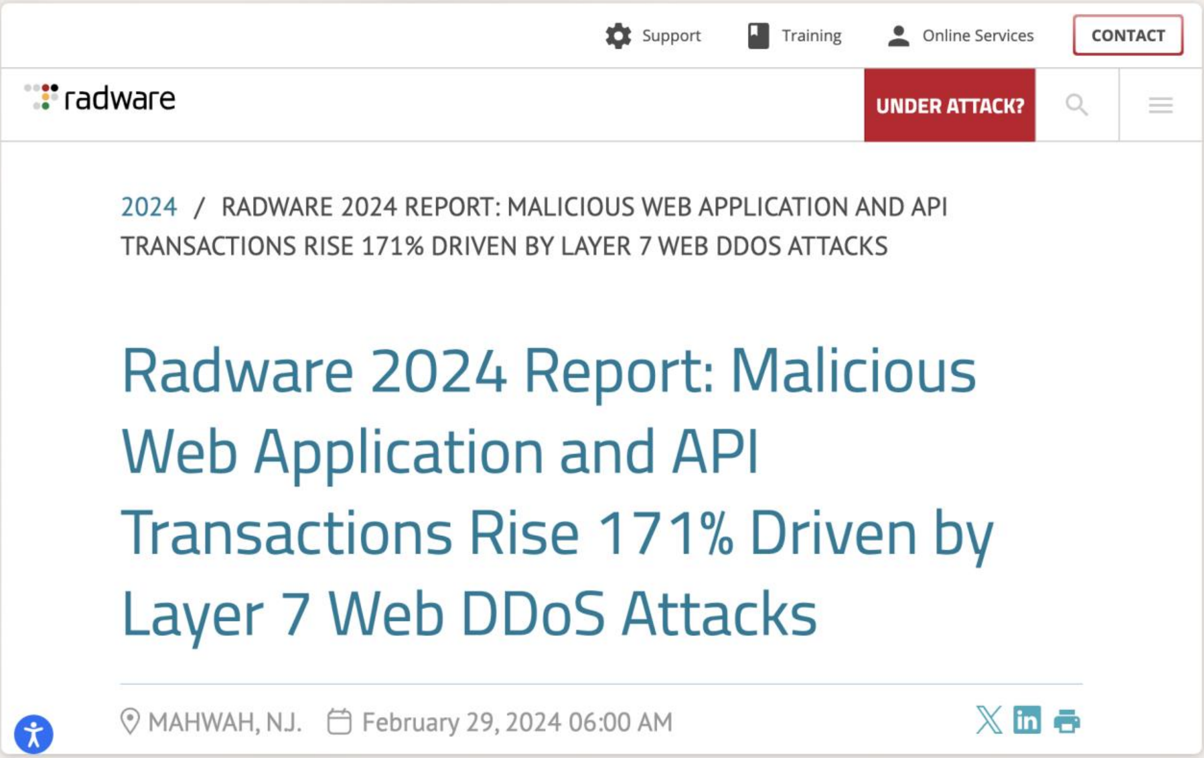


Article • Cyber Security

Zayo Group confirms DDoS attacks in 2023 are up 200%

By Amber Jackson

August 27, 2023 • 5 mins



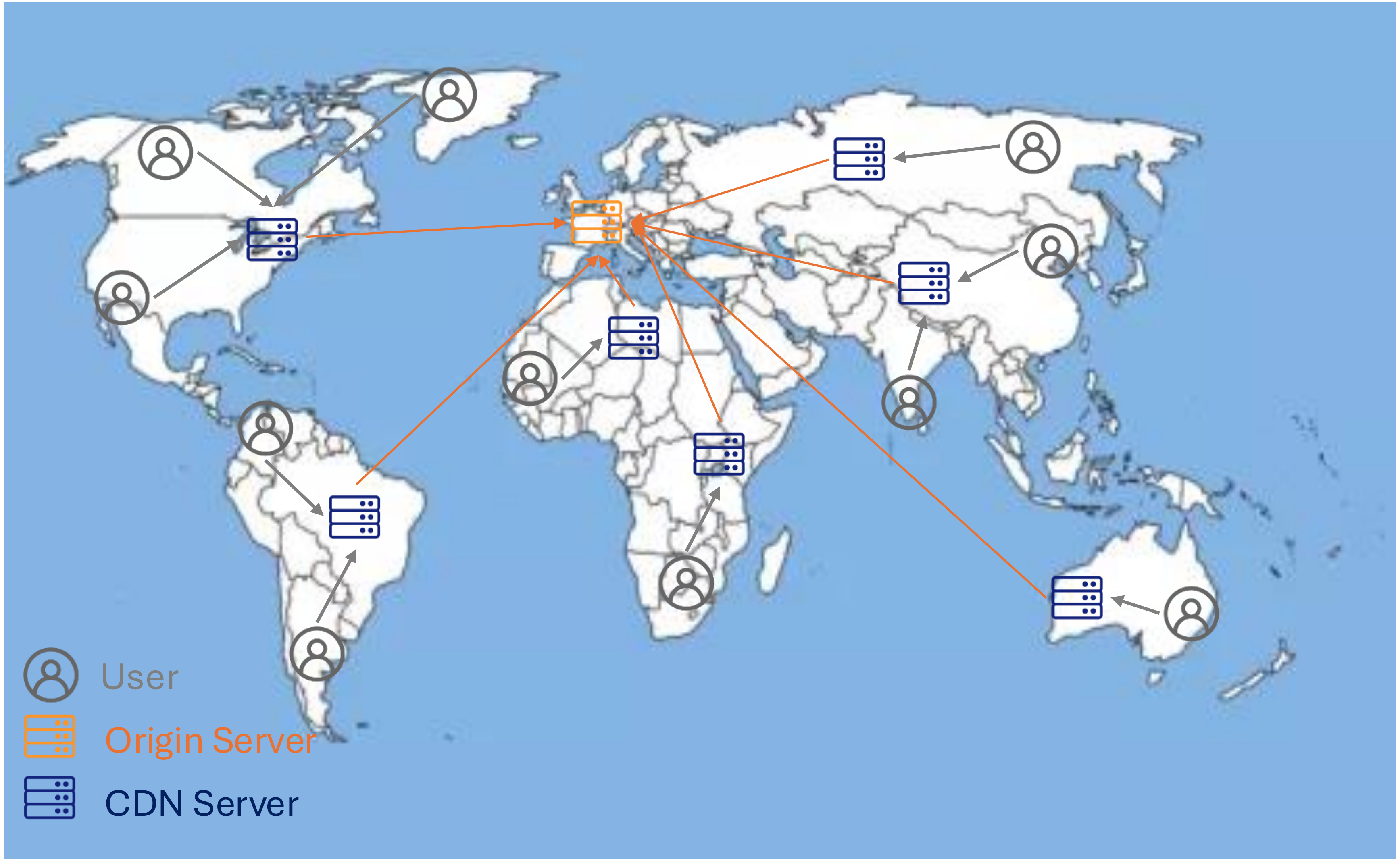
2024 / RADWARE 2024 REPORT: MALICIOUS WEB APPLICATION AND API TRANSACTIONS RISE 171% DRIVEN BY LAYER 7 WEB DDOS ATTACKS

Radware 2024 Report: Malicious Web Application and API Transactions Rise 171% Driven by Layer 7 Web DDoS Attacks

MAHWAH, NJ. February 29, 2024 06:00 AM

**DDoS attack cause websites reputation and monetary loss**

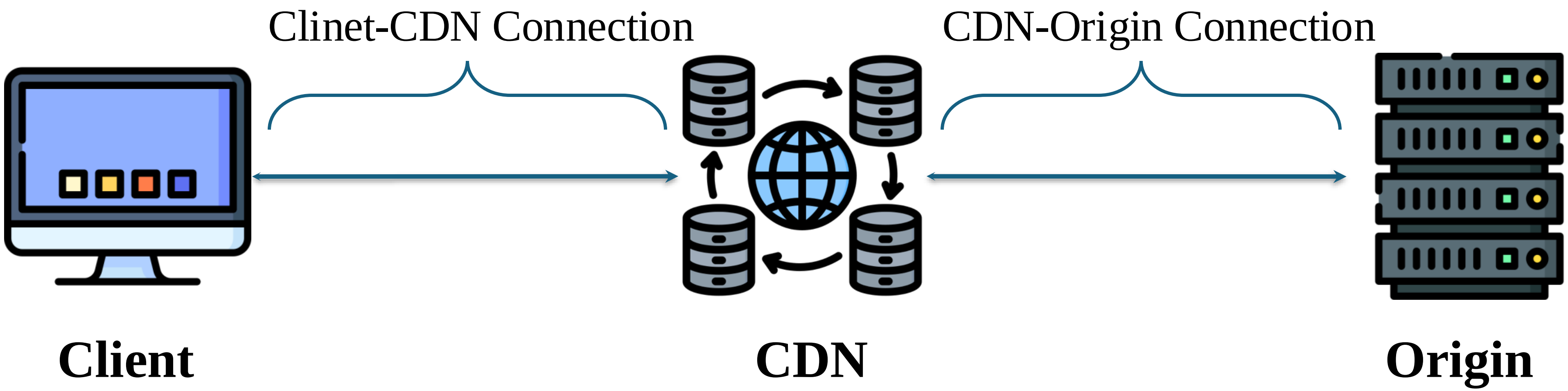
# CDN: Primary Solution for DDoS Defense



**The CDN-protected websites cannot be easily DDoSed**

# Content Delivery Network

- ❖ Infrastructure for access acceleration and DDoS defense.
  - ➢ 61.86% of Alexa Top 10K websites is hosted by a CDN[1]
  - ➢ Traditional DDoS attacks are ineffective against the CDN-protected websites.

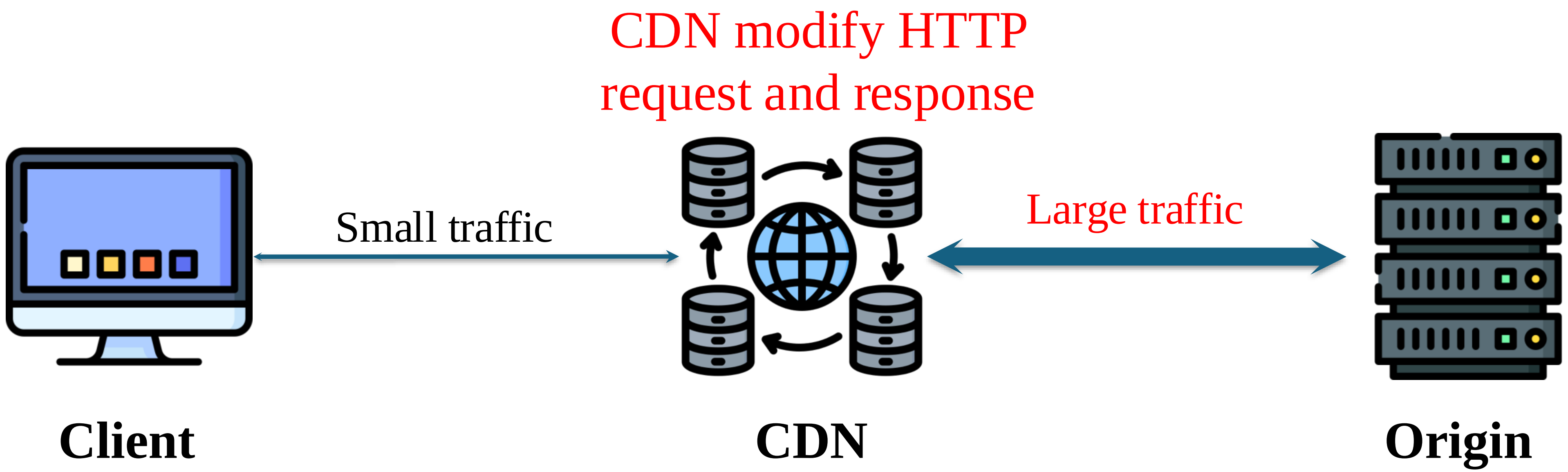


[1] https://trends.builtwith.com/CDN/Content-Delivery-Network

# Back-to-Origin Strategies

❖ Designed to improve Web access and Compatibility.

- ➢ Reduce web access latency
- ➢ Improve compatibility with origin and client



CDN modify HTTP request and response

Small traffic

Large traffic

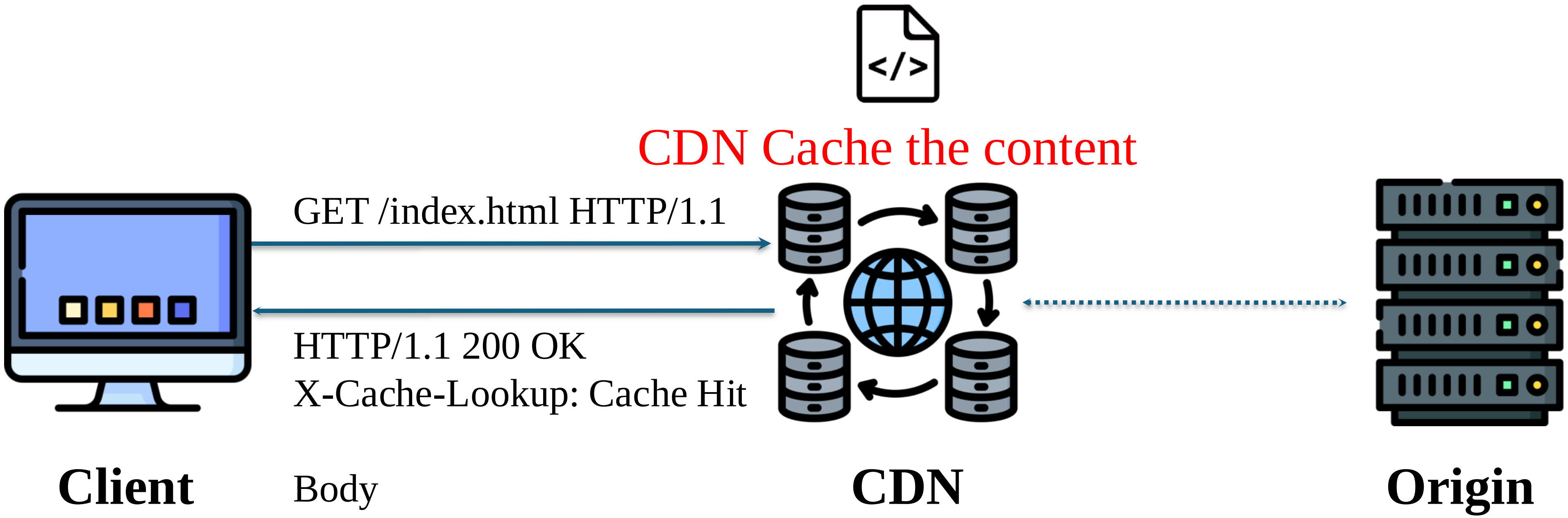
Client

CDN

Origin

# Back-to-Origin Strategies

- ❖ Designed to improve the cache hit rate.
  - ➢ Reduce the burden on the origin server
  - ➢ Speed up the response



CDN Cache the content

GET /index.html HTTP/1.1

HTTP/1.1 200 OK
X-Cache-Lookup: Cache Hit

Body

# Our Work

- Exploiting CDN Back-to-Origin Strategies to attack the origin

| | |
|---|---|
| BtOAmp | Image Optimization attack |
| | Request Modification attack |
| | Method Conversion attack |
| | Connection Decoupling attack |

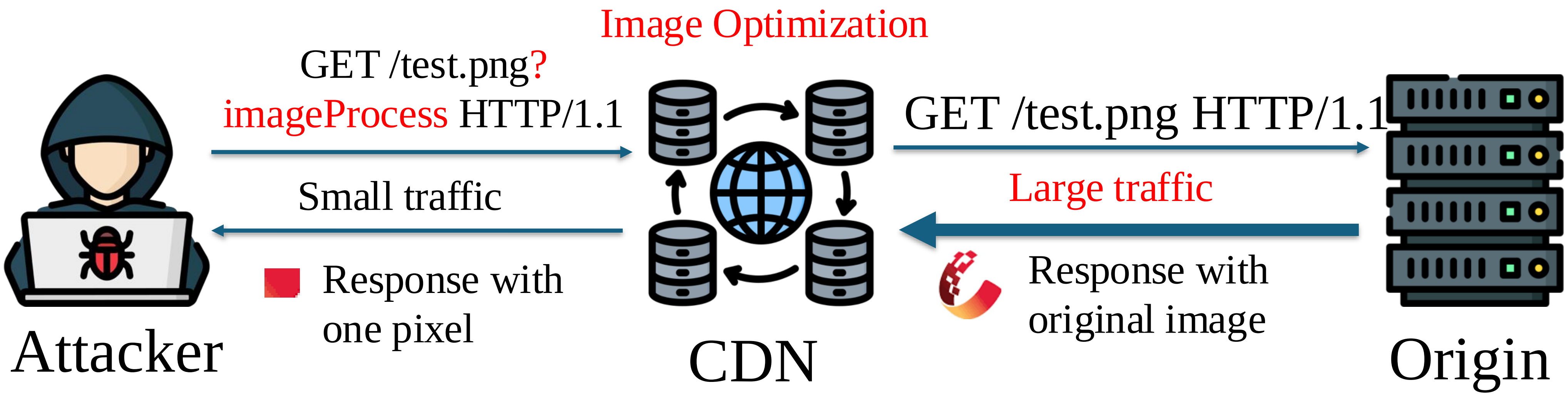
- Performed real-world evaluations on fourteen CDN vendors

# Image Optimization Attack: Root Cause

- Multiple formats and high-resolution images are becoming more and more used in web pages, but these large-sized images greatly delay web access.
- CDN vendors design a series of strategies for optimizing the transmission of image.
    - Format Conversion
    - Image Cropping
- CDN vendors do not impose limitations on the parameters of Image Optimization Strategies.

# Image Optimization Attack: Threat Model

- CDN adopts the query’s parameters to handle the image request.
  - When a CDN receives a request with image optimization parameters, it fetches the original image from the origin. CDN crop the image accordingly and returns it to the client.



# Image Optimization Attack: Damage Trend

- The amplification factor is higher for images with higher quality. (Format Conversion )
  - File Size ~ Amplification
  - BMP/TIFF ~ 1,011
- The amplification factor is higher for images with higher resolution. (Image Cropping)
  - File Size ~ Amplification
  - 720p ~ 1,628
  - 4320p ~ 39,000

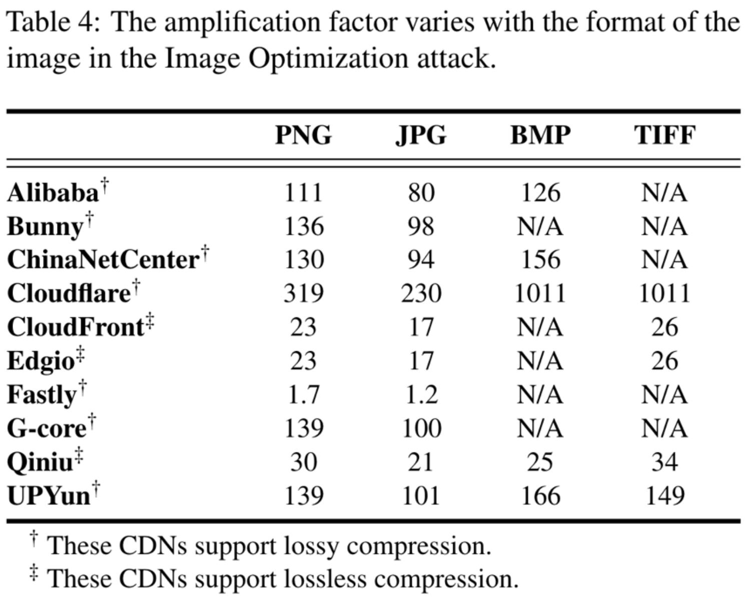


Table 4: The amplification factor varies with the format of the image in the Image Optimization attack.

| | PNG | JPG | BMP | TIFF |
|---|---|---|---|---|
| **Alibaba**[†] | 111 | 80 | 126 | N/A |
| **Bunny**[†] | 136 | 98 | N/A | N/A |
| **ChinaNetCenter**[†] | 130 | 94 | 156 | N/A |
| **Cloudflare**[†] | 319 | 230 | 1011 | 1011 |
| **CloudFront**[‡] | 23 | 17 | N/A | 26 |
| **Edgio**[‡] | 23 | 17 | N/A | 26 |
| **Fastly**[†] | 1.7 | 1.2 | N/A | N/A |
| **G-core**[†] | 139 | 100 | N/A | N/A |
| **Qiniu**[‡] | 30 | 21 | 25 | 34 |
| **UPYun**[†] | 139 | 101 | 166 | 149 |

[†] These CDNs support lossy compression.

[‡] These CDNs support lossless compression.

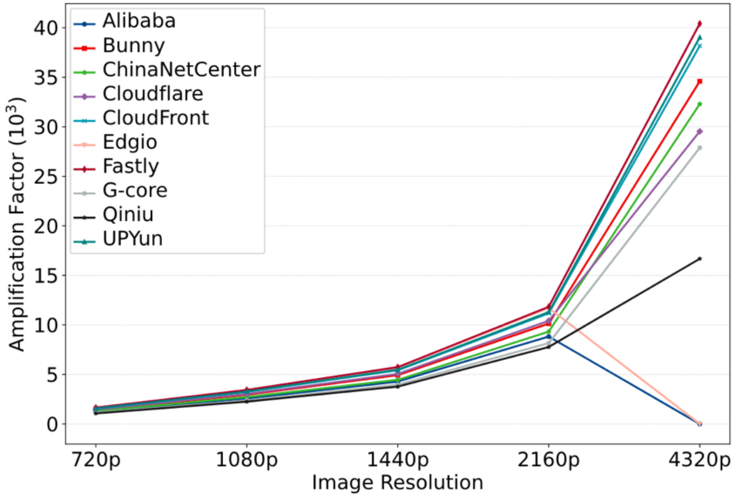
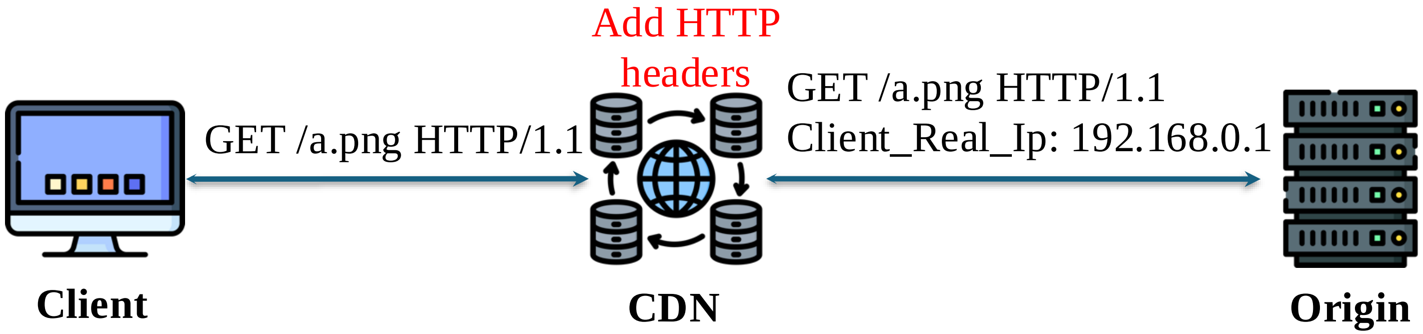
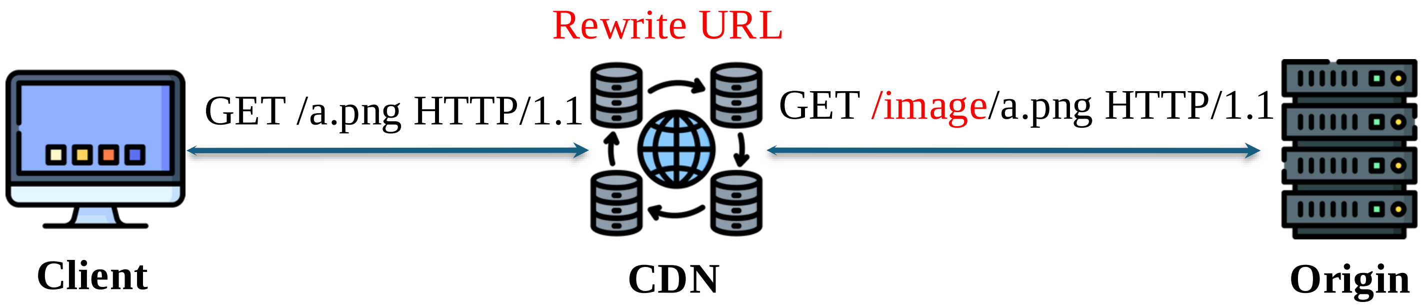


Figure 4: How the amplification factor changes with the resolution of images.

# Request Modification Attack: Root Cause

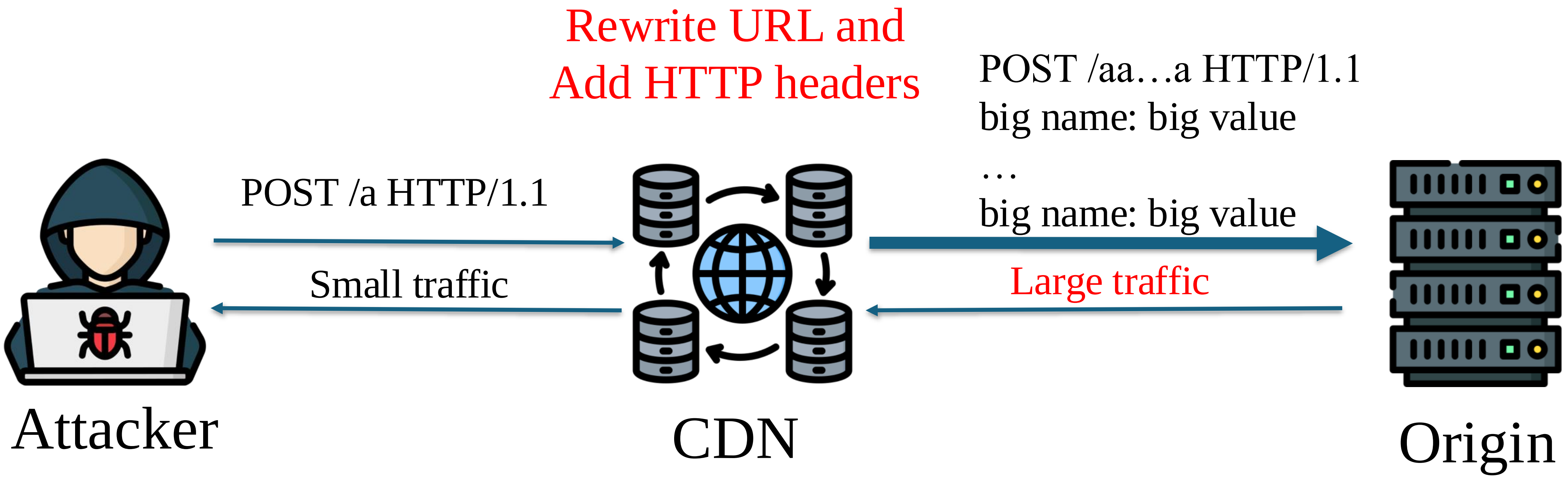
- To meet practical business needs, such as passing client IP to the origin server or handling file location changes in the origin.
- CDN needs to rewrite the URL or add an HTTP header when forwarding requests.
- CDN doesn’t impose limitations on the size of the modified request.





# Request Modification Attack: Threat Model

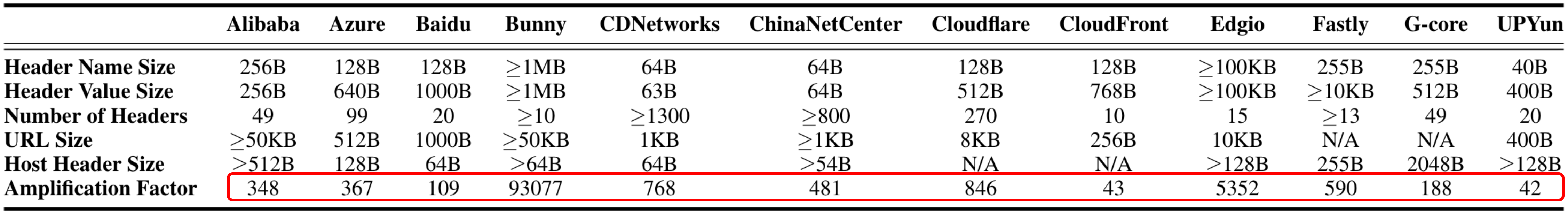
- Step1: Deploy victim’s website on CDN
- Step2: Configure the request modification strategy
- Step3: Send a lot of HTTP requests



# Request Modification Attack: Damage Trend

- The amplification factor increases with the URL size and HTTP header size.
  - ➢ Max Amplification Factor ~ 93,000
  - ➢ Header Name Size ~ 1MB
  - ➢ Header Value Size ~ 1MB
  - ➢ URL Size ~ 50KB
  - ➢ Host Header Size ~ 64B

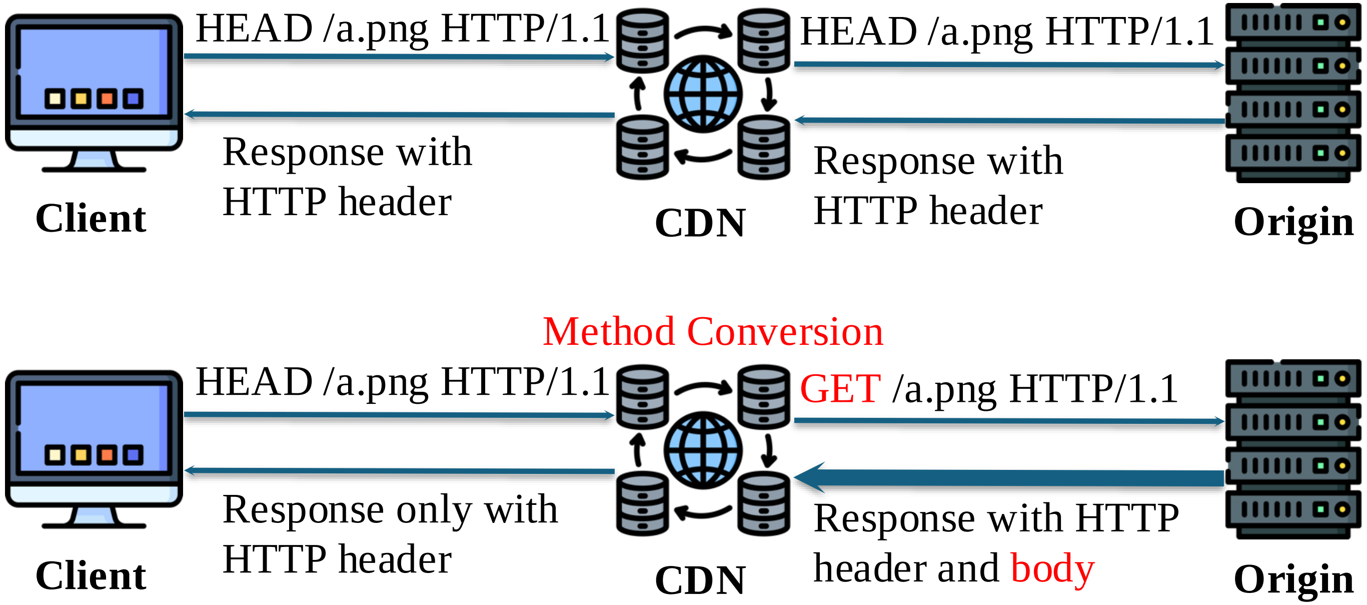
Table 5: The amplification factor in Request Modification attack.



| | Alibaba | Azure | Baidu | Bunny | CDNetworks | ChinaNetCenter | Cloudflare | CloudFront | Edgio | Fastly | G-core | UPYun |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Header Name Size** | 256B | 128B | 128B | ≥1MB | 64B | 64B | 128B | 128B | ≥100KB | 255B | 255B | 40B |
| **Header Value Size** | 256B | 640B | 1000B | ≥1MB | 63B | 64B | 512B | 768B | ≥100KB | ≥10KB | 512B | 400B |
| **Number of Headers** | 49 | 99 | 20 | ≥10 | ≥1300 | ≥800 | 270 | 10 | 15 | ≥13 | 49 | 20 |
| **URL Size** | ≥50KB | 512B | 1000B | ≥50KB | 1KB | ≥1KB | 8KB | 256B | 10KB | N/A | N/A | 400B |
| **Host Header Size** | >512B | 128B | 64B | >64B | 64B | >54B | N/A | N/A | >128B | 255B | 2048B | >128B |
| **Amplification Factor** | 348 | 367 | 109 | 93077 | 768 | 481 | 846 | 43 | 5352 | 590 | 188 | 42 |

# Method Conversion Attack: Root Cause

- The HEAD request does not return the body of the response, only the response header.
- To improve cache rate, CDN converts the HEAD request to GET request.
- Method Conversion strategy can cause a huge difference in traffic in the Client-CDN and CDN-Origin connection.



Client

HEAD /a.png HTTP/1.1

Response with HTTP header

CDN

HEAD /a.png HTTP/1.1

Response with HTTP header

Origin

Method Conversion

Client

HEAD /a.png HTTP/1.1

Response only with HTTP header

CDN

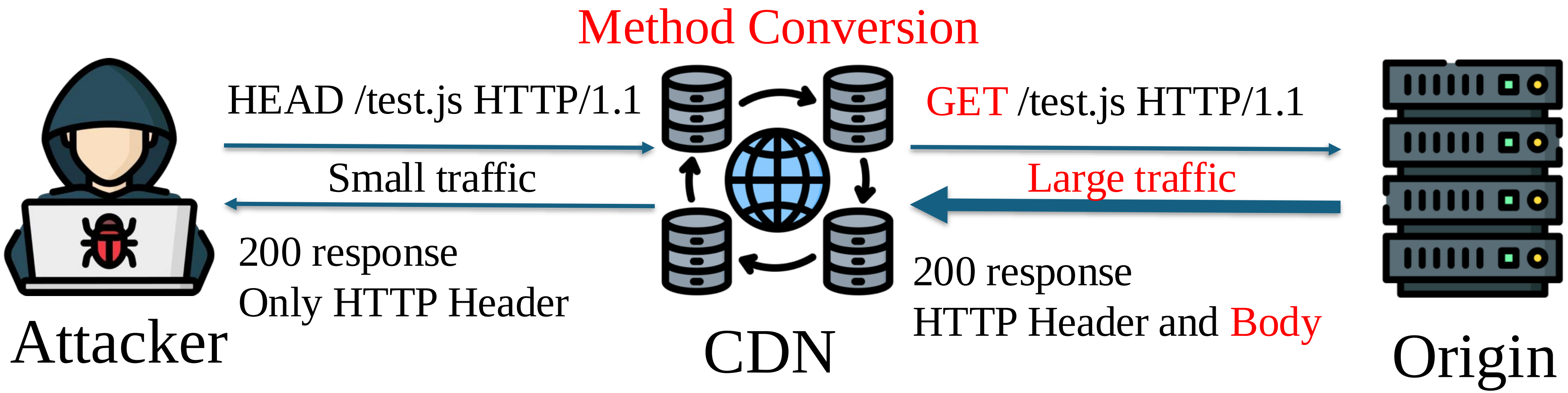
GET /a.png HTTP/1.1

Response with HTTP header and body

Origin

# Method Conversion Attack: Threat Model

- CDN converts the HEAD request to GET request
  - To improve cache rate, when the CDN receives a HEAD request, it thinks your next request will be a GET request, so it converts the HEAD request to a GET request.



# Method Conversion Attack: Damage Trend

- The amplification factor increase with the size of the target resource
  - File Size ~ Amplification Factor
  - **1MB ~ 2,106**
  - **25MB ~ 53,000**

Table 8: Amplification factors with different target resource sizes of Method Conversion attacks.

| | **Amplification Factor** | | |
|---|---|---|---|
| | **1MB** | **10MB** | **25MB** |
| **Alibaba** | 1340 | 13059 | 33952 |
| **Bunny** | 1212 | 11808 | 30702 |
| **Cachefly** | 1738 | 16940 | 44044 |
| **CDNetworks** | 1744 | 16995 | 44115 |
| **ChinaNetCenter** | 1784 | 17418 | 45212 |
| **Cloudflare** | 1170 | 11385 | 29698 |
| **Fastly** | 469 | 469 | 469 |
| **G-core** | 2106 | 20520 | 53352 |

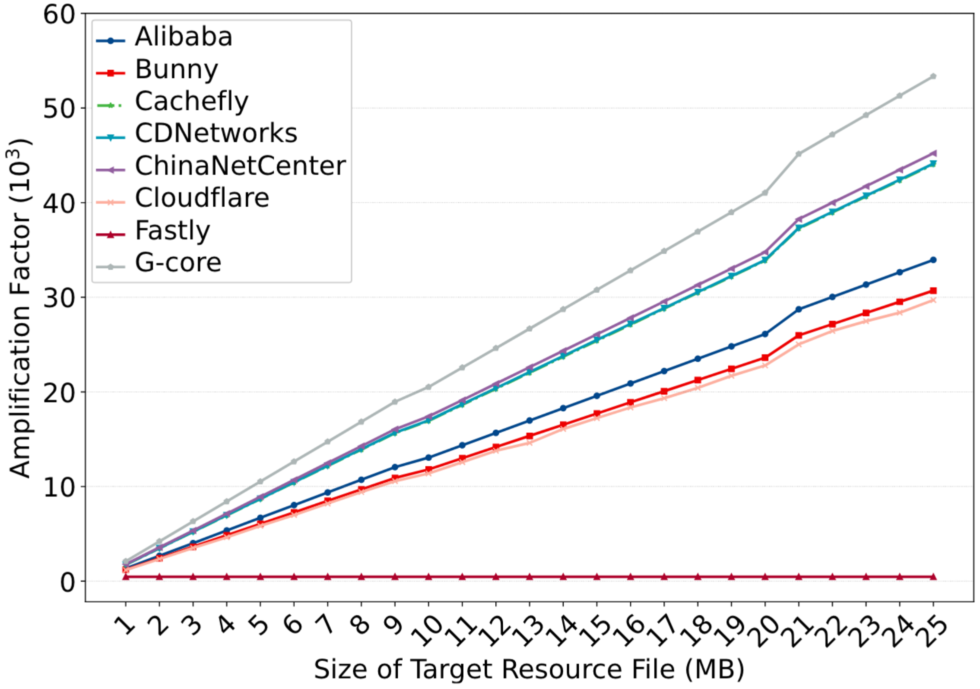
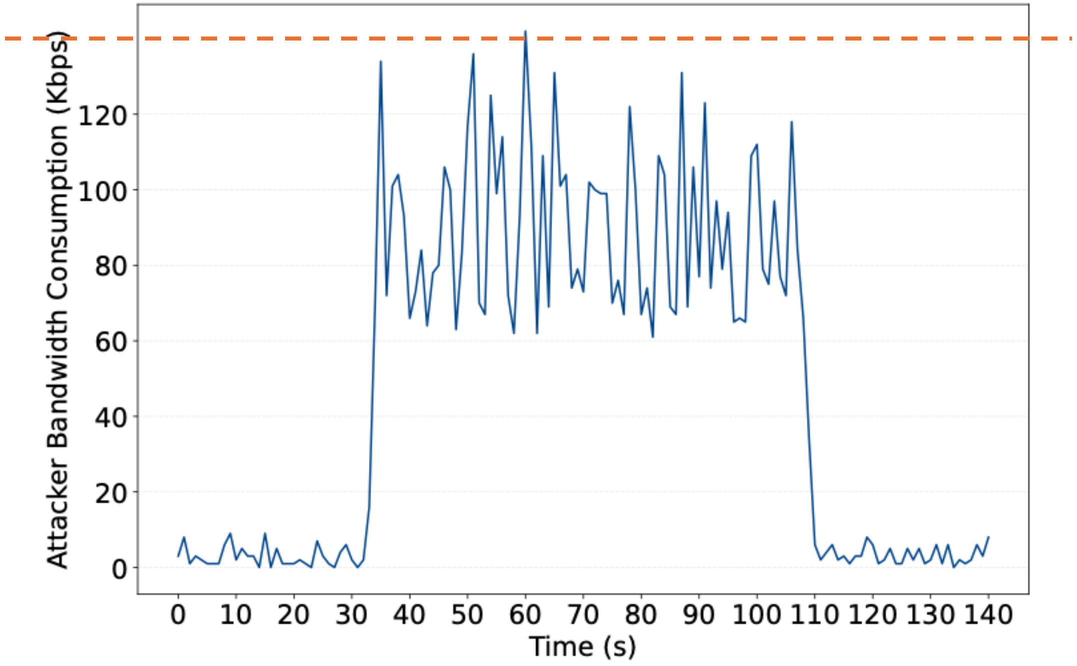


Figure 7: How does the Method Conversion attack amplification factor change with the size of a target resource file.

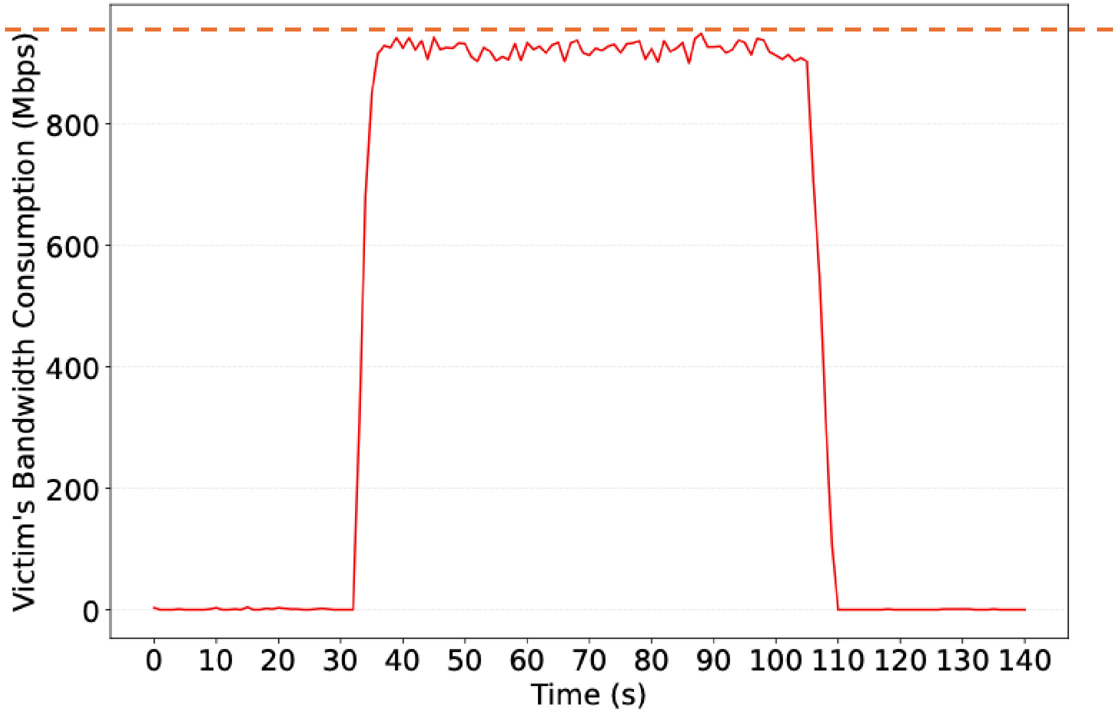
# Real-world Evaluation:

- Experiment setup: origin server's bandwidth (1000Mbps)

Attacker: **Kb-level cost**



Victim: **Gb-level damage**

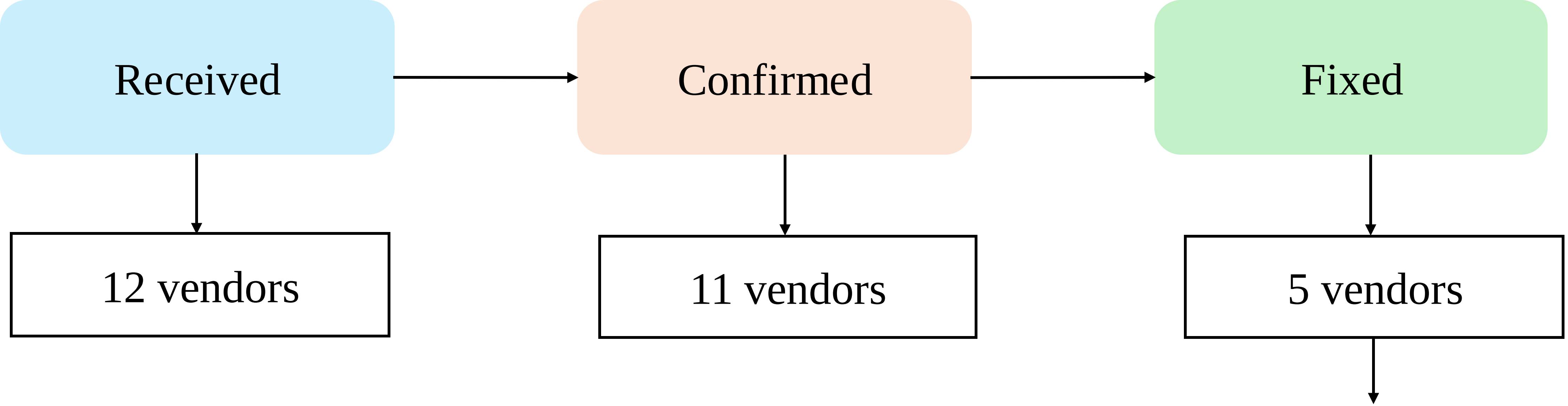


# Mitigation

- Limit parameters in the Back-to-Origin strategies
  - Impose limitations on parameters to prevent the traffic consumption gap between two connections.
- Validate the ownership of customer-supplied origin configuration
  - Stop CDN being abused to attack 3rd party targets
  - But Can still attack websites hosted on CDN
- Follow RFC standards for request forwarding
  - Directly forward HEAD request
- Synchronize client-CDN and CDN-origin connections
  - The CDN can keep connections for a few seconds and cut off if the client does not reconnect.

# Responsible Disclosure

- Response from affected CDN vendors.



Received

Confirmed

Fixed

12 vendors

11 vendors

5 vendors

- Other CDN vendors could also be affected!

Alibaba Cloud
CORE
ChinaNetCenter
QINIU
upyun

# Thank you for listening!
# Any question?