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

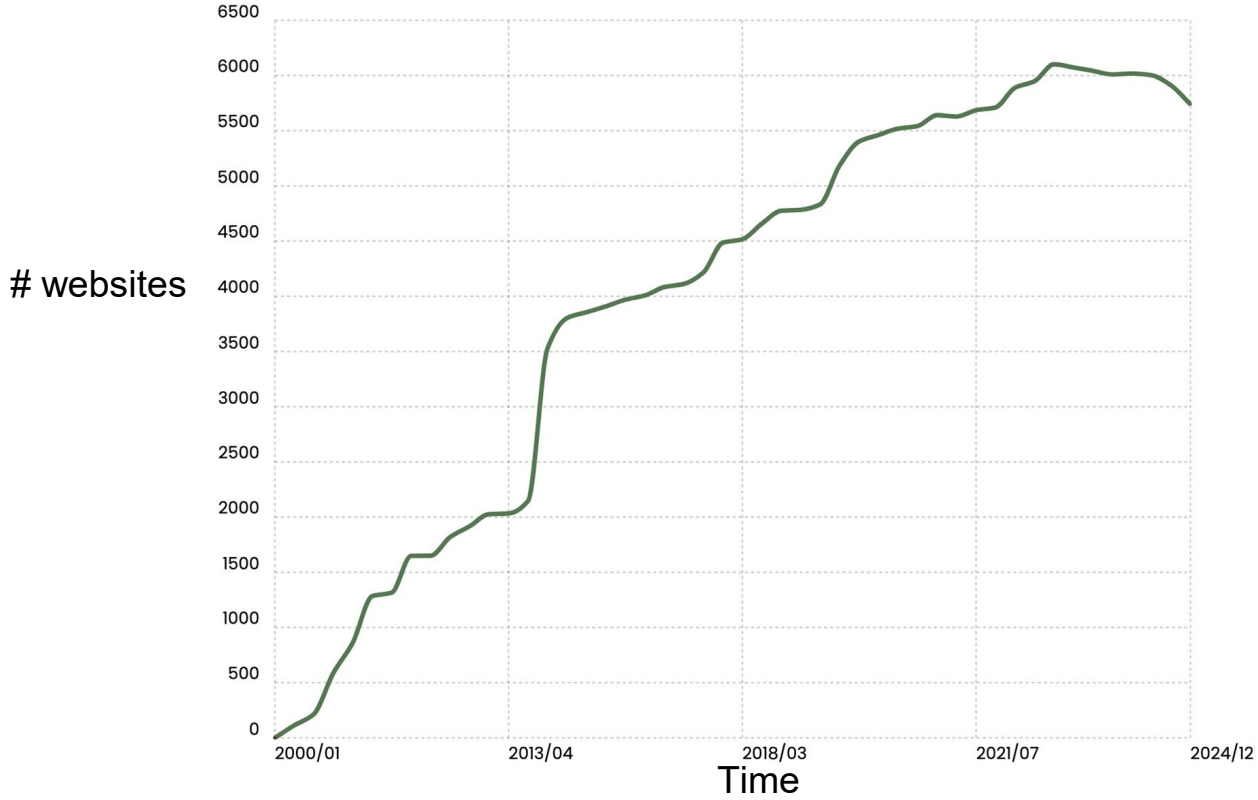
What is a Content Delivery Network (CDN)?

What is a Content Delivery Network (CDN)?

- Improve website load times
- Reduce bandwidth costs
- Provide DDoS defense

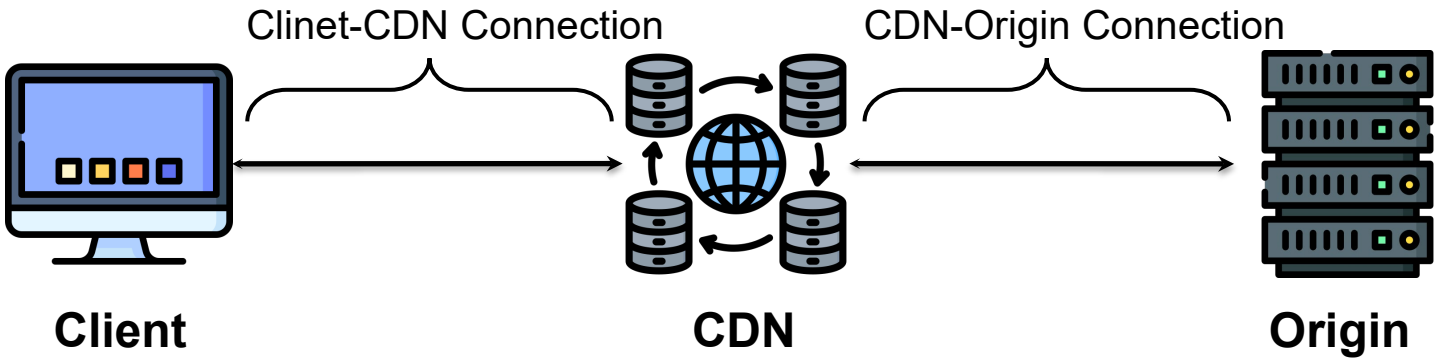
https://www.cloudflare.com/learning/cdn/what-is-a-cdn/

CDN Usage Statistics



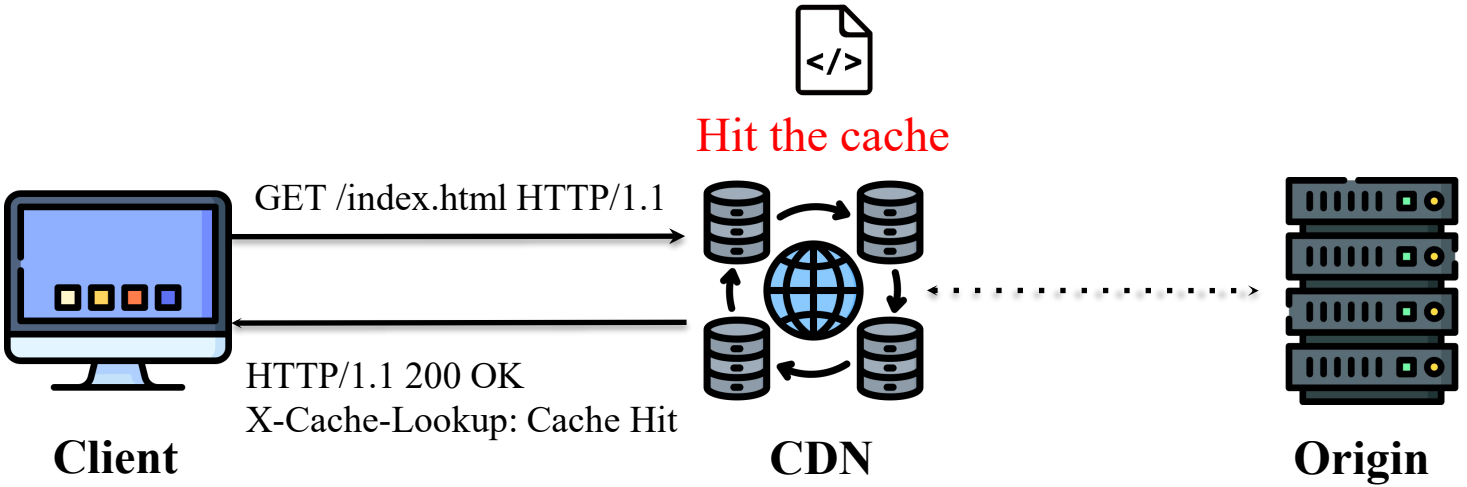
https://trends.builtwith.com/CDN/Content-Delivery-Network

How a CDN works?



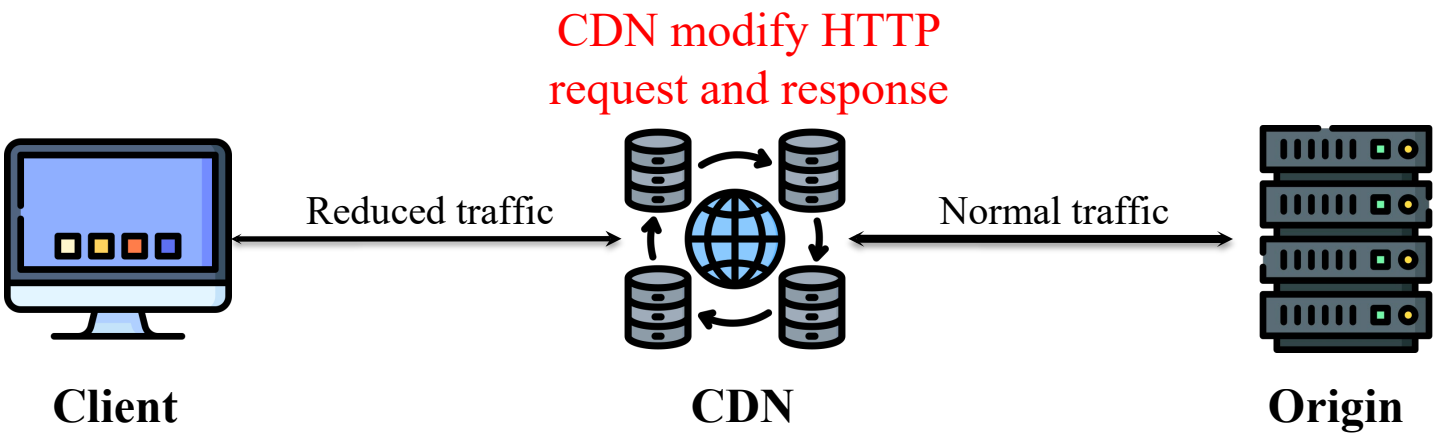
Back-to-Origin Strategies

Improve website load times



Back-to-Origin Strategies

Reduce bandwidth costs



BtOAmp Attacks

Image Optimization Strategies

Image Compression

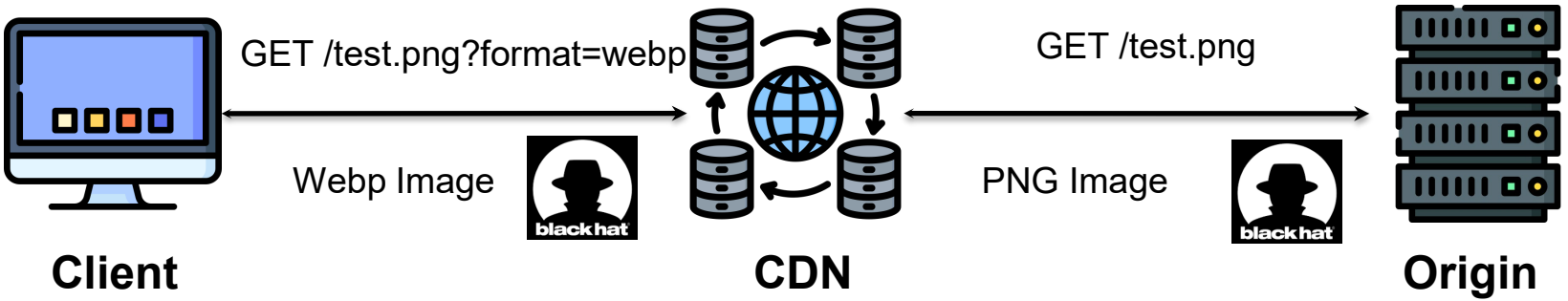


Image Optimization Strategies

Image Cropping

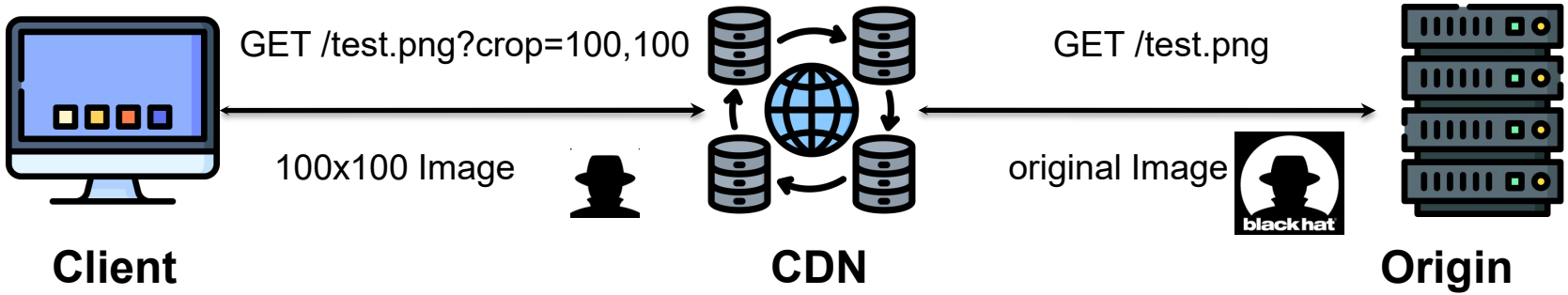
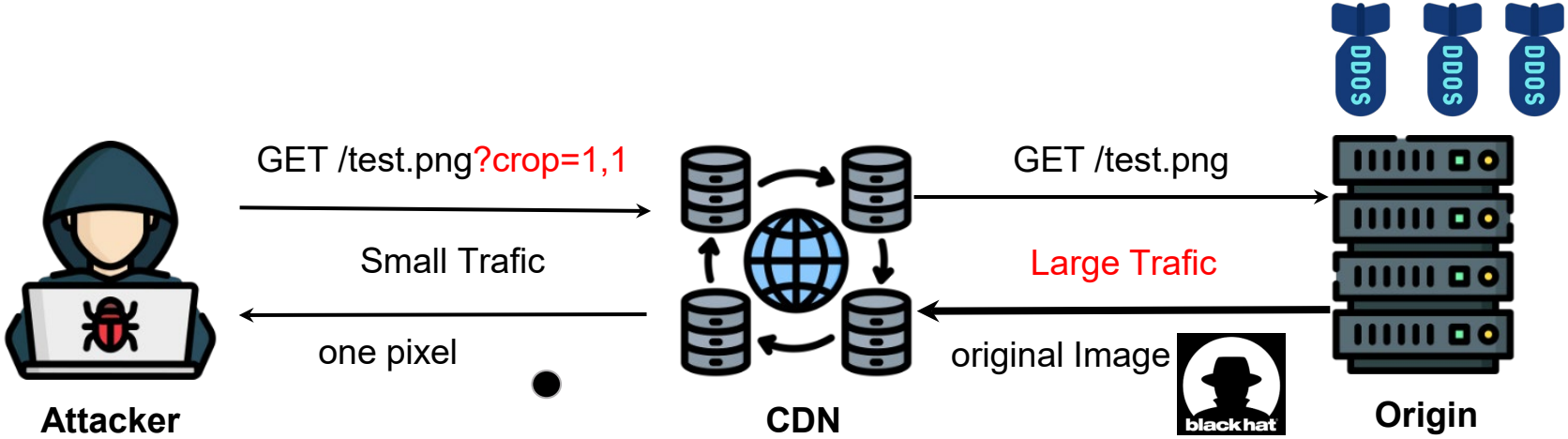
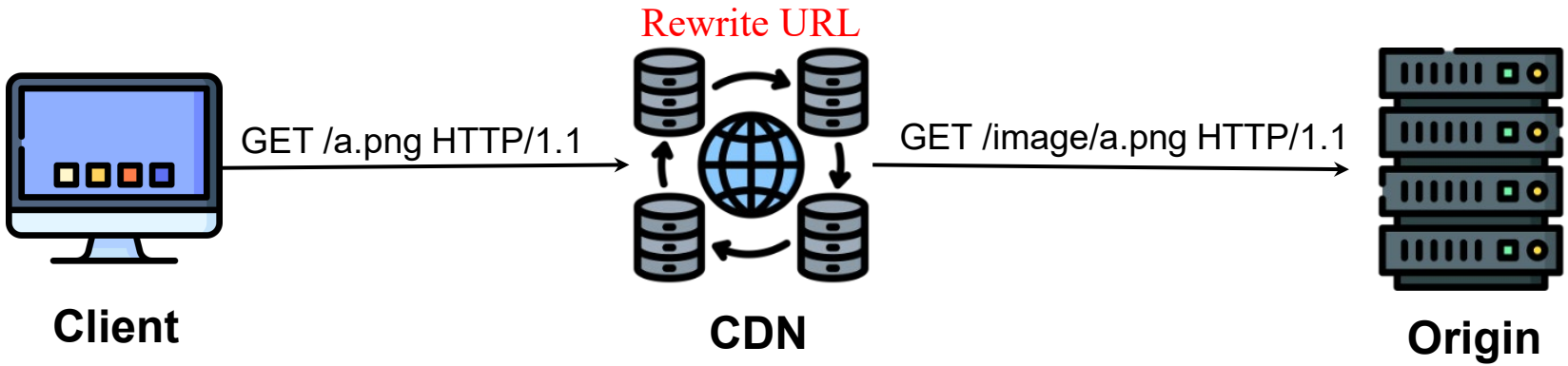


Image Optimization Attack



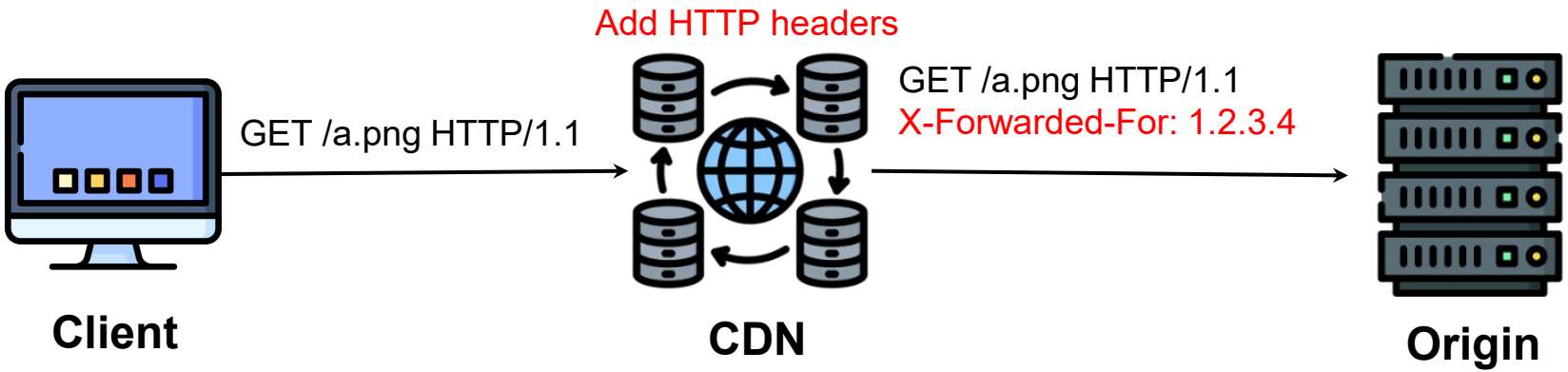
Request Modification Strategy

Rewrite URL



Request Modification Strategy

Modify request header



Request Modification Attack

(1) Deploy victim's website on CDN

Pull Zone Name

Required

blackhatasiaexample .b-cdn.net

The name and hostname of your Pull Zone where your files will be accessible.
(letters and numbers only)

Origin Type

Origin URL | Storage Zone

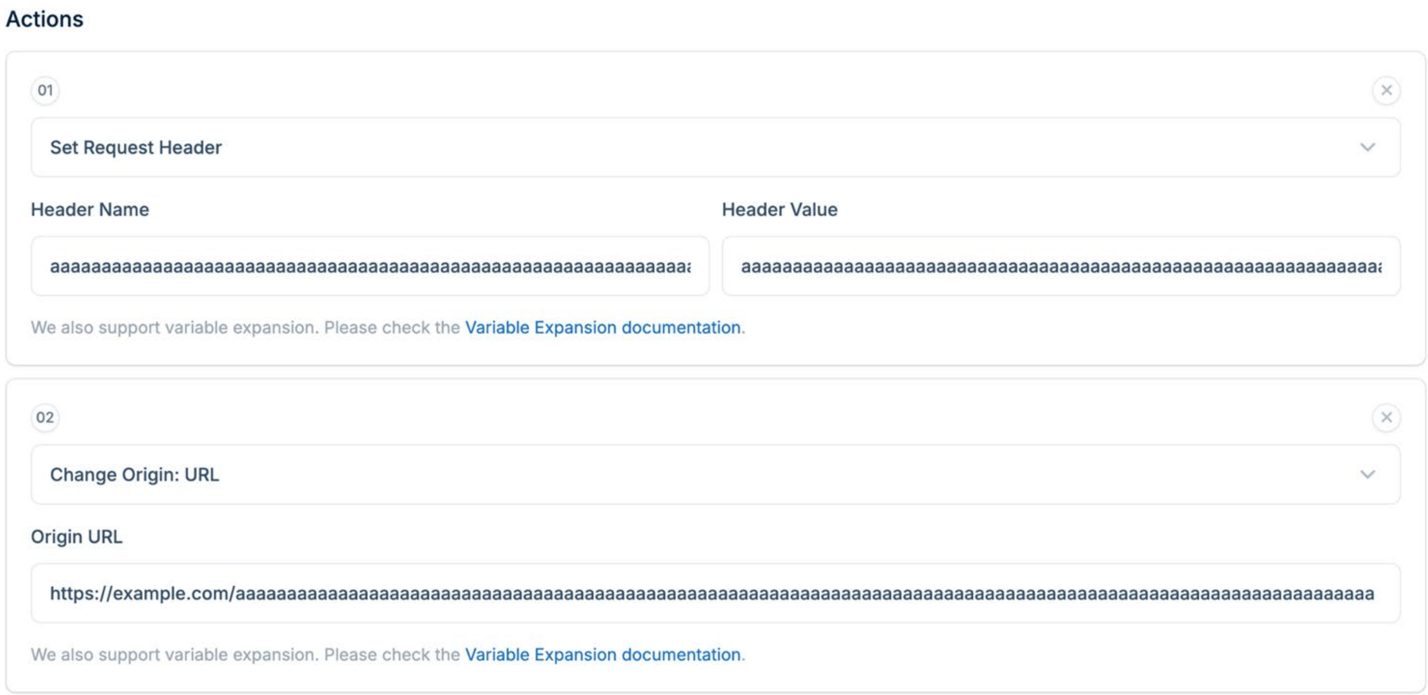
Origin URL

Required

victim.com

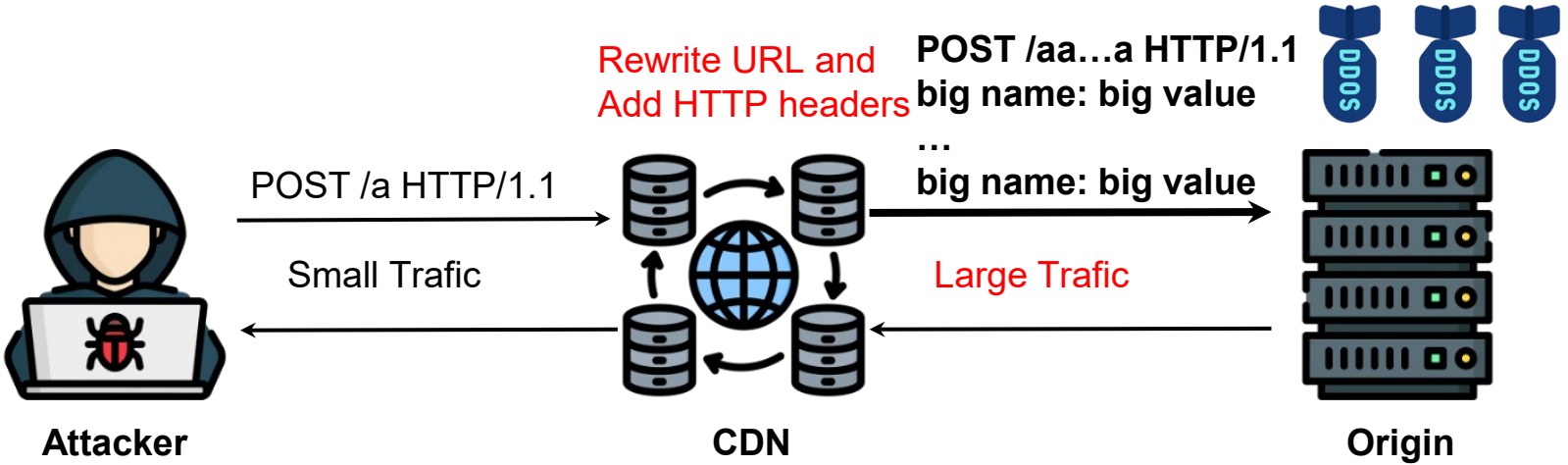
Request Modification Attack

(2) Configure the request modification strategy

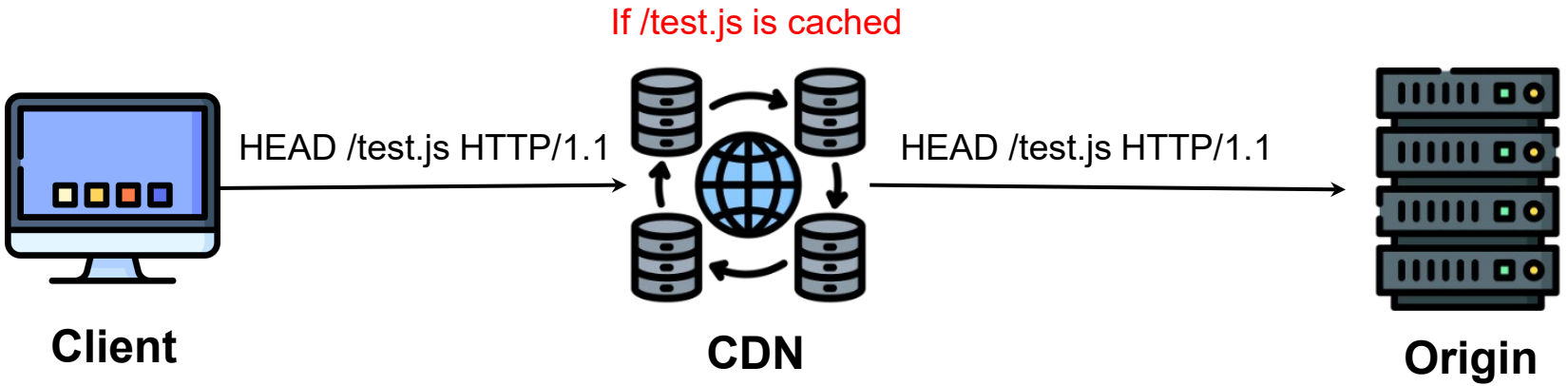


Request Modification Attack

(3) Send a lot of HTTP requests

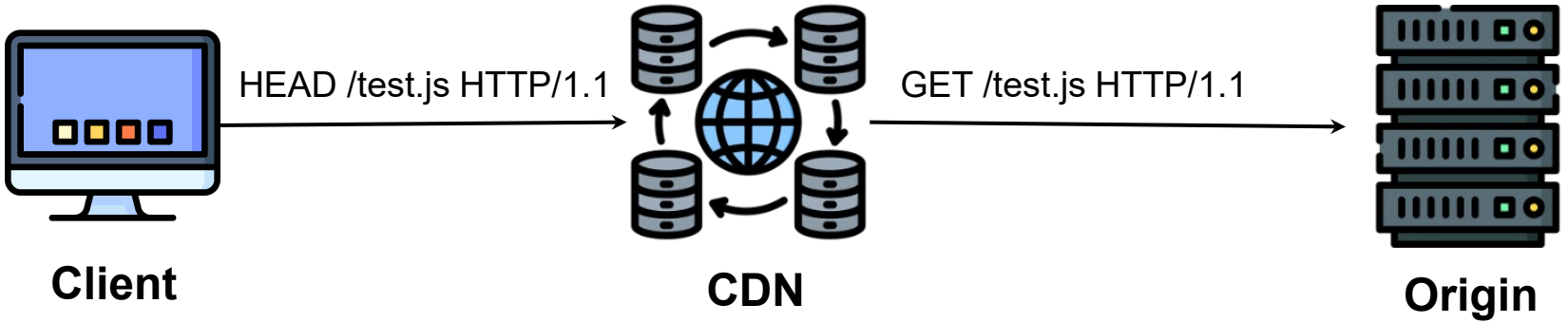


Method Conversion Strategy

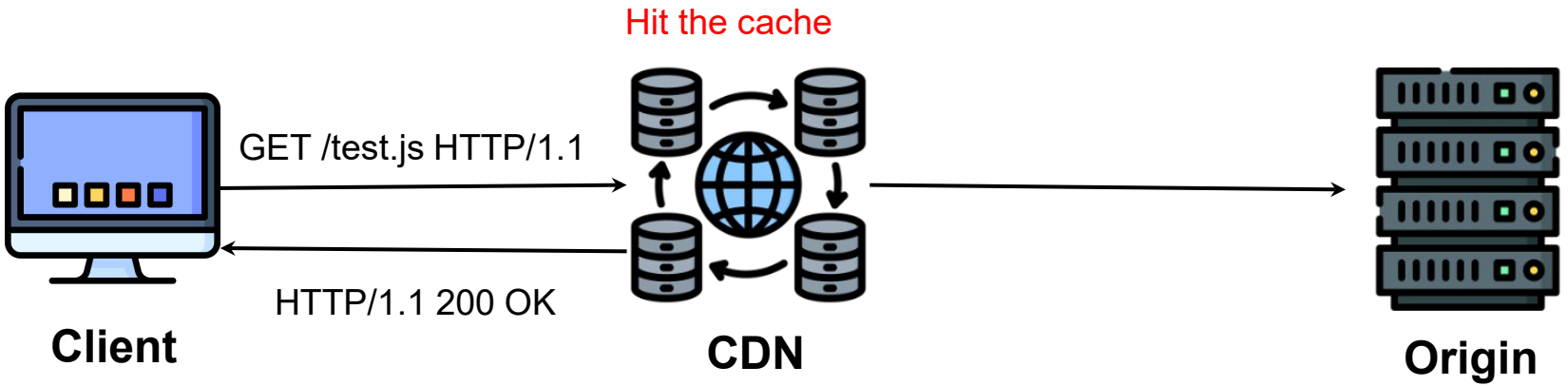


Method Conversion Strategy

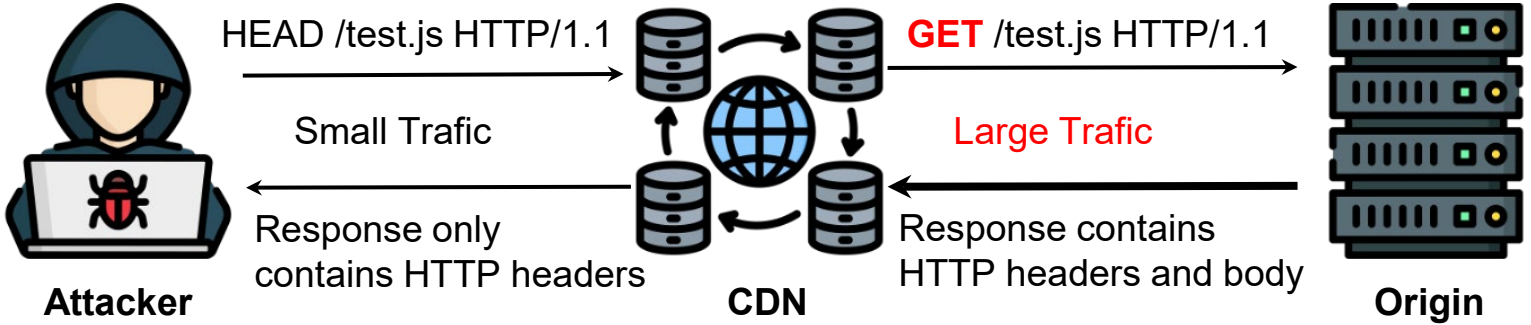
If /test.js is not cached



Method Conversion Strategy

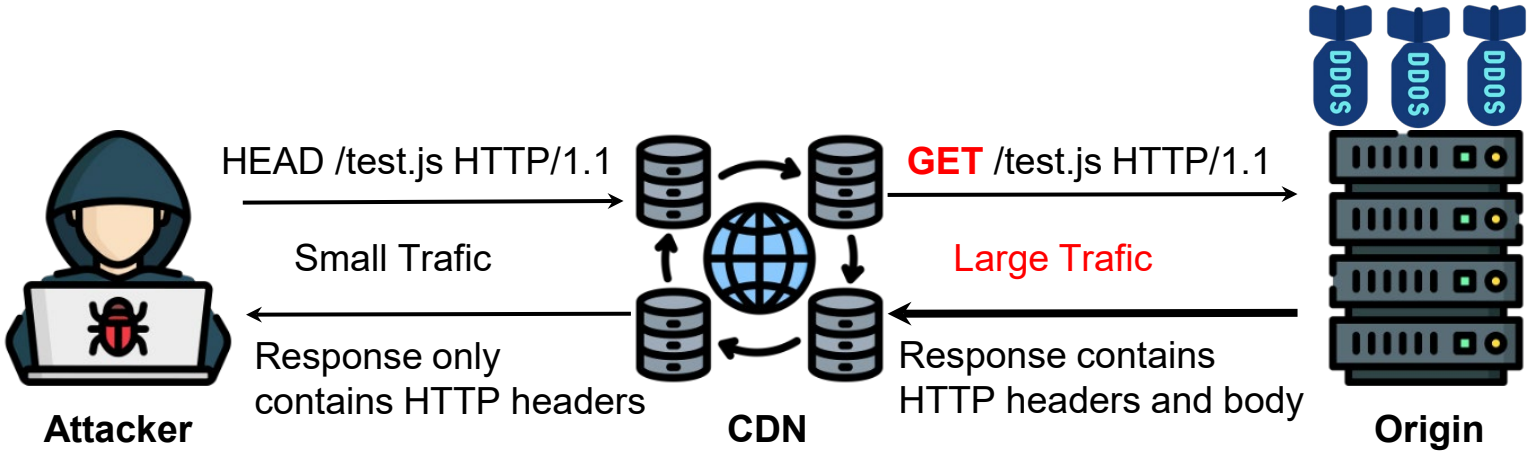


Method Conversion Attack



Method Conversion Attack

Send a lot of HTTP HEAD requests and Bypass the cache mechnisim



Evaluations

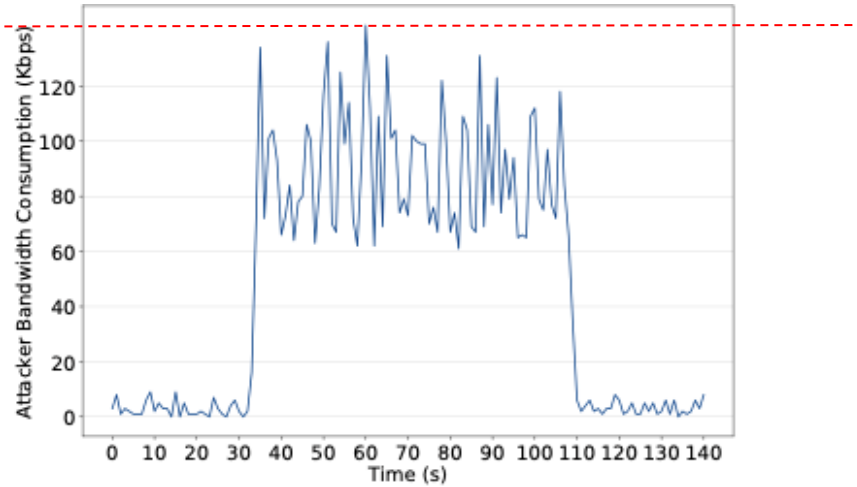
Real-world Evaluation

- The setup of victim server
  - An HTTP service(2.5GHz/2GB/1Gbps/Nginx 1.21.3) in Silicon Valley.
- The setup of attacker client
  - A ubuntu VPS (2.5GHz/2GB/30Mbps) in Singapore.

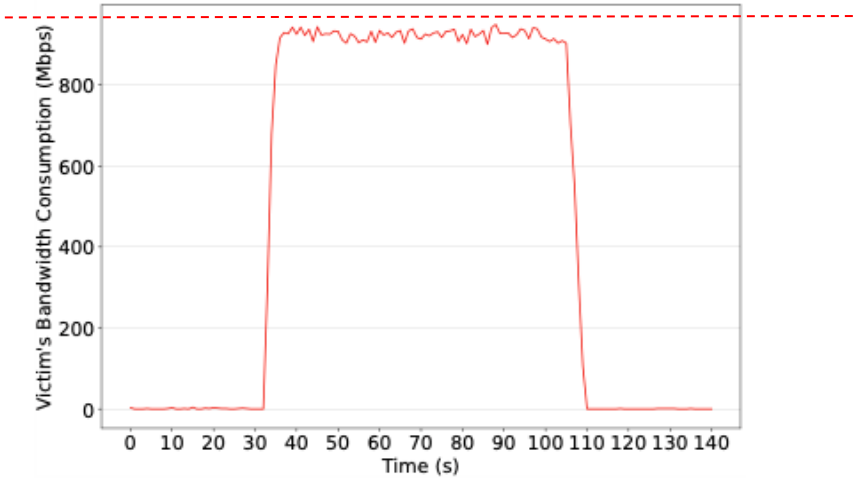
Real-world Evaluation

- Kb level can cost Gb level damage

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.

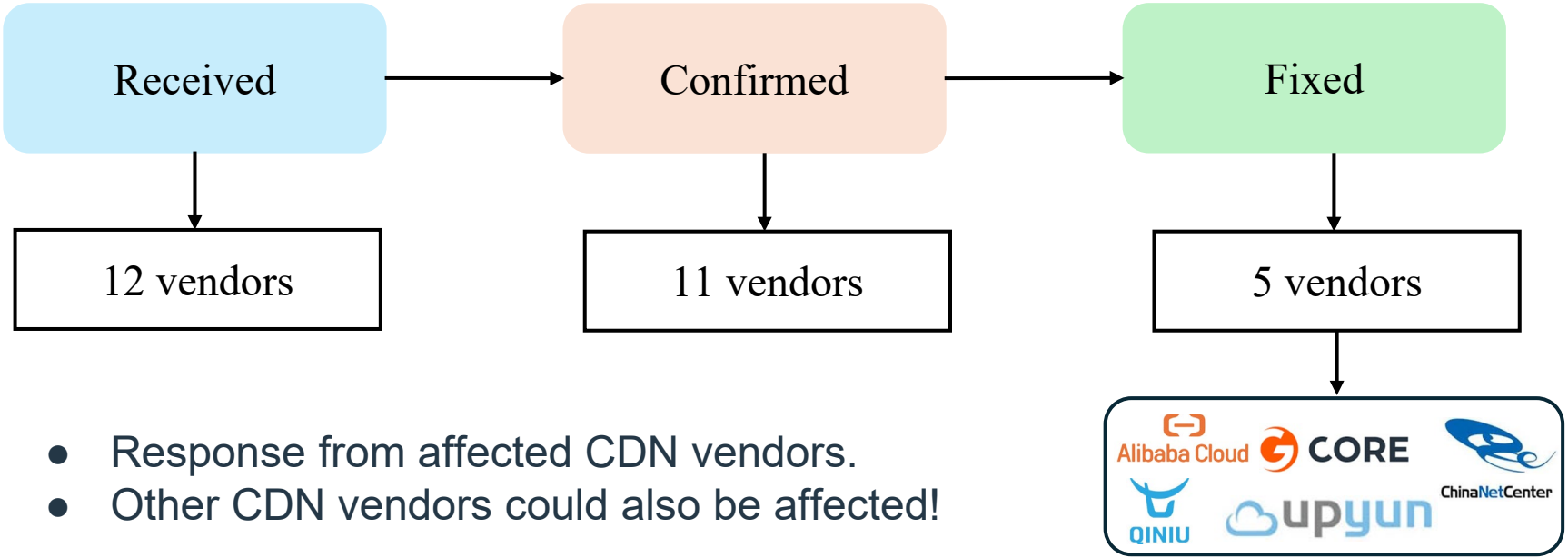
- Validate the ownership of customer-supplied origin configuration
  - Stop CDN being abused to attack 3rd party targets
  - But Can still attack websites hosted on CDN

Mitigation

- 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.
- Other CDN vendors could also be affected!

Lessons learnd

- CDN trades bandwidth for speed, but attackers exploit this design.

- Specifications must account for resource consumption in real-world implementations.

black hat ASIA 2025

APRIL 3-4, 2025

BRIEFINGS

Thank you
Q & A

Our Paper