CLOUDFLARE

DDoS Attack Mitigation at Cloudflare

Wouter de Vries
Systems Engineer

CLOUDFLARE

Currently:

- Systems Engineer at Cloudflare

Previously:

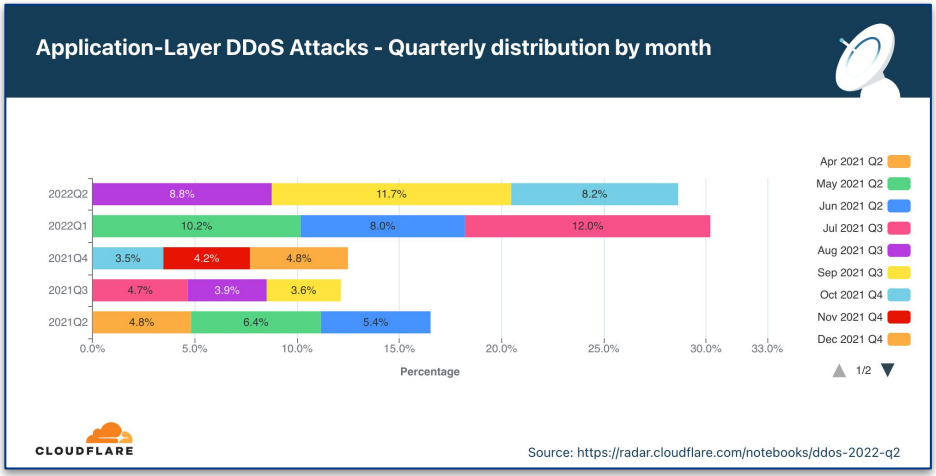
- Research Engineer at Tesorion
- PhD Candidate at University of Twente
  - Topic: Improving Anycast with Measurements

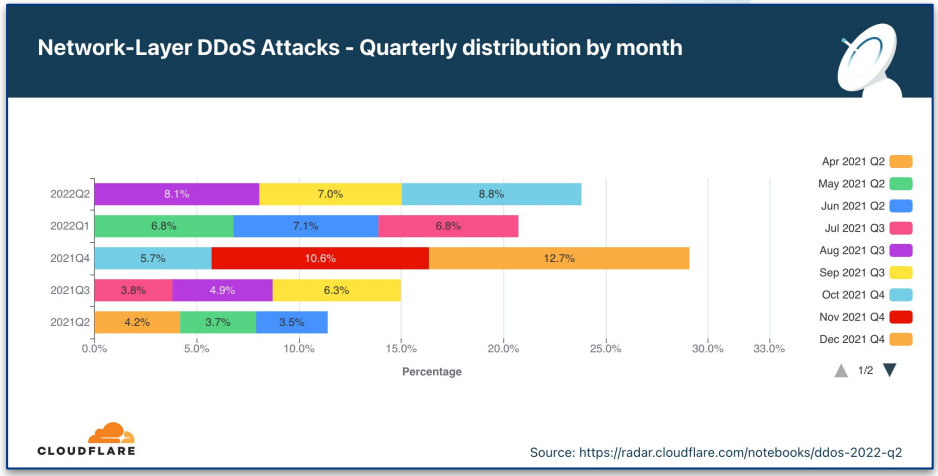
CLOUDFLARE

DDoS attack trends:
The view from Cloudflare's network

Are DDoS attacks increasing?

In Q2, DDoS attacks soared by 72%-109% YoY

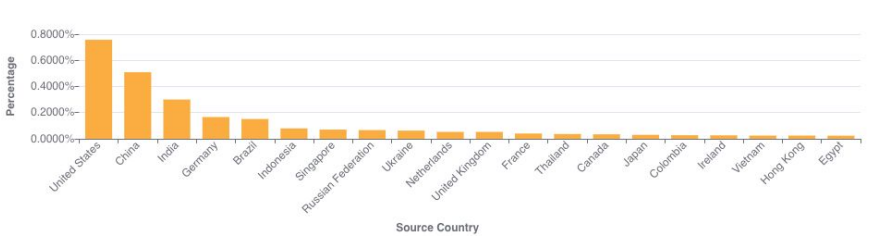




Where are DDoS attacks coming from?

A third of traffic in Palestine was DDoS, but US remains main source of DDoS attacks

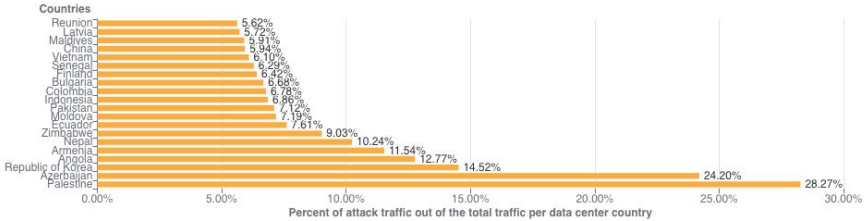
Application-Layer DDoS Attacks - Distribution by source country



CLOUDFLARE

Source: https://radar.cloudflare.com/notebooks/ddos-2022-q2

Network-layer DDoS Attacks - Top Countries (Worldwide)



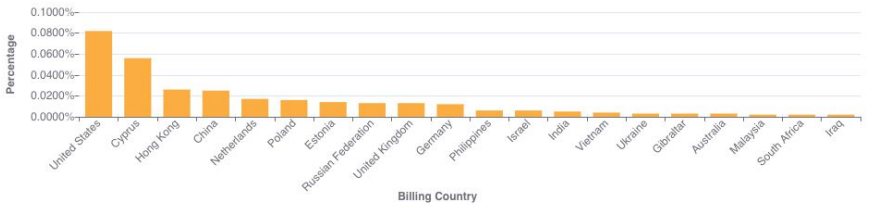
CLOUDFLARE

Source: https://radar.cloudflare.com/notebooks/undefined

Which countries are being attacked?

The US is the most attacked; attacks on US grew by 67%-95% QoQ.

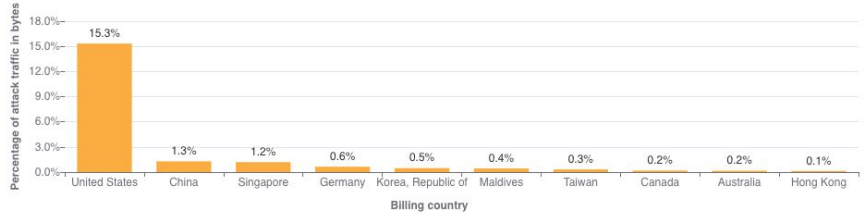
Application-Layer DDoS Attacks - Distribution by target country



CLOUDFLARE

Source: https://radar.cloudflare.com/notebooks/ddos-2022-q2

Network-Layer DDoS Attacks - Distribution of bytes by target country

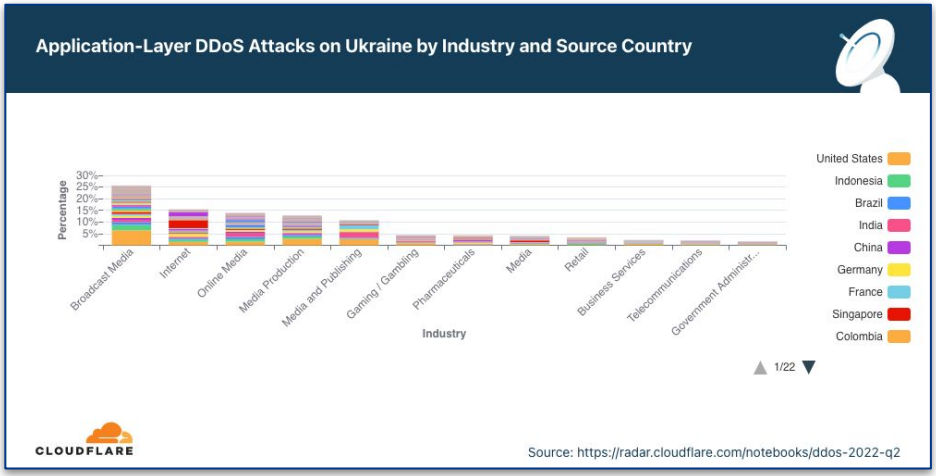


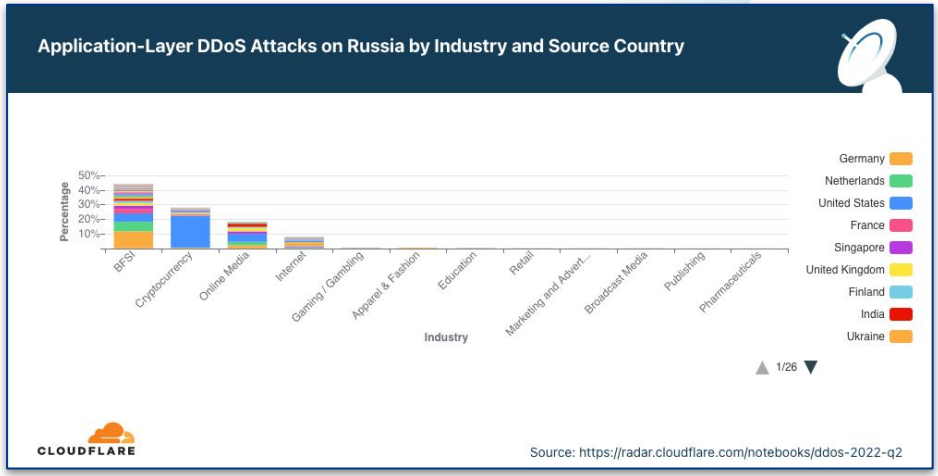
CLOUDFLARE

Source: https://radar.cloudflare.com/notebooks/ddos-2022-q2

What's going on in the Ukraine & Russia cyberspace?

The war on the ground is accompanied by attacks targeting the spread of information.



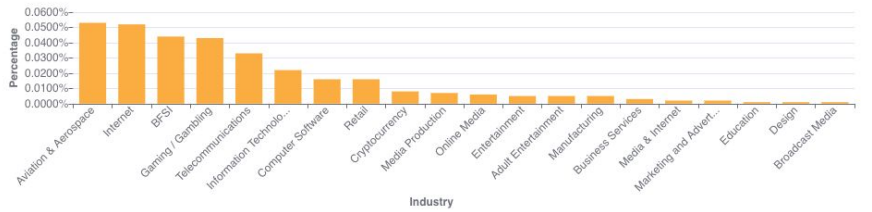


CLOUDFLARE

Which industries are being attacked?

Aviation & Aerospace was the most targeted by L7 attacks, Telcos were the most targeted by L3/4 attacks.

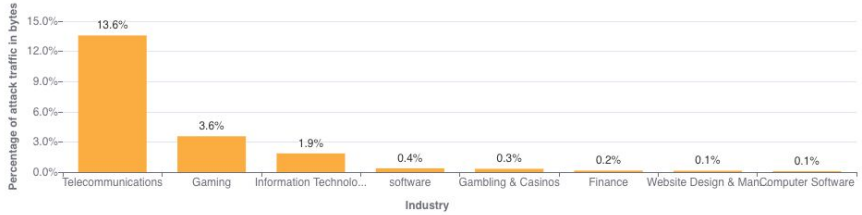
Application-Layer DDoS Attacks - Distribution by industry



CLOUDFLARE

Source: https://radar.cloudflare.com/notebooks/ddos-2022-q2

Network-Layer DDoS Attacks - Distribution of bytes by industry



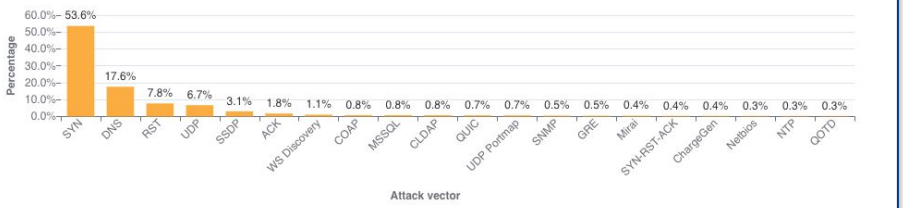
CLOUDFLARE

Source: https://radar.cloudflare.com/notebooks/ddos-2022-q2

What are the popular attack vectors?

SYN floods and DNS attacks the most popular, while attacks over CHARGEN, Ubiquity and Memcached soar.

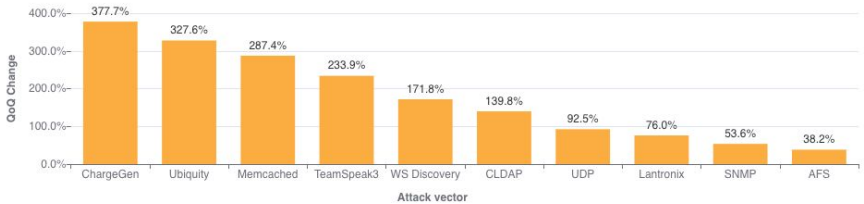
Network-Layer DDoS Attacks - Distribution by top attack vectors



CLOUDFLARE

Source: https://radar.cloudflare.com/notebooks/ddos-2022-q2

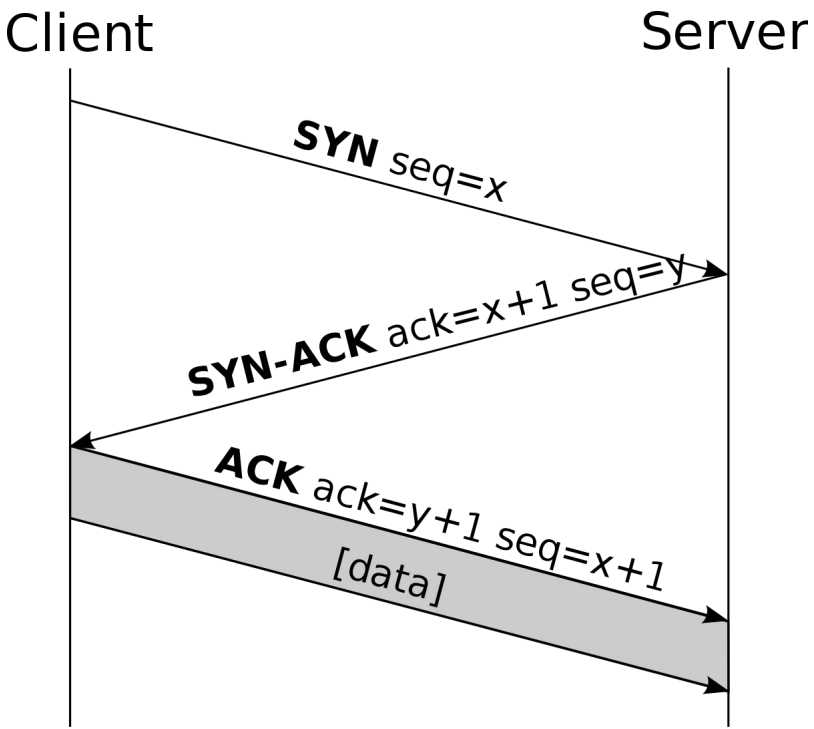
Network-Layer DDoS Attacks - Distribution by top emerging threats



CLOUDFLARE

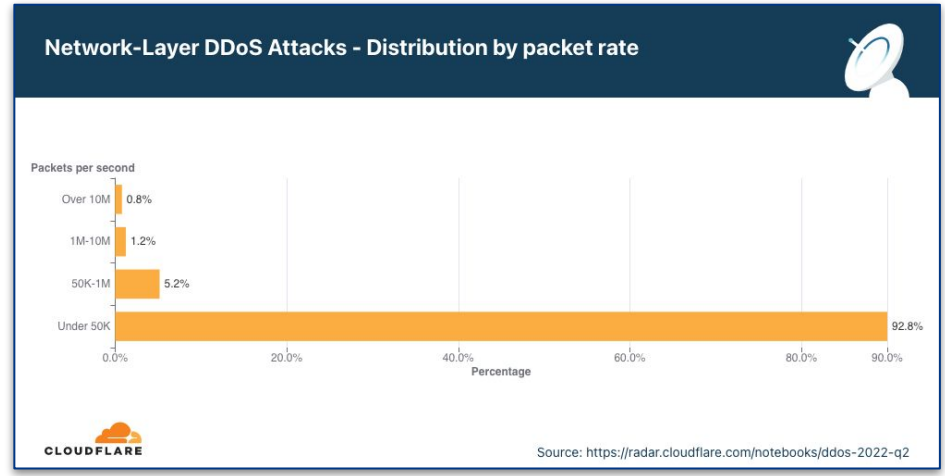
Source: https://radar.cloudflare.com/notebooks/ddos-2022-q2

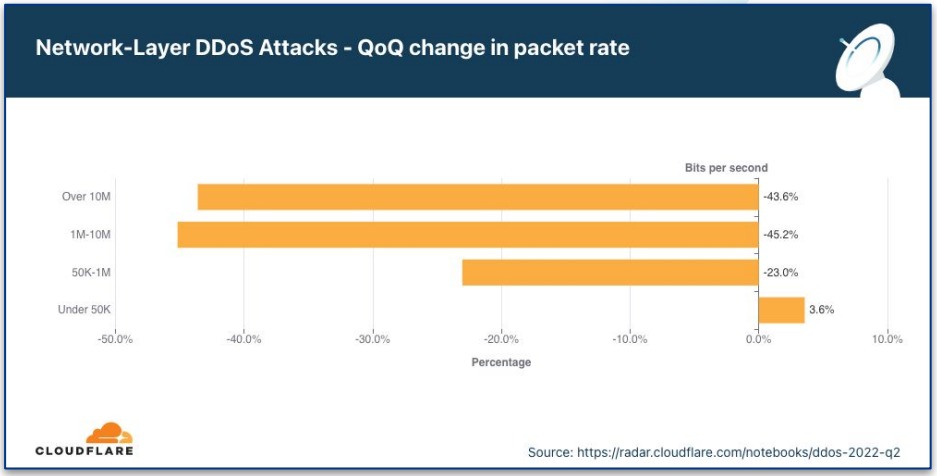
Abusing TCP handshakes



How many attacks are volumetric? (pps)

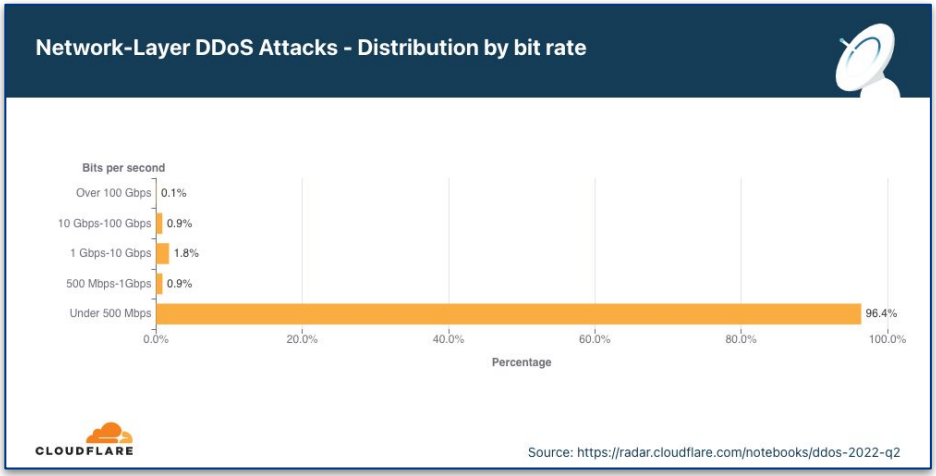
Majority of attacks are ‘small’ (50 Kpps), less than 1% exceeds 10M pps.

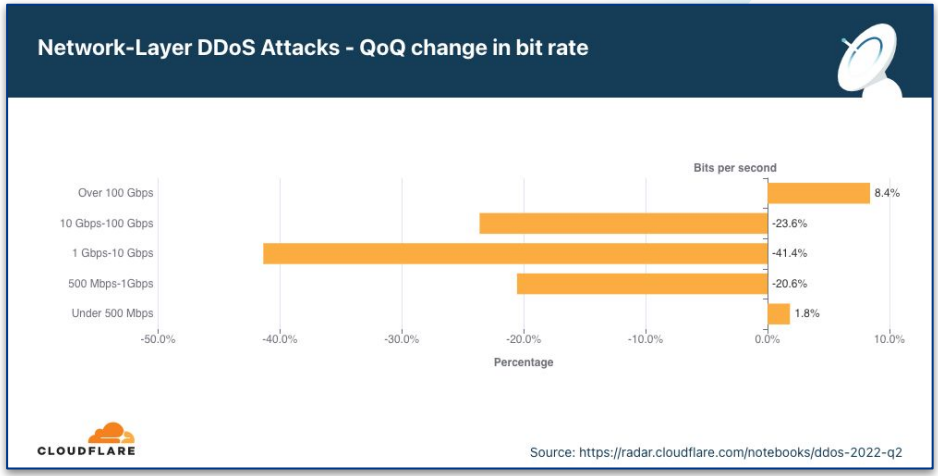




How many attacks are volumetric? (bps)

While most attacks are small, volumetric attacks of over 100 Gbps increased by 8% QoQ.

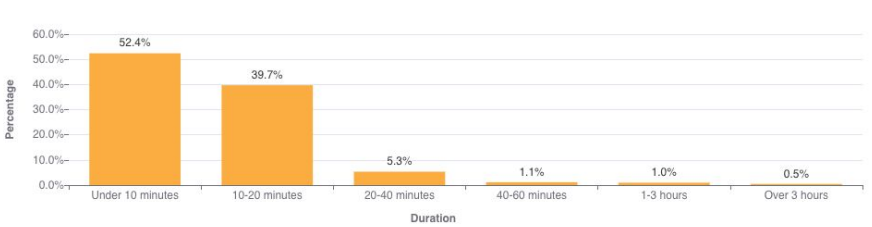




How long are the attacks?

Over 90% of attacks end within 20 minutes, but attacks lasting over three hours increased by 12% QoQ.

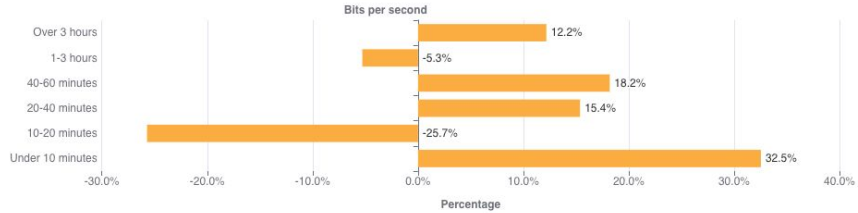
Network-Layer DDoS Attacks - Distribution by duration



CLOUDFLARE

Source: https://radar.cloudflare.com/notebooks/ddos-2022-q2

Network-Layer DDoS Attacks - QoQ change in duration



CLOUDFLARE

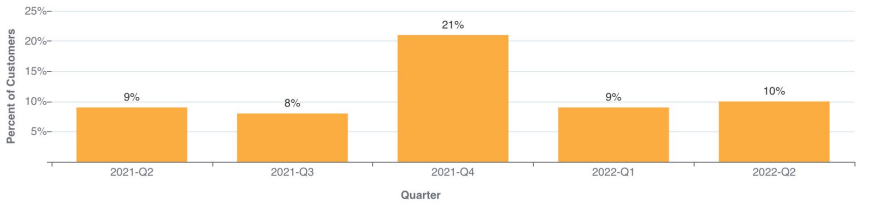
Source: https://radar.cloudflare.com/notebooks/ddos-2022-q2

Are Ransom DDoS attacks increasing?

RDDoS attacks increased by 11% QoQ.

June saw the highest number of RDDoS attacks in 6 months.

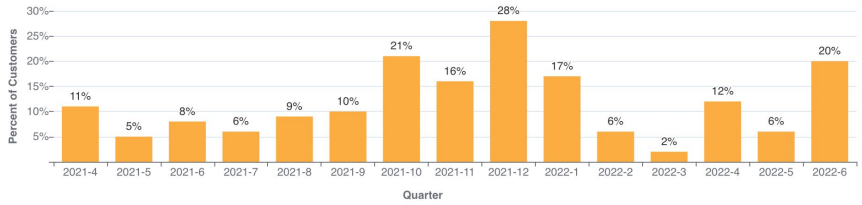
Ransom DDoS Attacks & Threats by Quarter



CLOUDFLARE

Source: https://radar.cloudflare.com/notebooks/ddos-2022-q2

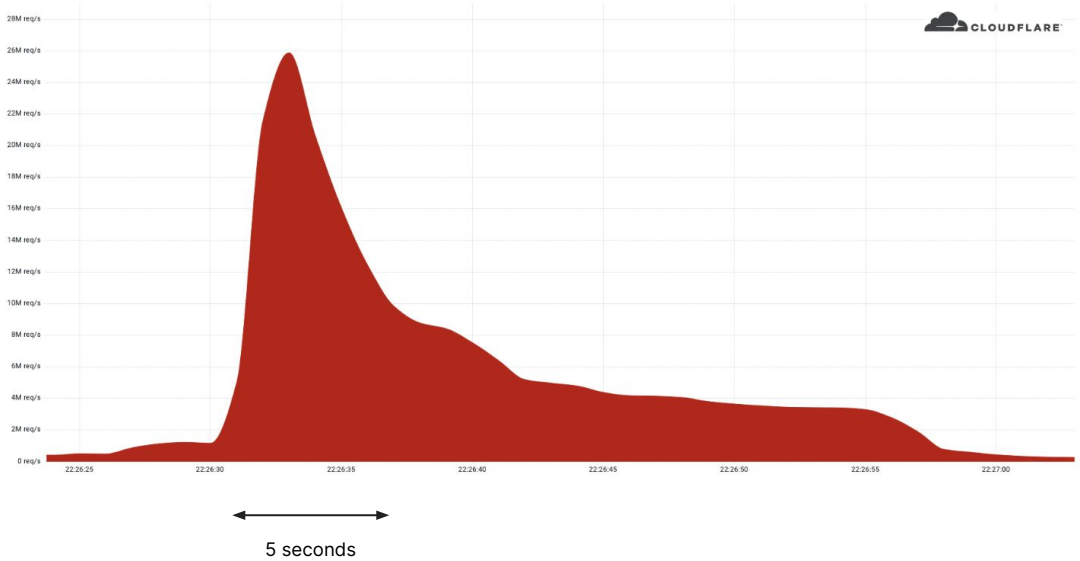
Ransom DDoS Attacks & Threats



CLOUDFLARE

Source: https://radar.cloudflare.com/notebooks/ddos-2022-q2

Largest HTTPS DDoS attack on record 26M rps by “Mantis”



Largest HTTPS attack detected to date

Cloudflare detected and stopped a **26M** requests-per-second **HTTPS DDoS attack.**

Targeted a website using the **Cloudflare free plan**.

Launched from a known botnet of **5K bots** originating from **1,500 networks** in **121 countries.**

Takeaways

Botnets move from residential ISPs to Cloud infrastructure; **from IoTs to VMs.**

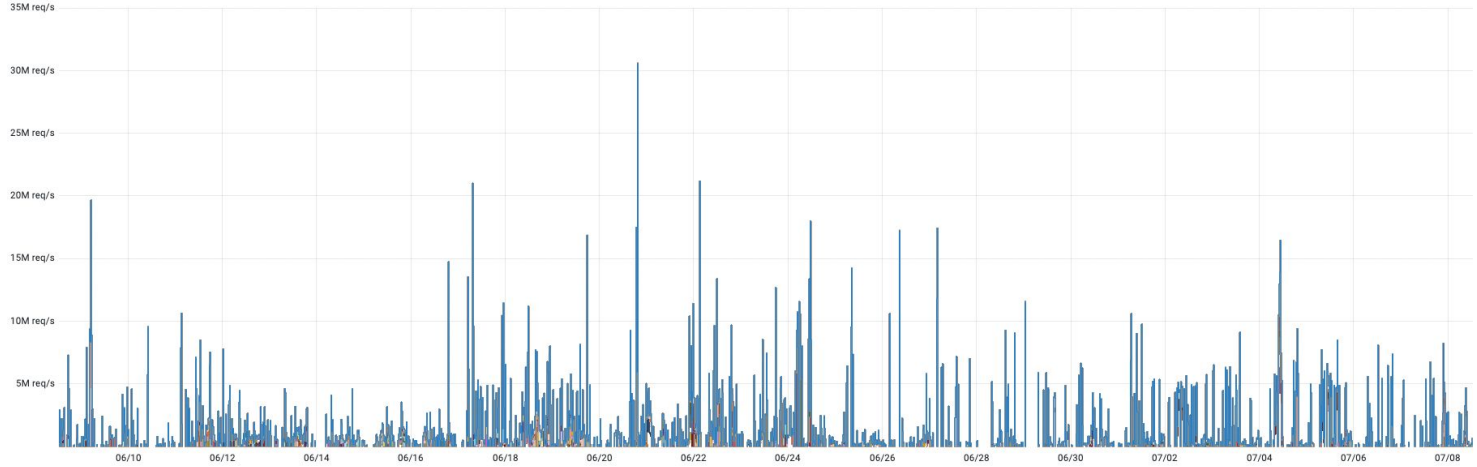
5 second attack peak requires scalable, automated, and **alway-on protection.**

CLOUDFLARE

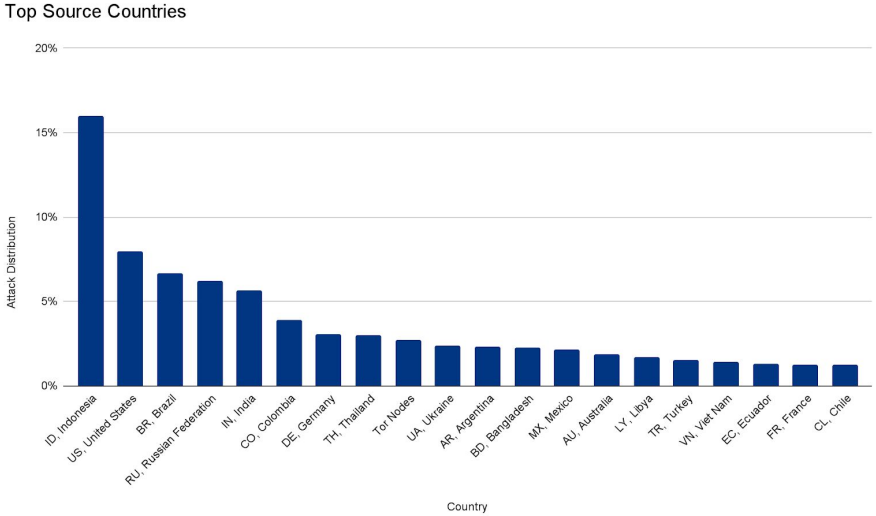
Mantis botnet

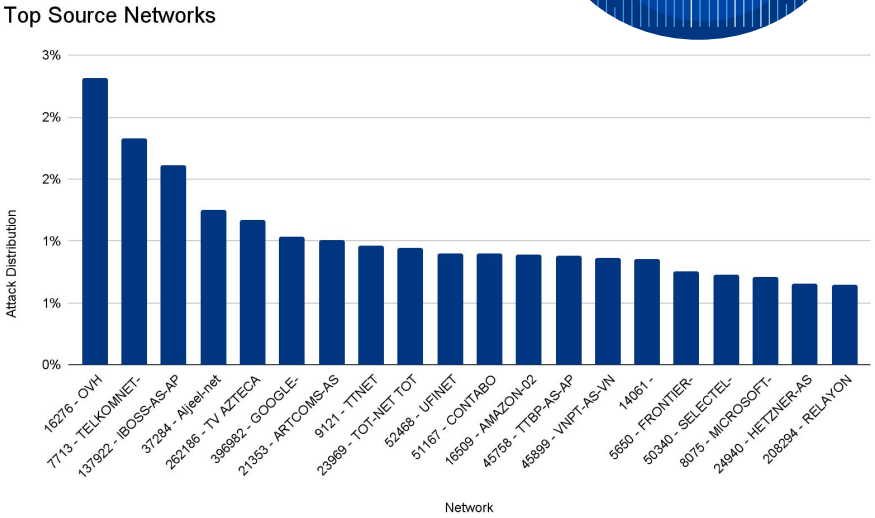
Meet “Mantis” - the most powerful botnet to date

- VM-based botnet 5K-strong
- Launched the 26M rps DDoS attack
- Launched over 3K attacks against 1K Cloudflare customers



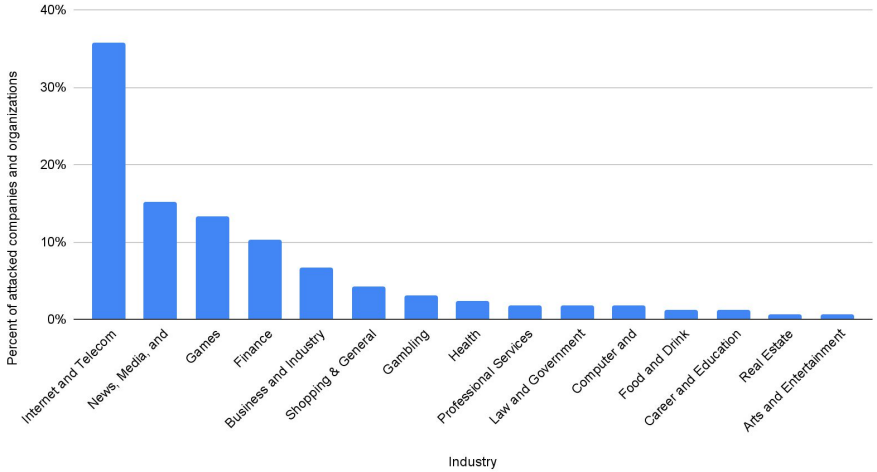
Internet & Telco companies the most attacked



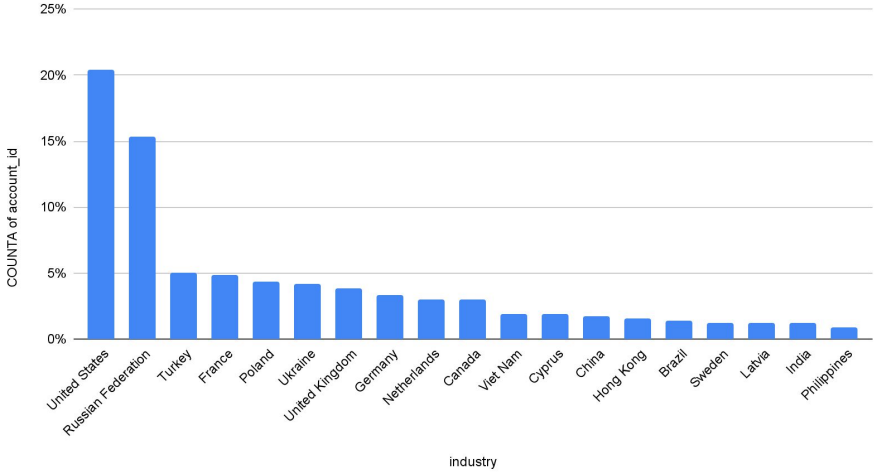


Internet & Telco companies the most attacked

Mantis botnet: top attacked industries



Top attacked countries by Mantis



CLOUDFLARE

Dealing with DDoS

The Cloudflare global network

270+

cities in 100+ countries,
including mainland China
50ms from 95% of users

11,000+

networks directly connect
to Cloudflare, including ISPs,
cloud providers & large enterprises

155 Tbps

of network edge
capacity & growing with
100% uptime SLA

117B

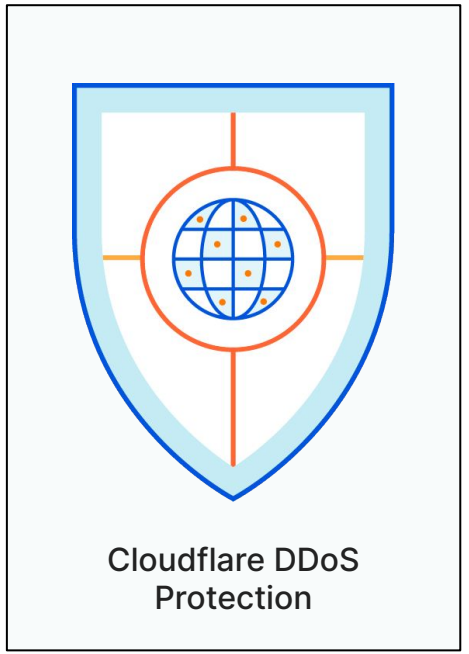
Cyber threats blocked
each day *Q2'22

CLOUDFLARE

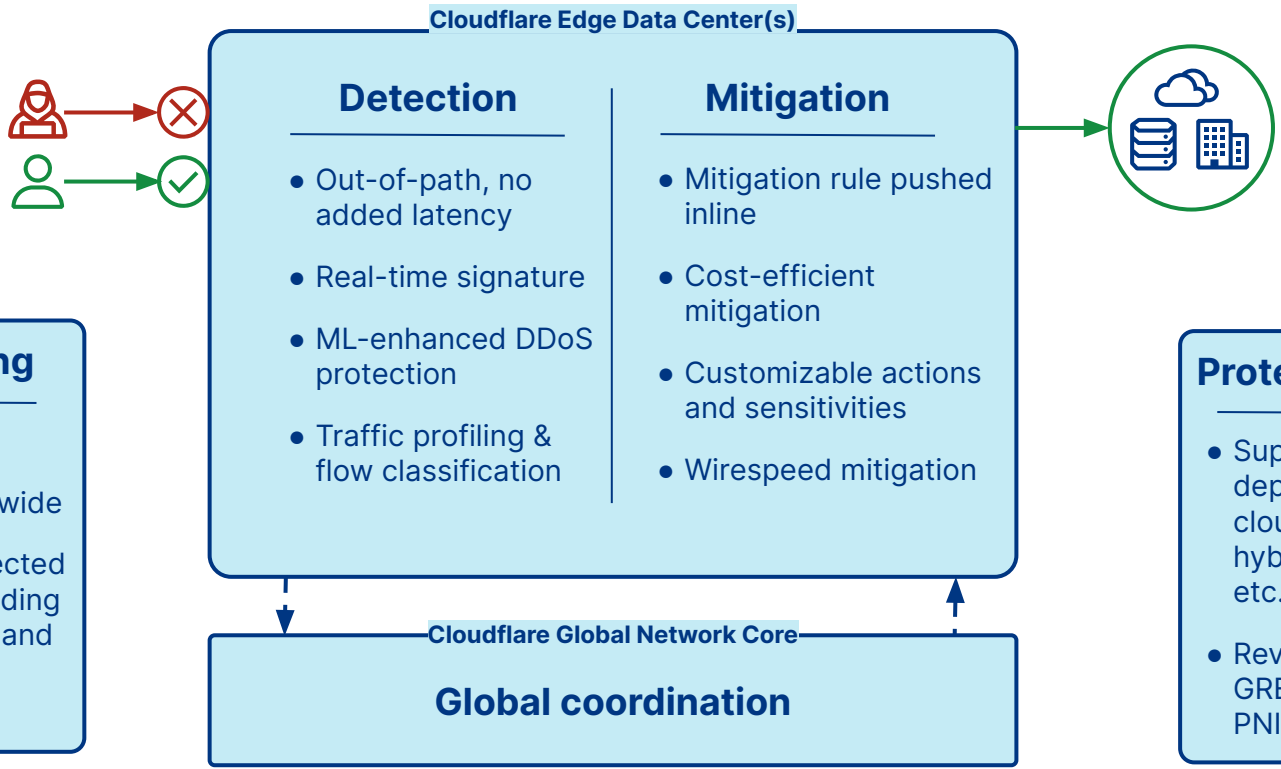
● = Cloudflare city (Map data as of December 15, 2021)

DDoS Protection — OSI stack

7	Application Layer	Cloudflare DDoS Protection for Web Applications
6	Presentation Layer	
5	Session Layer	
4	Transport Layer	Cloudflare Spectrum
3	Network Layer	Cloudflare Magic Transit
2	Datalink Layer	
1	Physical Layer	



Cloudflare DDoS Protection - Accurate & Autonomous

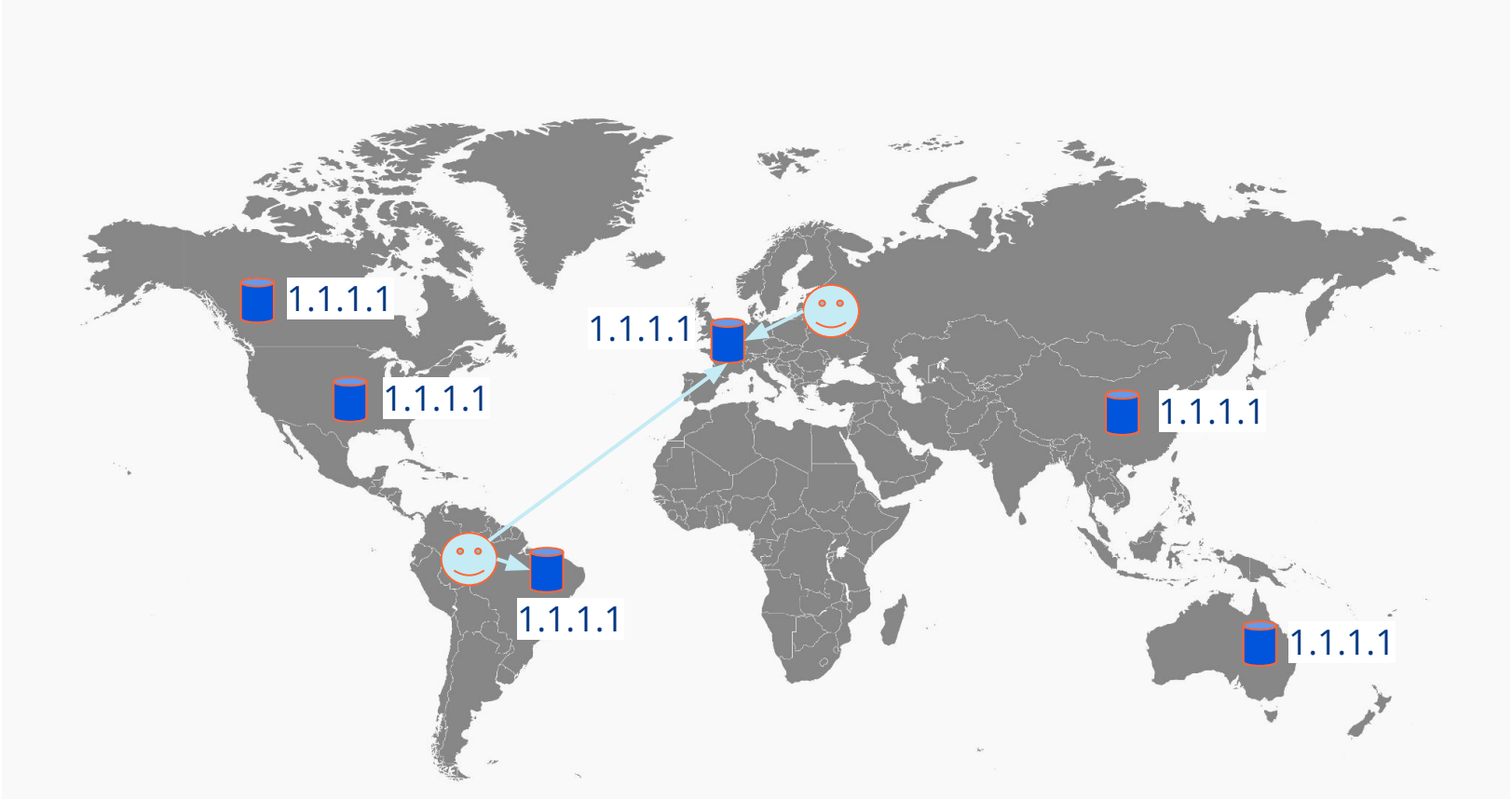


Traffic Routing

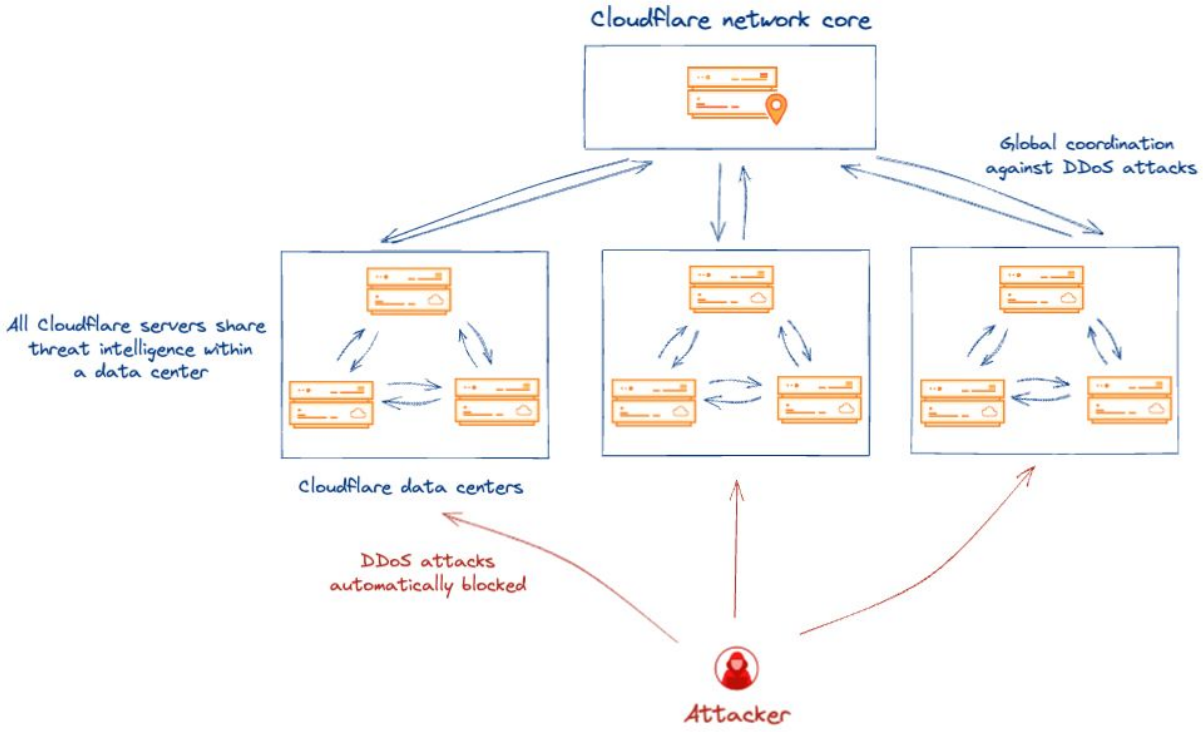
- Global Anycast
- 275 cities worldwide
- +10K interconnected network — including all major clouds and eyeball ISPs

Protected Assets

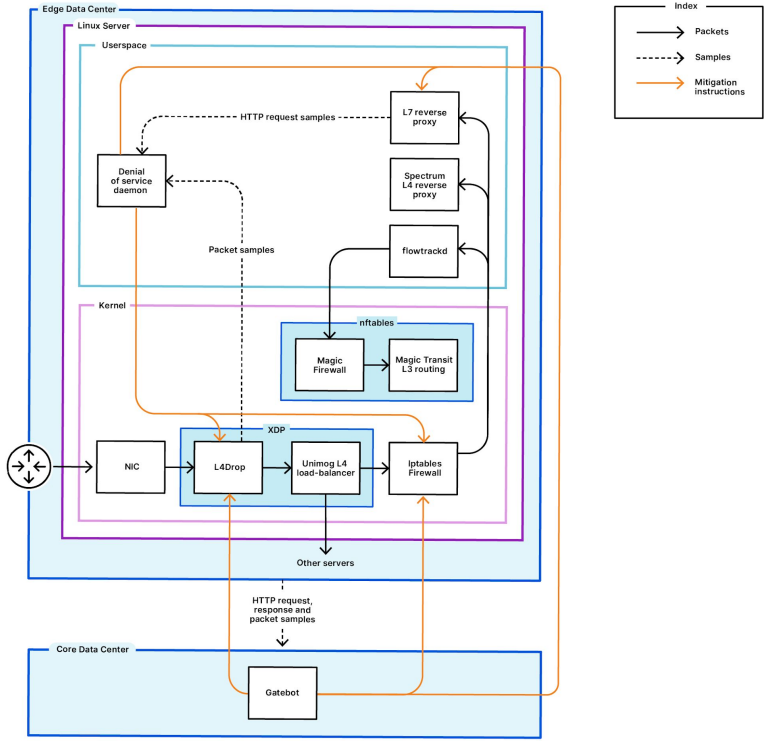
- Support for any deployment type: cloud, multi cloud, hybrid, on-premise, etc.
- Reverse-proxy, GRE/IPSec tunnels, PNI, CNI


1.1.1.1
1.1.1.1
1.1.1.1
1.1.1.1
1.1.1.1
1.1.1.1

Cloudflare DDoS Protection - Accurate & Autonomous



Cloudflare DDoS Protection - Let's dive in deeper



CLOUDFLARE

Thank you for listening