CLOUDFLARE

Anatomy of an Attack: Protecting Customer Networks from Application and DDoS Attacks

Steve Carlson
Public Sector Field Solutions Engineer
scarlson@cloudflare.com

Scott Reilly
Client Executive - CA/HI
sreilly@cloudflare.com

Jenna Bodie
Named Account Executive, CA
jbodie@cloudflare.com

CLOUDFLARE

Understanding and Responding to Distributed Denial-of-Service Attacks

Publication: March 21, 2024
Cybersecurity and Infrastructure Security Agency (CISA)

https://www.cisa.gov/sites/default/files/publications/understanding-and-responding-to-ddos-attacks_508c.pdf

https://www.cisa.gov/news-events/cybersecurity-advisories?f%5B0%5D=advisory_type%3A93

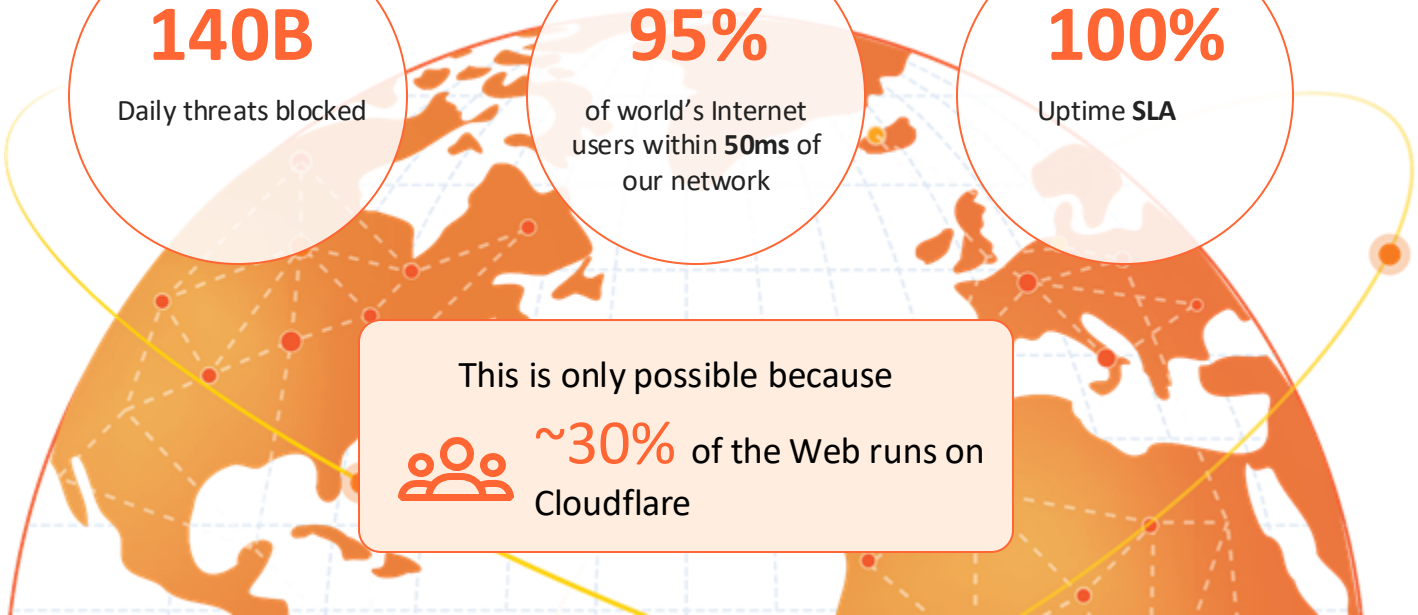
CLOUDFLARE

To provide a private, secure, reliable, performant, agile enterprise-grade Internet experience, Cloudflare is everywhere

140B
Daily threats blocked

95%
of world's Internet users within **50ms** of our network

100%
Uptime **SLA**

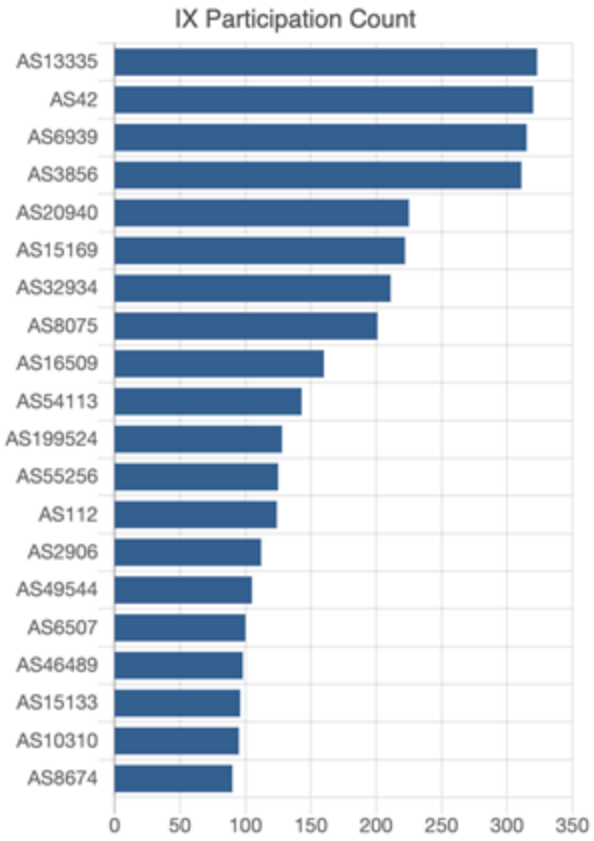


This is only possible because

~30% of the Web runs on Cloudflare

CLOUDFLARE

IX Participation Count		
ASN	Name	IXes
AS13335	Cloudflare, Inc.	323
AS42	WoodyNet, Inc.	320
AS6939	Hurricane Electric LLC	315
AS3856	Packet Clearing House, Inc.	311
AS20940	Akamai International B.V.	225
AS15169	Google LLC	222
AS32934	Facebook, Inc.	211
AS8075	Microsoft Corporation	201
AS16509	Amazon.com, Inc.	160
AS54113	Fastly, Inc.	143
AS199524	G-Core Labs S.A.	128
AS55256	Netskope Inc	125
AS112	DNS-OARC	124
AS2906	Netflix Streaming Services Inc.	112
AS49544	i3D.net B.V	105
AS6507	Riot Games, Inc	100
AS46489	Twitch Interactive Inc.	98
AS15133	EdgeCast Networks, Inc. d/b/a Verizon Digital Media Services	96
AS10310	Oath Holdings Inc.	95
AS8674	Netnod AB	90



https://bgp.he.net/report/exchanges#_participants

Agenda

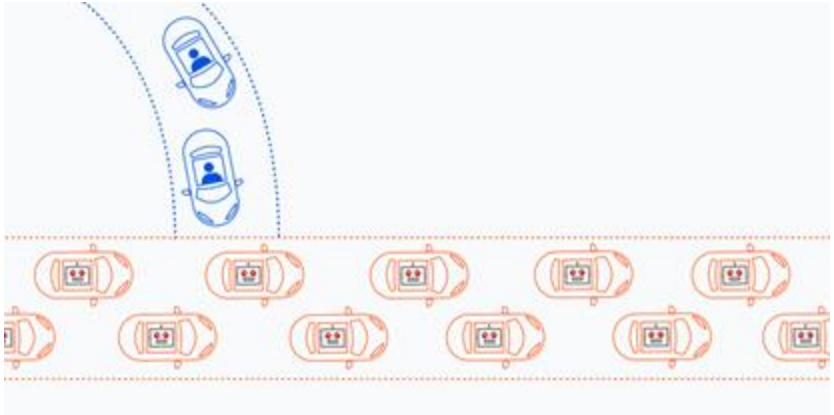
1. What is a DDoS Attack?
2. WHY? What does it look like? How can I tell?
3. Types of DDoS Attacks
4. How bad is it? - the details…
5. Protection and Prevention Strategies
6. How to Engage

Section

What is a DDoS Attack?

WHAT IS A DDoS ATTACK?

- From a high level, a DDoS attack is like an unexpected traffic jam clogging up the highway, preventing regular traffic from arriving at its destination.
  - A malicious attempt to disrupt the normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic.

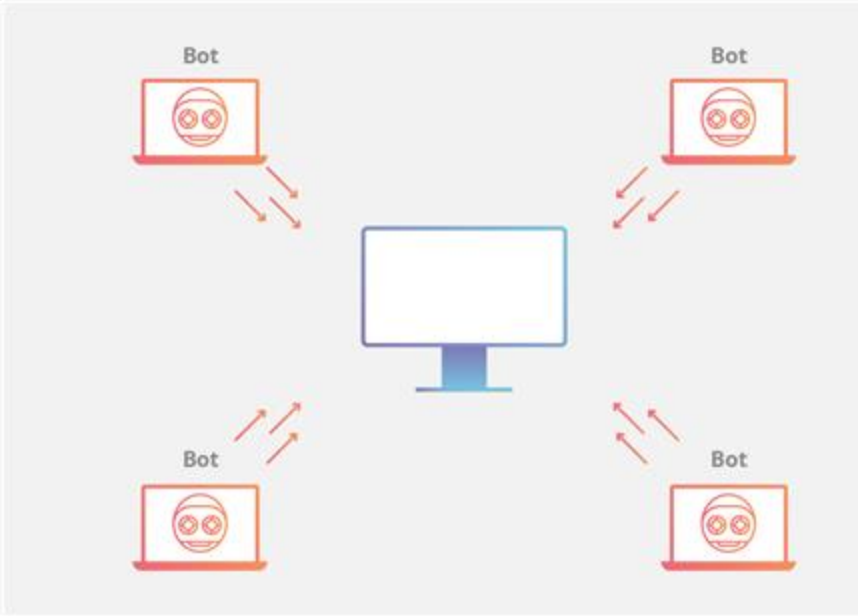


DDoS attacks are like traffic jams…

WHAT IS A DDoS ATTACK?

CLOUDFLARE

DDoS attacks utilize BotNets: Robot + Network

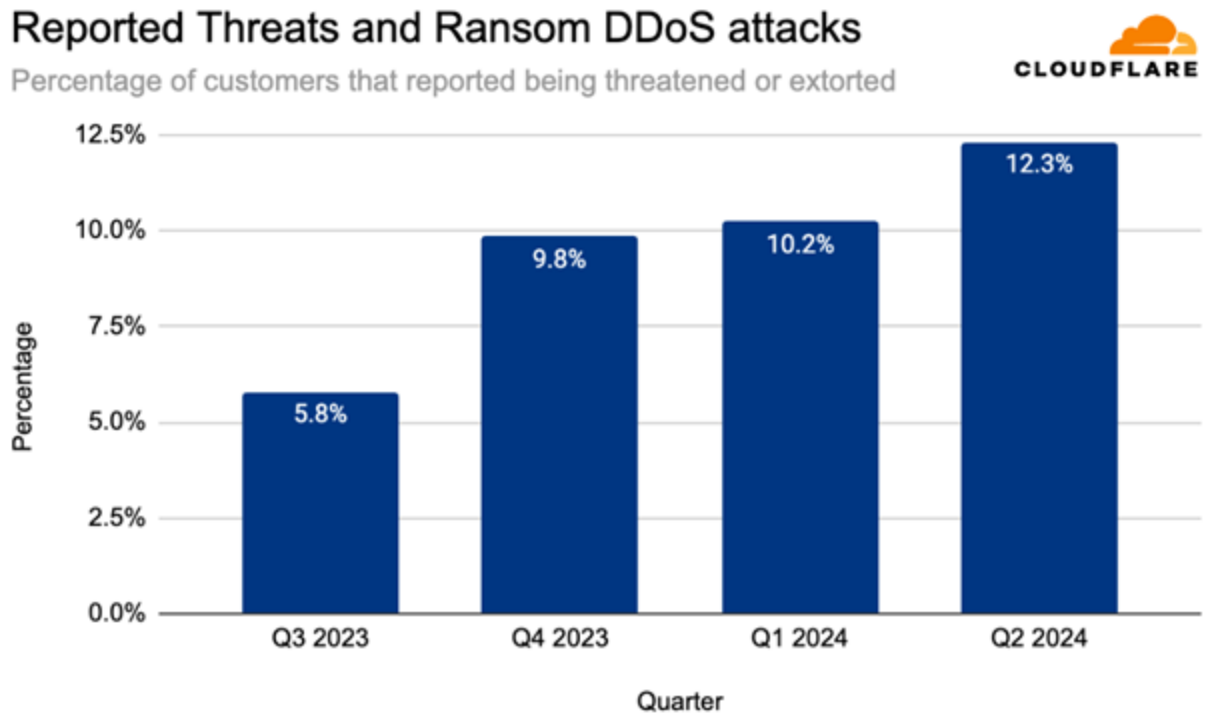


- Attacker sends instructions to botnet
- Bots send requests to target
- Target server or network overflows capacity
- Difficult to separate good from bad traffic

Section

WHY? What does it look like? How can I tell?

Ransom DDoS Becomes a new Strategy



CLOUDFLARE

Ransom DDoS Becomes a new Strategy

	Ransomware	vs.	Ransom DDoS
Method of Operation	'Denial of data' by a malicious script*		Denial of service by a botnet
Required Access	Requires access to internal systems		Only requires knowledge of IPs/URL
Required Expertise	Medium/High		Low

* More specifically, Malware or Ransomware can be used to encrypt, leak or delete the victim's data.

WHY?

CLOUDFLARE

Subject: ddos attack

Hi!

If you dont pay 8 bitcoin until 17. january your network will be hardly ddosed! Our attacks are super powerfull. And if you dont pay until 17. january ddos attack will start and price to stop will double!

We are not kidding and we will do small demo now on [XXXXXXXX] to show we are serious.

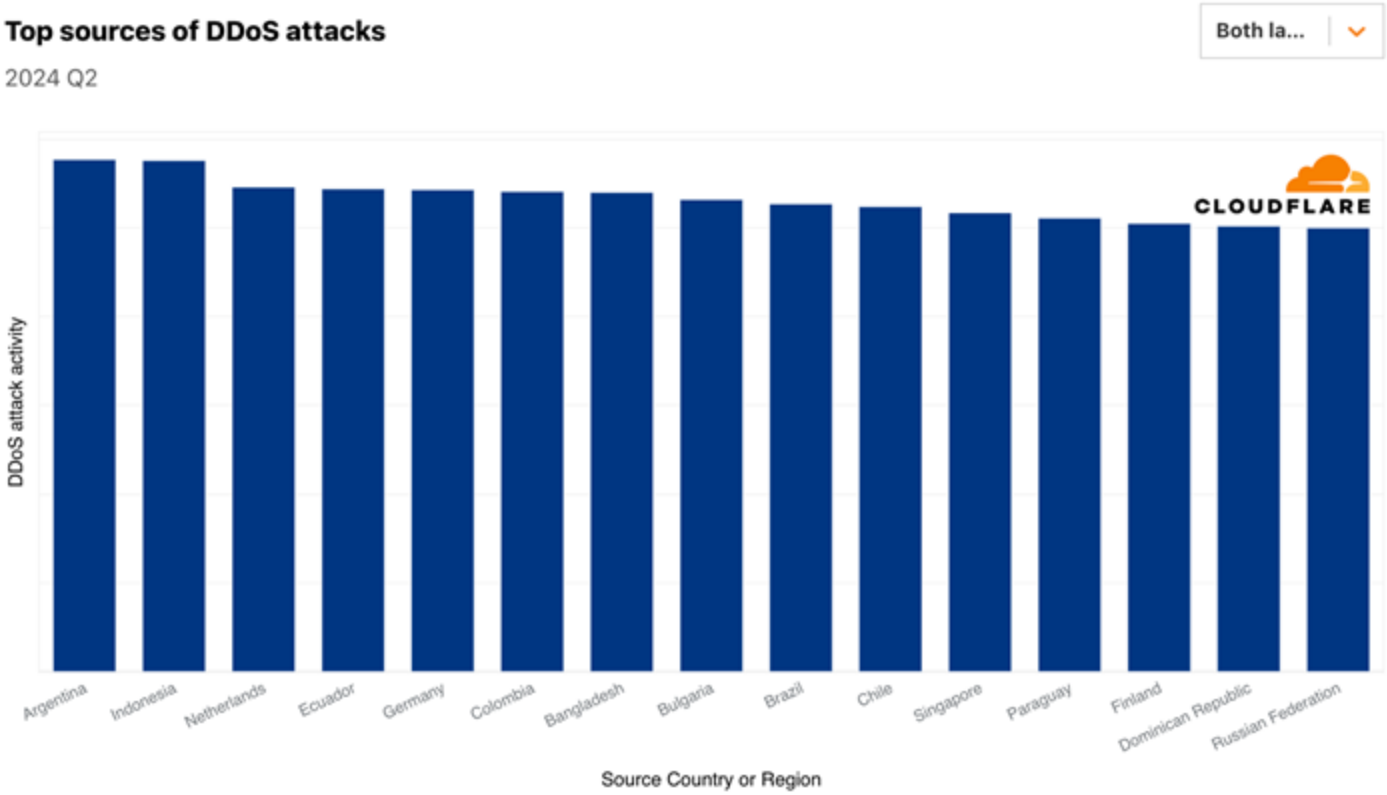
Pay and you are safe from us forever.

OUR BITCOIN ADDRESS: [XXXXXXXX]

Dont reply, we will ignore! Pay and we will be notify you payed and you are safe.

Cheers!

FROM WHERE?



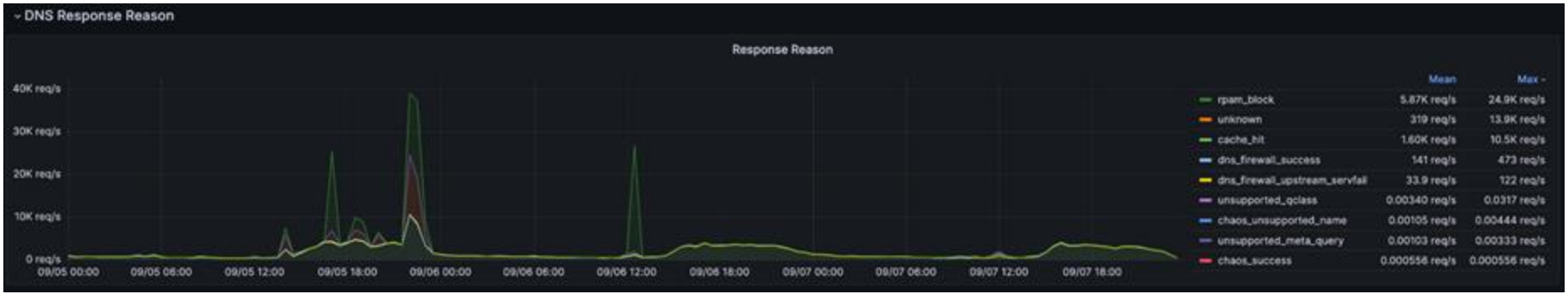
15 largest sources of DDoS attacks in 2024 Q2

WHAT DOES IT LOOK LIKE?

CLOUDFLARE

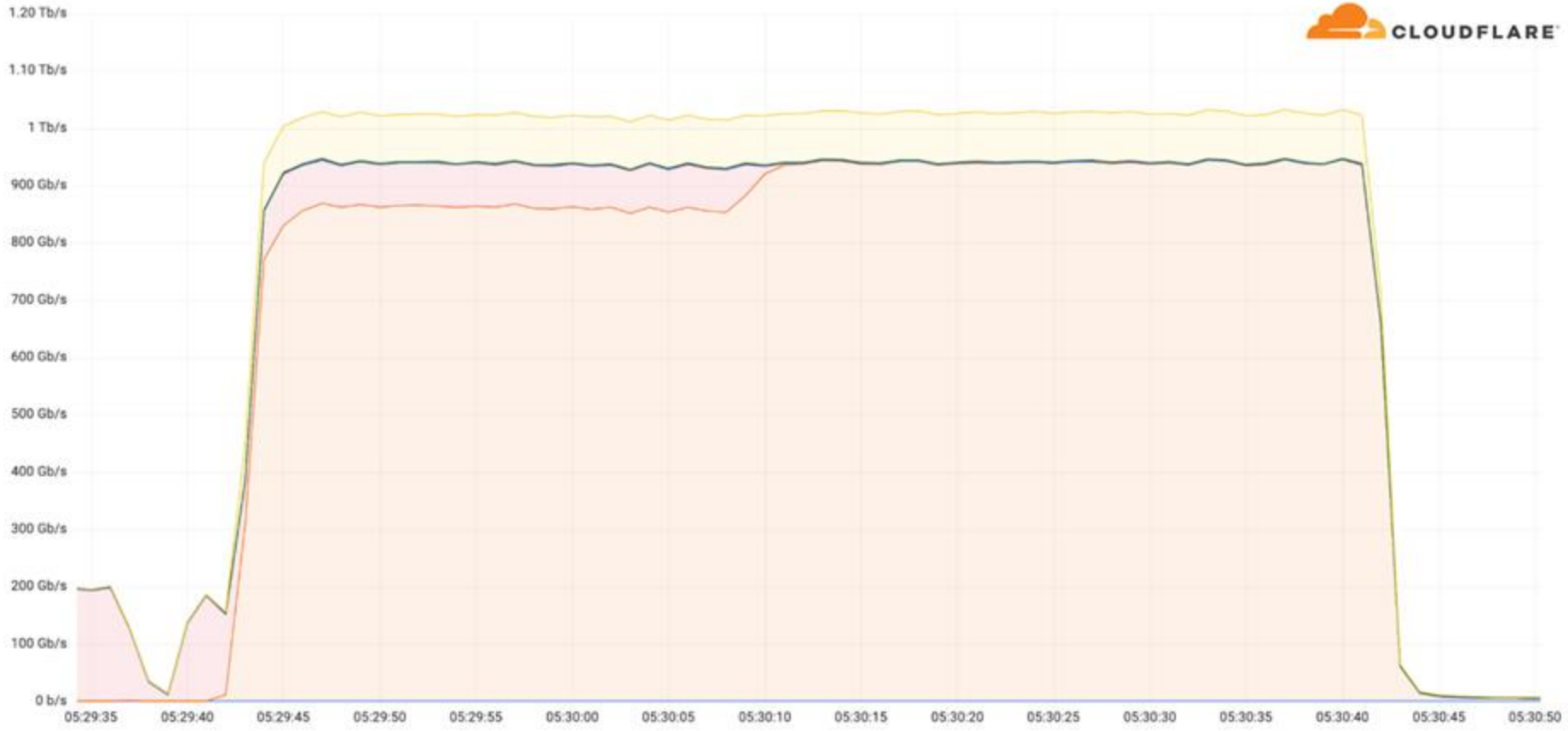
Receive Time	Type	Threat/C	Source address	Destination address	Application	IP Proto	Destinat	Bytes Sent	Bytes Received	Action	Session End Reason	Source Z	Destinat	NAT Sou
11/9/23 12:45	TRAFFIC	end	172.69.66.65		dns-base	udp	53	104	1091	allow	aged-out	l3-outside1	l3-inside	172.69.66
11/9/23 12:45	TRAFFIC	end	172.68.33.31		dns-base	udp	53	100	1079	allow	aged-out	l3-outside1	l3-inside	172.68.33
11/9/23 12:45	TRAFFIC	end	172.70.249.114		dns-base	tcp	53	416	1698	allow	tcp-fin	l3-outside1	l3-inside	172.70.24
11/9/23 12:45	TRAFFIC	end	172.71.157.20		dns-base	udp	53	84	846	allow	aged-out	l3-outside1	l3-inside	172.71.15
11/9/23 12:45	TRAFFIC	end	172.68.2.56		dns-base	udp	53	95	1074	allow	aged-out	l3-outside1	l3-inside	172.68.2.
11/9/23 12:45	TRAFFIC	end	172.68.2.56		dns-base	udp	53	98	1085	allow	aged-out	l3-outside1	l3-inside	172.68.2.
11/9/23 12:45	TRAFFIC	end	172.71.141.71		dns-base	tcp	53	138	70	allow	tcp-rst-from-client	l3-outside1	l3-inside	172.71.14
11/9/23 12:45	TRAFFIC	end	172.70.177.36		dns-base	udp	53	92	1071	allow	aged-out	l3-outside1	l3-inside	172.70.17
11/9/23 12:45	TRAFFIC	end	172.68.2.56		dns-base	udp	53	99	1079	allow	aged-out	l3-outside1	l3-inside	172.68.2.
11/9/23 12:45	TRAFFIC	end	172.68.33.31		dns-base	udp	53	103	1091	allow	aged-out	l3-outside1	l3-inside	172.68.33
11/9/23 12:45	TRAFFIC	end	172.69.66.65		dns-base	udp	53	104	1084	allow	aged-out	l3-outside1	l3-inside	172.69.66
11/9/23 12:45	TRAFFIC	end	172.70.249.114		dns-base	tcp	53	138	70	allow	tcp-rst-from-client	l3-outside1	l3-inside	172.70.24
11/9/23 12:45	TRAFFIC	end	172.71.157.20		dns-base	udp	53	84	84	allow	aged-out	l3-outside1	l3-inside	172.71.15
11/9/23 12:45	TRAFFIC	end	172.71.157.20		dns-base	udp	53	84	84	allow	aged-out	l3-outside1	l3-inside	172.71.15
11/9/23 12:45	TRAFFIC	end	172.71.157.20		dns-base	udp	53	84	846	allow	aged-out	l3-outside1	l3-inside	172.71.15
11/9/23 12:45	TRAFFIC	end	172.70.249.112		dns-base	udp	53	84	84	allow	aged-out	l3-outside1	l3-inside	172.70.24
11/9/23 12:45	TRAFFIC	end	172.70.245.110		dns-base	udp	53	95	307	allow	aged-out	l3-outside1	l3-inside	172.70.24
11/9/23 12:45	TRAFFIC	end	172.70.249.112		dns-base	udp	53	95	307	allow	aged-out	l3-outside1	l3-inside	172.70.24
11/9/23 12:45	TRAFFIC	end	172.70.249.112		dns-base	udp	53	84	84	allow	aged-out	l3-outside1	l3-inside	172.70.24
11/9/23 12:45	TRAFFIC	end	172.70.33.69		dns-base	udp	53	84	84	allow	aged-out	l3-outside1	l3-inside	172.70.33
11/9/23 12:45	TRAFFIC	end	172.70.33.69		dns-base	udp	53	88	303	allow	aged-out	l3-outside1	l3-inside	172.70.33
11/9/23 12:45	TRAFFIC	end	172.71.145.87		dns-base	udp	53	84	84	allow	aged-out	l3-outside1	l3-inside	172.71.14
11/9/23 12:45	TRAFFIC	end	172.70.33.69		dns-base	udp	53	84	84	allow	aged-out	l3-outside1	l3-inside	172.70.33
11/9/23 12:45	TRAFFIC	end	172.71.145.87		dns-base	udp	53	84	84	allow	aged-out	l3-outside1	l3-inside	172.71.14
11/9/23 12:45	TRAFFIC	end	172.71.145.87		dns-base	udp	53	84	846	allow	aged-out	l3-outside1	l3-inside	172.71.14
11/9/23 12:45	TRAFFIC	end	172.71.165.79		dns-base	udp	53	104	1084	allow	aged-out	l3-outside1	l3-inside	172.71.16
11/9/23 12:45	TRAFFIC	end	172.69.66.65		dns-base	udp	53	104	1084	allow	aged-out	l3-outside1	l3-inside	172.69.66
11/9/23 12:45	TRAFFIC	end	172.71.169.78		dns-base	udp	53	104	1084	allow	aged-out	l3-outside1	l3-inside	172.71.16
11/9/23 12:45	TRAFFIC	end	172.71.165.79		dns-base	udp	53	104	1084	allow	aged-out	l3-outside1	l3-inside	172.71.16
11/9/23 12:45	TRAFFIC	end	172.69.66.23		dns-base	tcp	53	258	198	allow	tcp-fin	l3-outside1	l3-inside	172.69.66
11/9/23 12:45	TRAFFIC	end	172.69.66.23		dns-base	tcp	53	416	1698	allow	tcp-fin	l3-outside1	l3-inside	172.69.66
11/9/23 12:45	TRAFFIC	end	172.68.33.33		dns-base	udp	53	100	1079	allow	aged-out	l3-outside1	l3-inside	172.68.33

WHAT DOES IT LOOK LIKE?



WHAT DOES IT LOOK LIKE?

CLOUDFLARE



Section

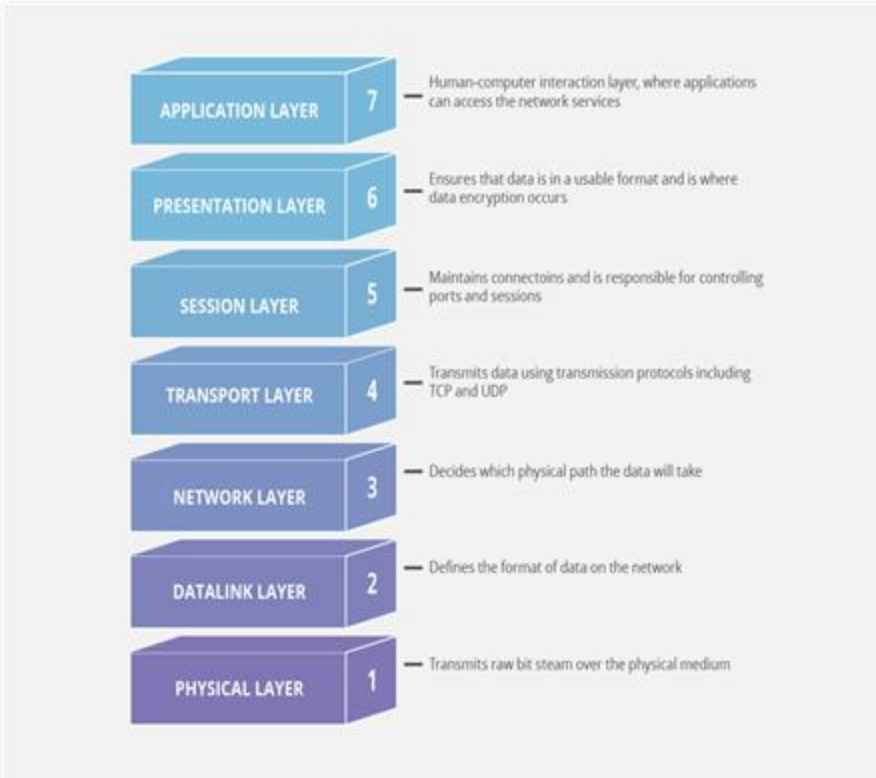
How Do Bad Actors Target Public Sector with DDoS?

Types of DDoS Attacks:

TYPES OF DDOS ATTACKS

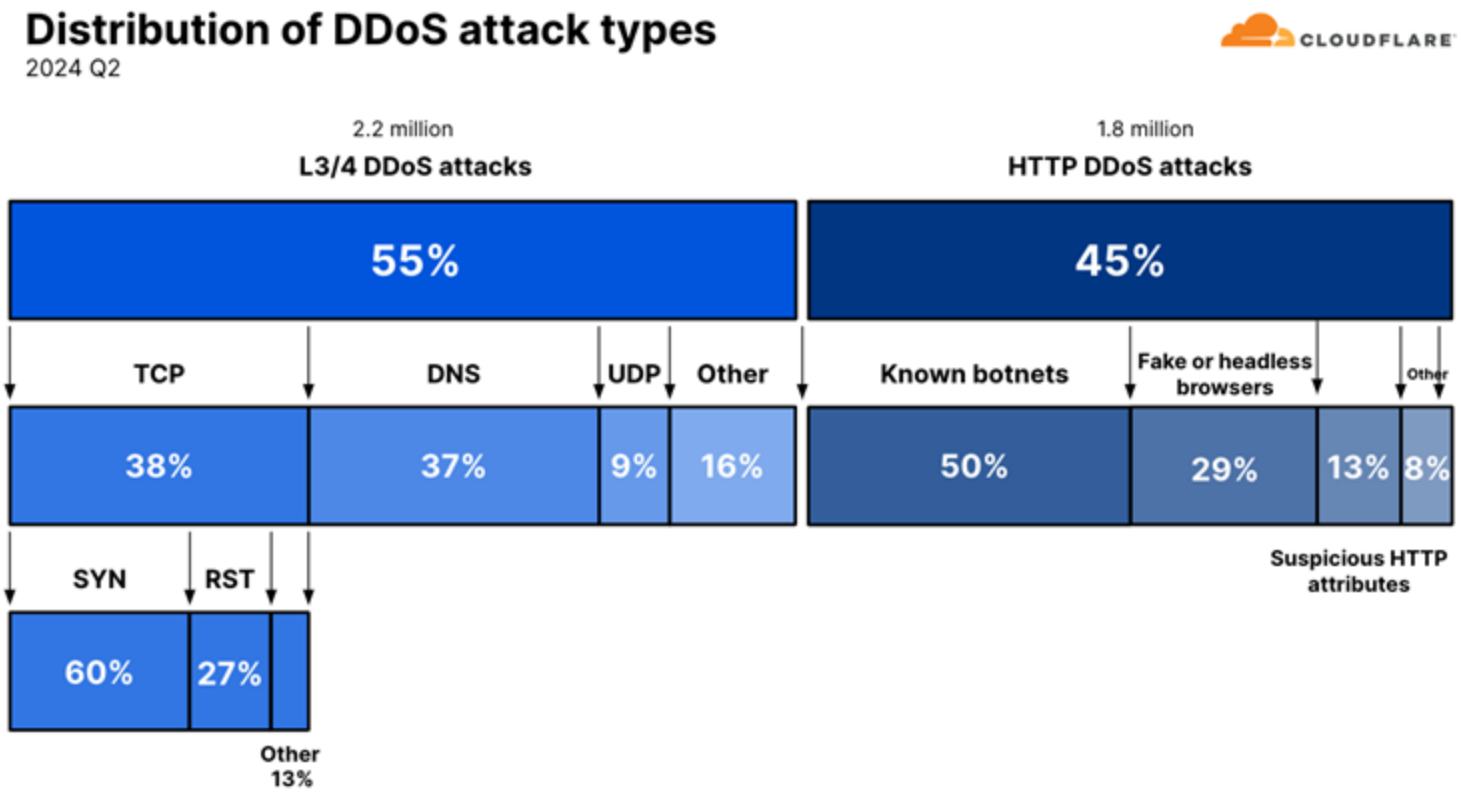
CLOUDFLARE

Common attack patterns



- **Application Resource Overload (L7)** - Exploiting the behavior of an application to exhaust compute or storage resources (e.g. sending excessive search requests, slow POSTs)
- **Protocol Resource Overload (L4)** - A protocol attack that seeks to overwhelm a server or routers ability to track network sessions. (e.g. TCP SYN Flood attacks)
- **Network Resource Overload (L3)** - A volumetric attack to overwhelm available network bandwidth (e.g. UDP amplification attacks)

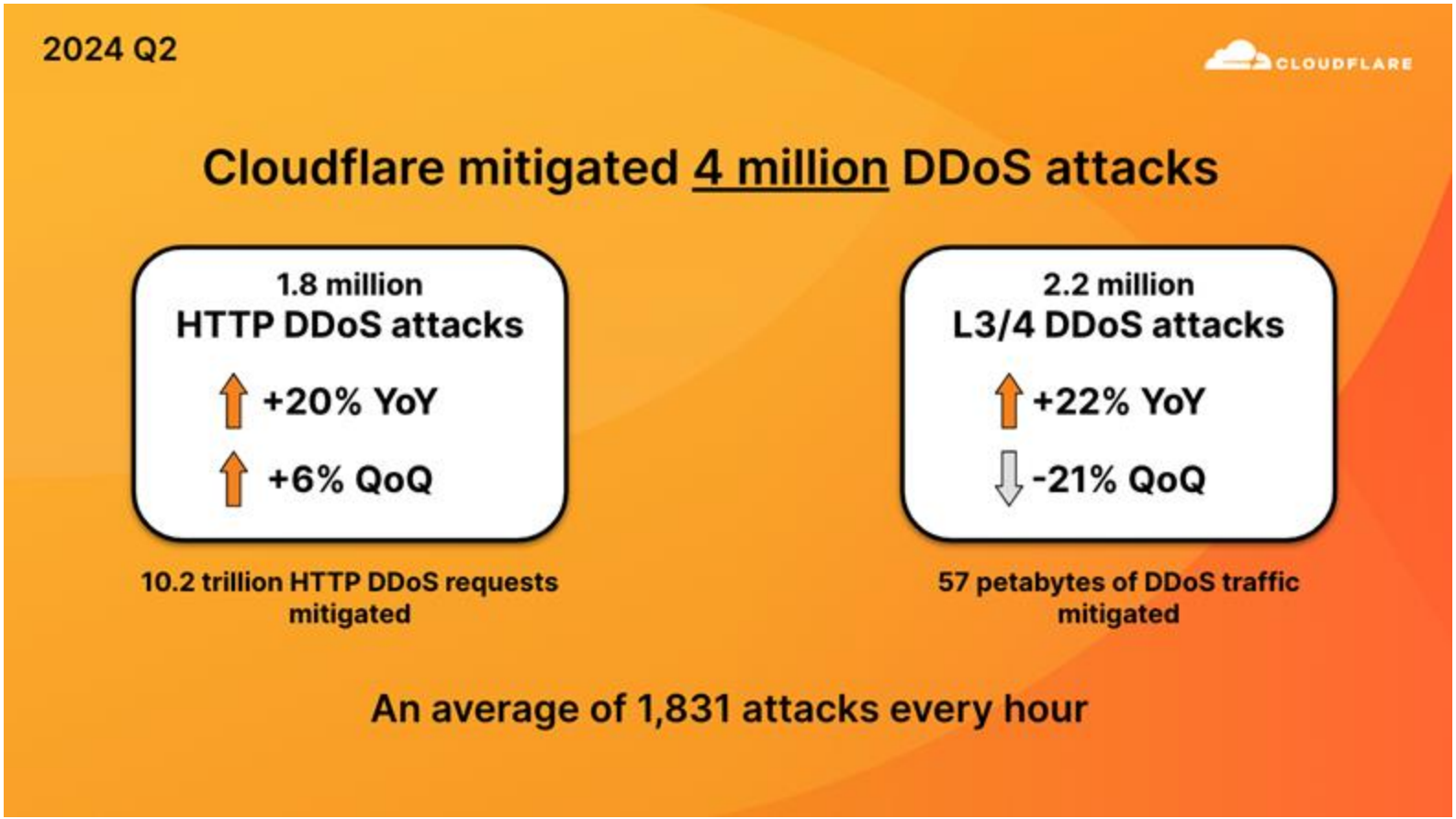
TYPES OF DDOS ATTACKS



Section

How bad is it?

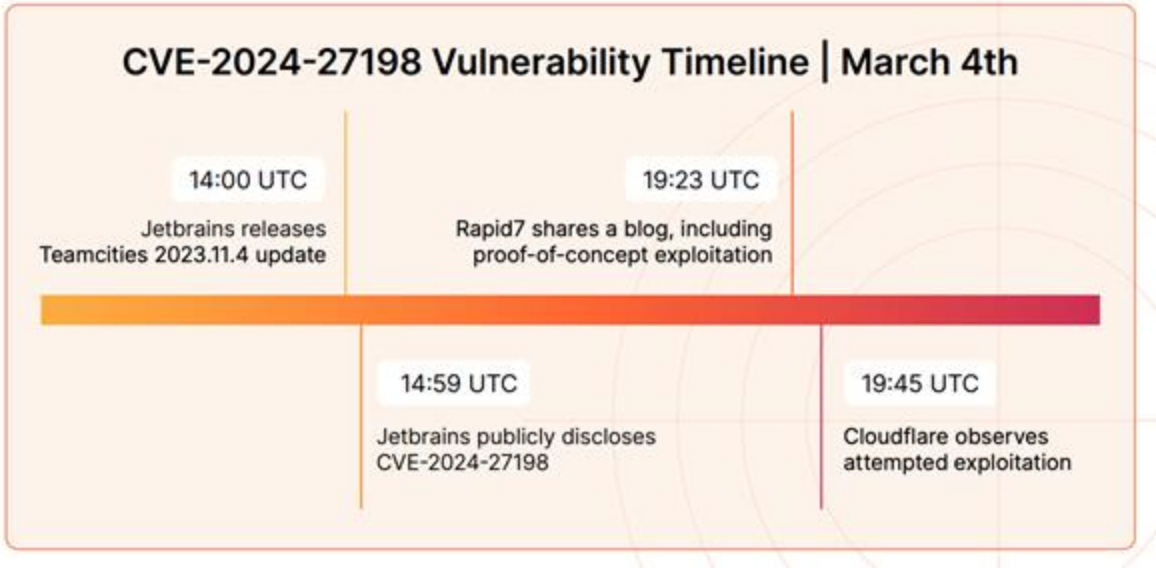
HOW BAD IS IT?


2024 Q2
CLOUDFLARE
Cloudflare mitigated 4 million DDoS attacks
1.8 million
HTTP DDoS attacks
+20% YoY
+6% QoQ
2.2 million
L3/4 DDoS attacks
+22% YoY
-21% QoQ
10.2 trillion HTTP DDoS requests mitigated
57 petabytes of DDoS traffic mitigated
An average of 1,831 attacks every hour

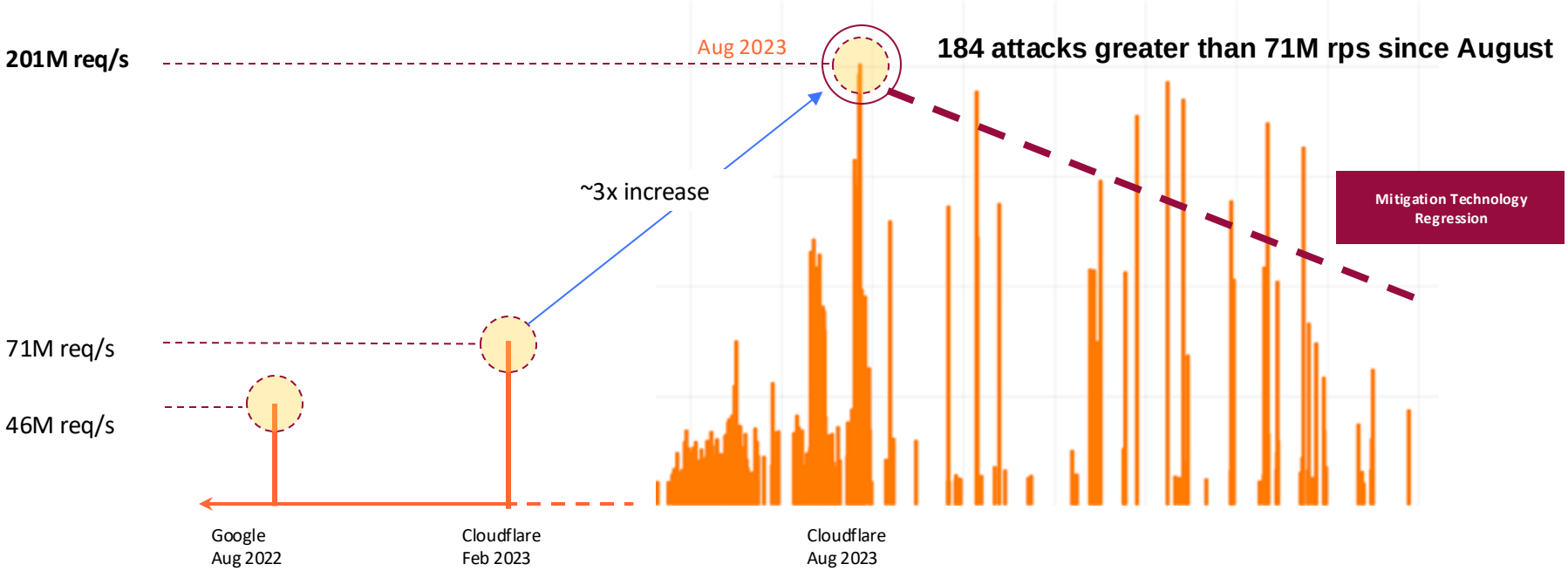
CLOUDFLARE

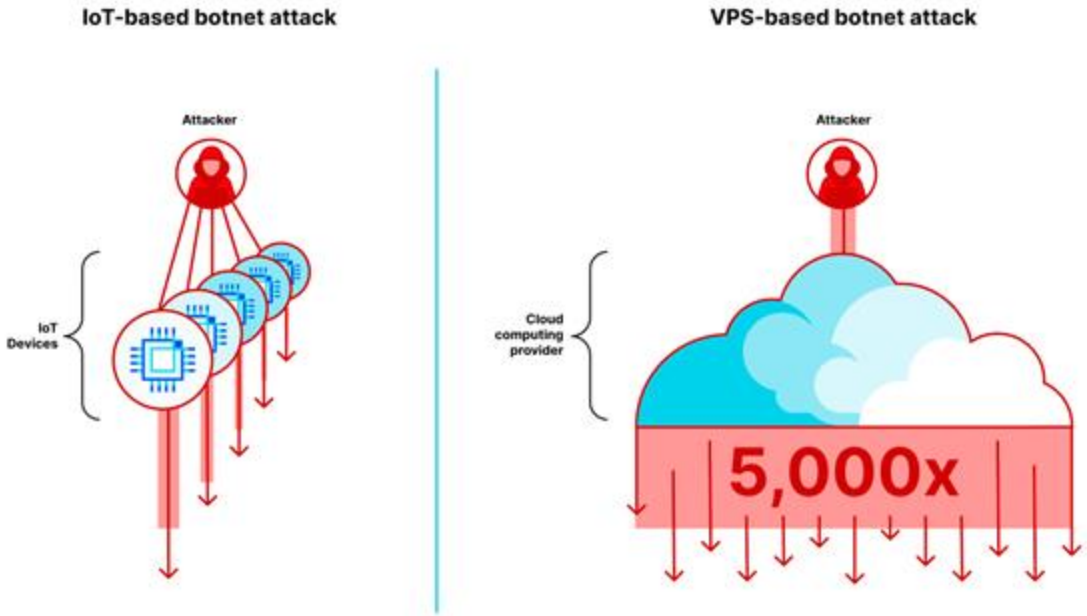
Zero Day Trends

- **97 zero-days** were exploited in the wild in 2023 with a **22-Minute** time to exploit
- # of CVEs between 2022 and 2023 increased by **15%**
- **More than 5000 critical vulnerabilities** were disclosed in 2023, yet the mean time to release a patch for a critical severity web application vulnerability is **35 days**

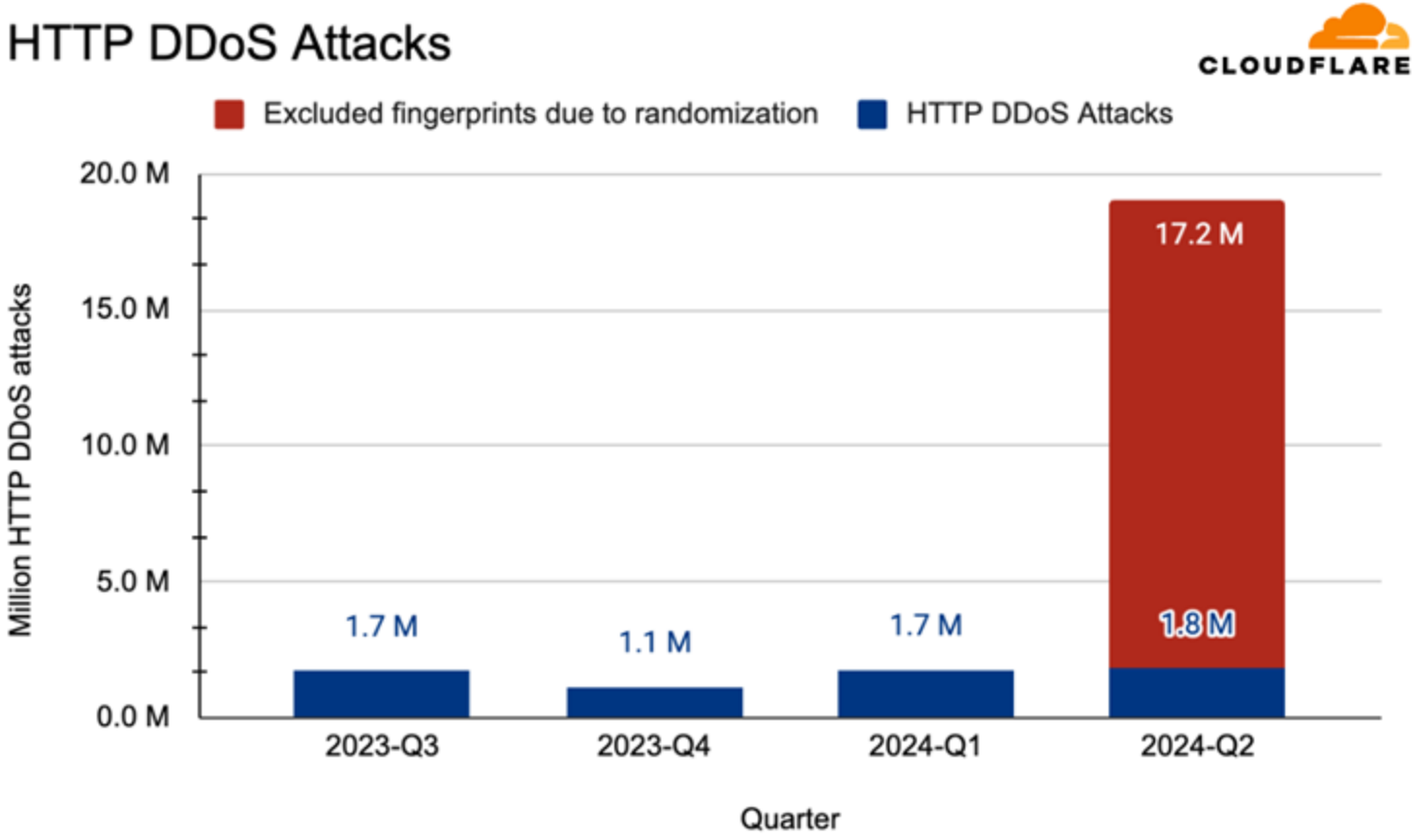


Cloudflare was attacked and we mitigated against the largest HTTP DDoS attack on our record




IoT-based botnet attack
Attacker
IoT Devices
VPS-based botnet attack
Attacker
Cloud computing provider
5,000x

HOW BAD IS IT? - MORPHING



CLOUDFLARE

Web Applications

201M rps

Largest HTTP DDoS Attack on Record

CLOUDFLARE

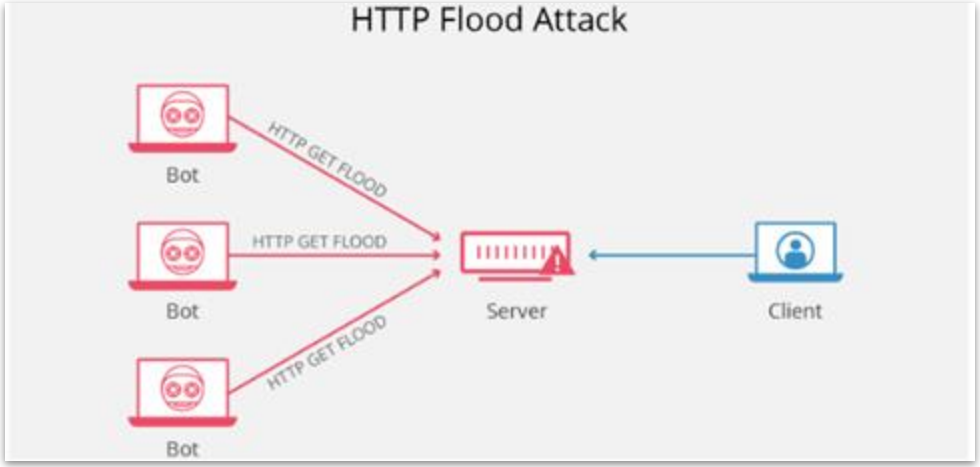
The Role of Web Applications

- **Web Applications** (i.e. websites) act as your public internet facing presence
  - Users engage with your apps as a way to engage with you
  - Your website is your brand
- **How** do users leverage websites?
  - Users may use your website to engage, registrar for a class, check payroll, etc…
  - These users may be anonymous or restricted to trusted users based on the application
- Securing **Websites** is essential in Public Sector

CLOUDFLARE

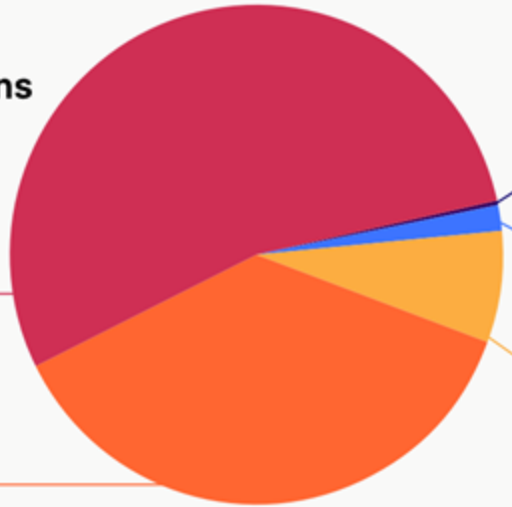
HTTP Flood

- Ex. Overwhelm websites with seemingly normal HTTP GET requests
- Resource Consumption
  - Low Cost - Client Request
  - High Cost - Server Response
- Brings operations to a halt



WAF product mitigations also took over as the No. 1 mitigation technique — a spot that DDoS protections previously held.

Figure 1: Mitigated traffic by Cloudflare product group[9]



57%
WAF and Bot mitigations
(includes OWASP top 10 rules, rate limit rules, exposed credential checks, custom rules, uploaded content scanning, and more)

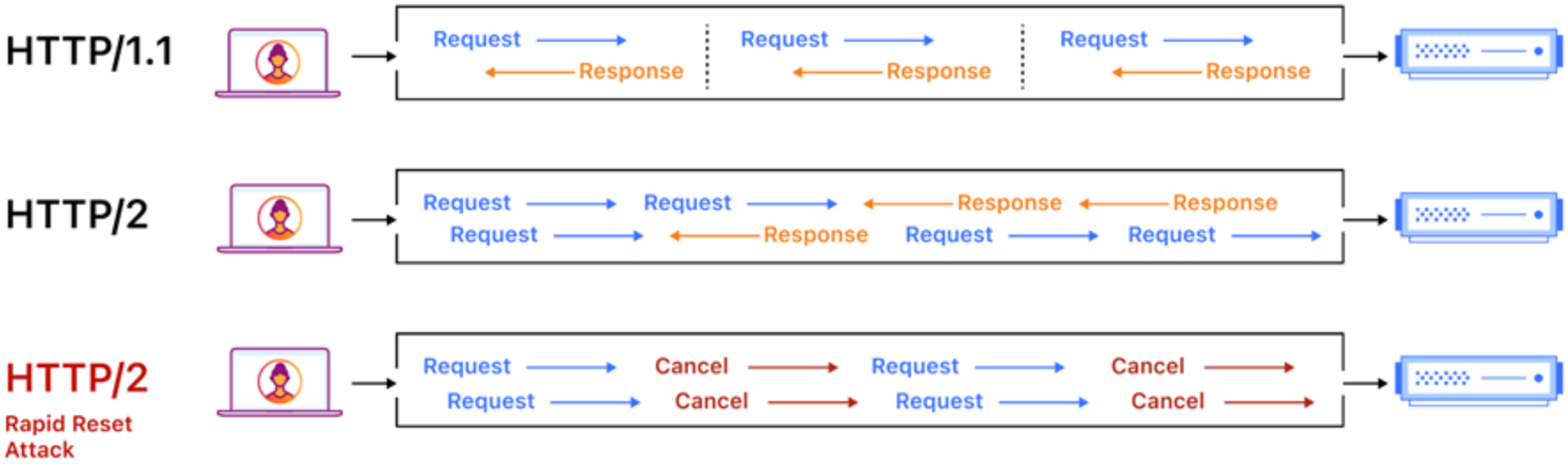
37.1%
HTTP DDoS rules

.01%
Other

1.7%
Access rules

7.2%
IP Reputation

HTTP/2 Rapid Reset attack exploit



DNS

37%

#1 Network DDoS Attack Vector

CLOUDFLARE

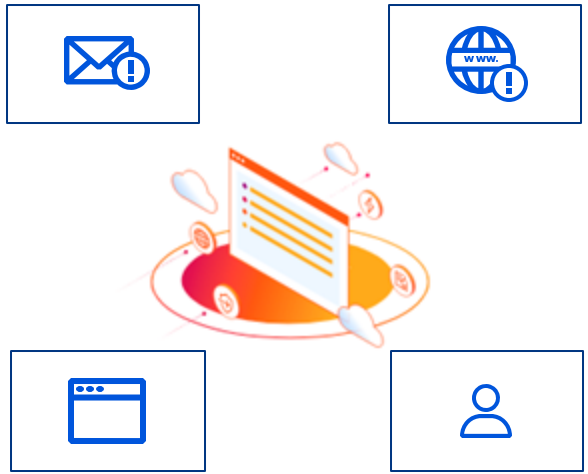
The Role of DNS

- **DNS** is the phonebook of the Internet
  - Humans can understand and memorize domain names easily compared to IP addresses
- **DNS** is a Mission-critical Component for Any Online Business
  - Without DNS, it would be almost impossible to find any website

CLOUDFLARE

Impact from DNS Outage

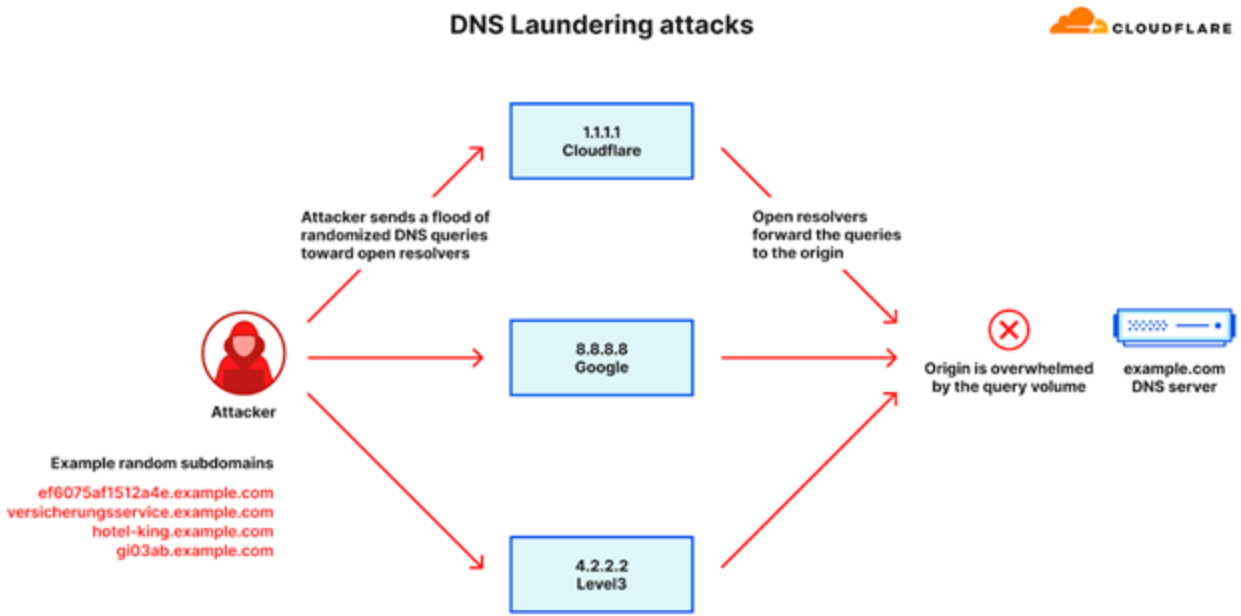
- **Websites** are inaccessible
- **Emails** Stop
- **Remote Users** can't connect (VPN / ZT)



The majority of your infrastructure's core function is powered by DNS

CLOUDFLARE

Volumetric Attacks

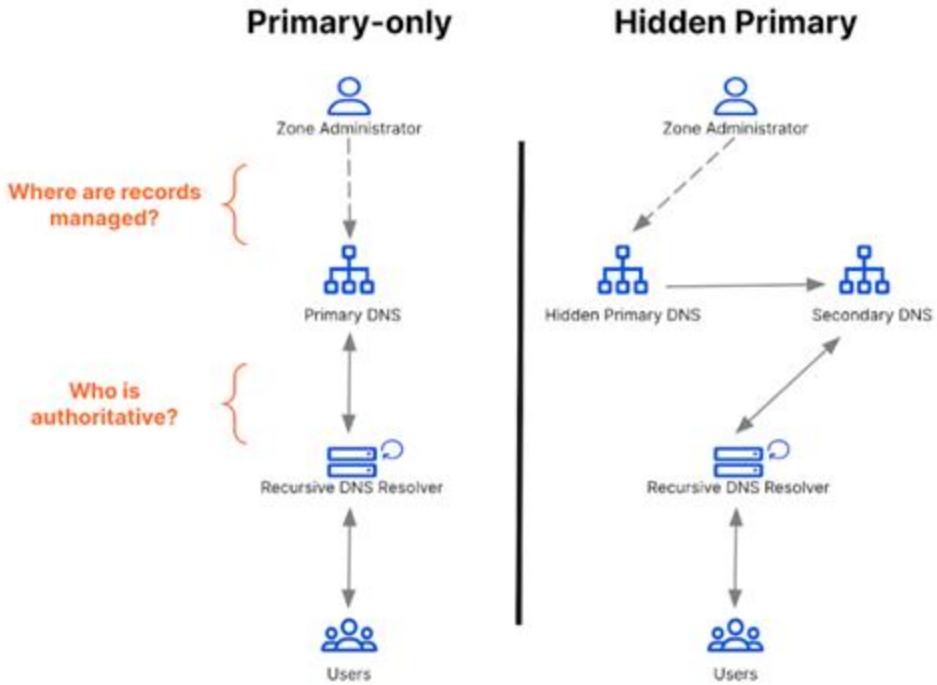


A DNS Amplification attack is like if someone were to call a restaurant and say “I’ll have one of everything, please call me back and tell me my whole order,” where the callback phone number they give is the target’s number. With very little effort, a long response is generated.

CLOUDFLARE

Ways to Protect DNS Servers

- Managed DNS Provider
  - Primary Setup
  - Secondary Setup



Networks

1.4Tbps

Highest Average Bandwidth of L3 DDoS Attack in 1H 2023

CLOUDFLARE

What is your Network and why is it important?

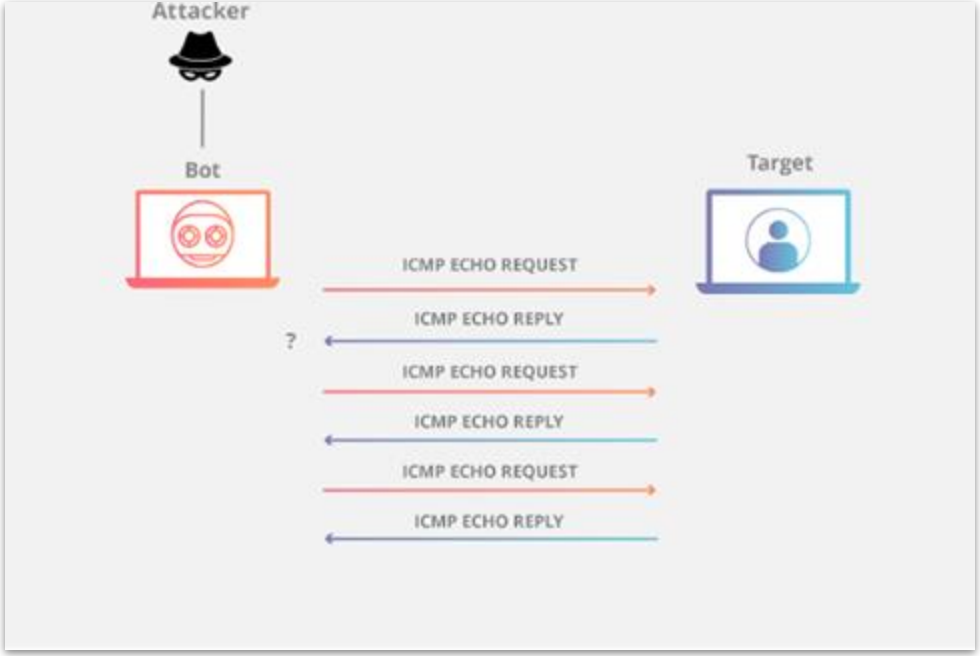
- What is your public IP footprint? What resources do you have tied to Public IPs?
  - Beyond DNS & websites - things like VPNs, email, & any other service could be tied to a public routable IP and potentially could be targeted by DoS

- To get started **Protecting your Network:**
  - Identify what resources are tied to a public routable IP
    - *Ask yourself: "Can I reduce the number of public routable IPs associated with resources?"*
  - How would my network be protected from DoS?
    - Is your network equipment built to withstand? Are you relying on your ISP? Some other solution?

CLOUDFLARE

Ping (ICMP) Flood

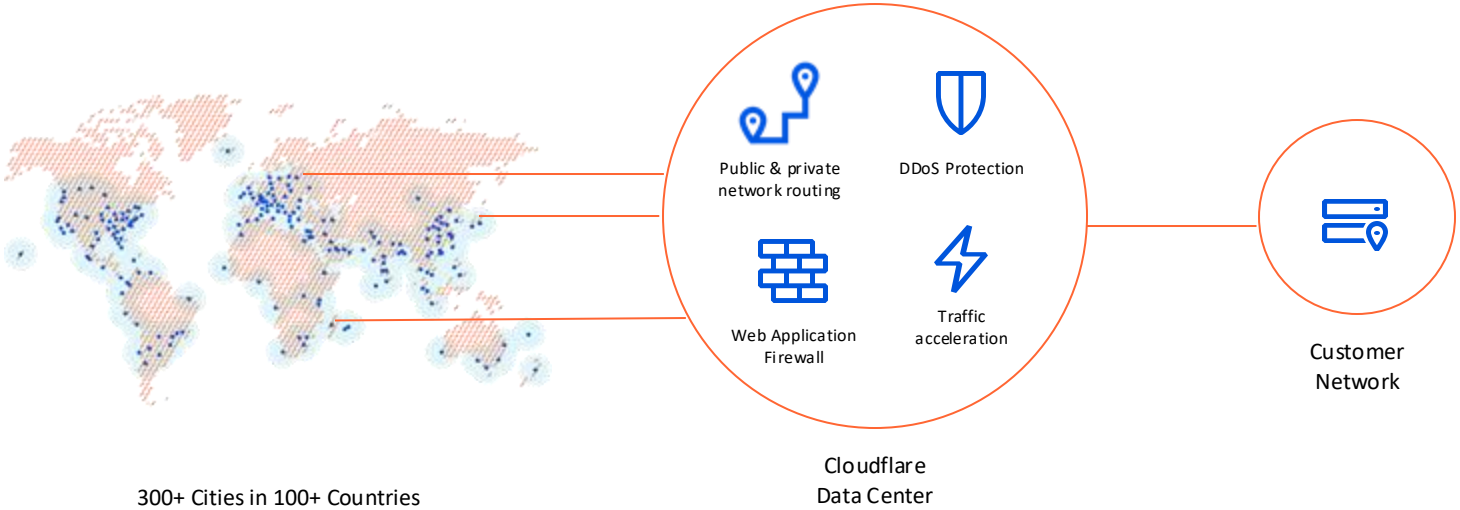
- Typically attackers leverage a botnet to use sheer volume of pings as a mechanism to bring down a single IP within your network
- High enough L3 DDoS related traffic can saturate your circuits
- Brings operations to a halt



Section

Protection and Prevention Strategies

Cloudflare's network as an extension of yours



https://www.cloudflare.com/2024-application-security-trends/

CLOUDFLARE

773%

Increase in size of largest DDoS attack

From 26 million requests per second in 2022, to 201 million in 2023

33%

More APIs found via ML than what orgs self-reported

Organizations have larger API attack surface than they think

75%

Of orgs adopting Zero Trust **plan to or have replaced VPN** for all employees*

22 minutes

from POC to exploitation

Vulnerability weaponization is accelerating

Phishing is still the #1 initial attack vector

*Source: IT & security professionals implementing Zero Trust. Enterprise Strategy Group, a division of TechTarget, Inc. Research Survey, Cloudflare Zero Trust for the Workforce Survey, May 2024.

Cloudflare Radar

https://radar.cloudflare.com

Cloudflare Radar

Search for locations, autonomous systems, reports, domain and IP address information

- Overview
- Traffic
- Security & Attacks
- Adoption & Usage
- Internet Quality
- Routing
- Domain Rankings
- Email Security New
- Outage Center
- URL Scanner
- My Connection
- Reports
- API

Report

← Back to reports

DDoS threat report for 2024 Q2

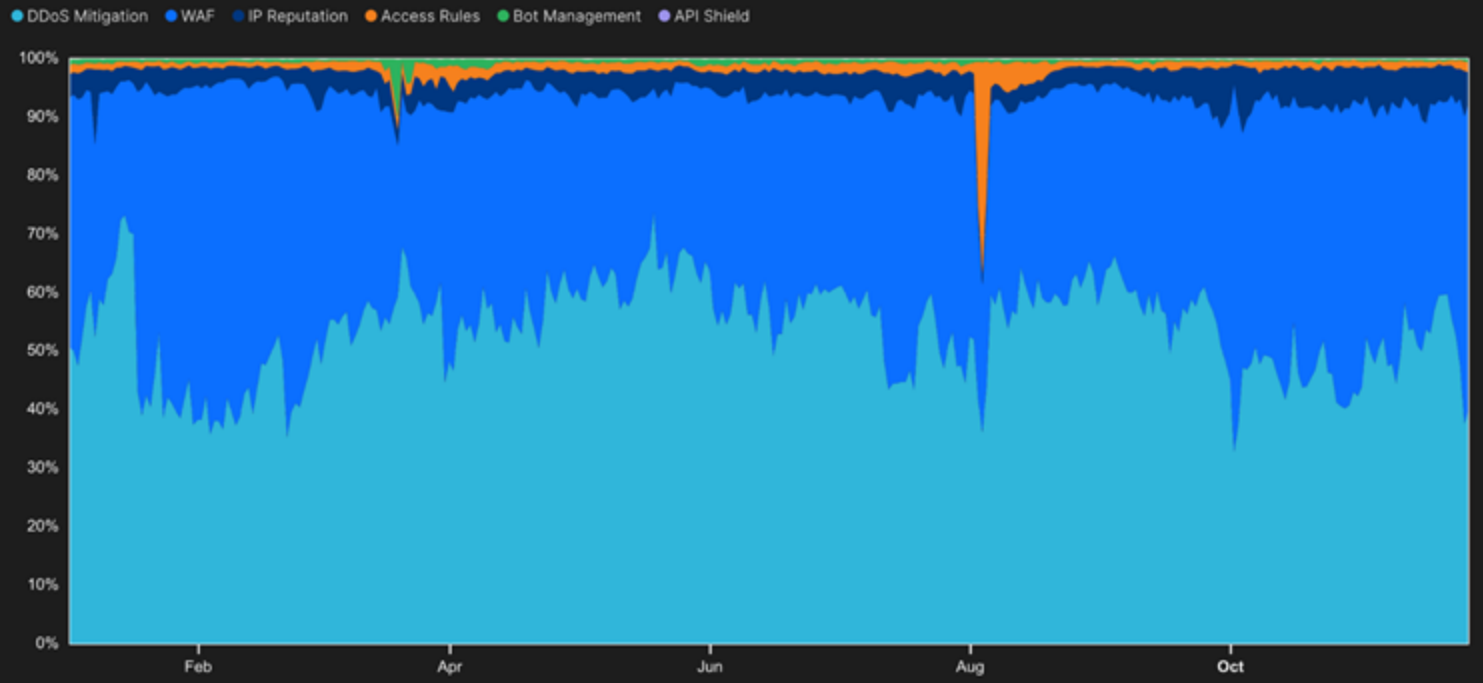
Cloudflare automatically detects and mitigates DDoS attacks across its global network using its autonomous edge DDoS detection and mitigation engine. This report includes the DDoS insights and trends as observed on our network.

90%+

of mitigated traffic used the WAF or DDoS mitigation techniques

DDoS mitigation techniques and Web Application Firewalls are the two most effective defences against Application Layer (Layer 7) attacks. These attacks can take a high traffic website down for hours or steal customer data.

The graph shows the percentage of attacks mitigated by each product group on a daily basis.



https://radar.cloudflare.com/year-in-review/2022#approaches-to-attack-mitigation

https://radar.cloudflare.com/security-and-attacks

Questions?

Steve Carlson

916.426.8242

scarlson@cloudflare.com

www.cloudflare.com

Thank you

Comprehensive Protection Against Cyber Attacks.

Cyber Emergency Hotline: +1 (866)-325-4810

Scott Reilly, California Client Executive

916.390.4946

sreilly@cloudflare.com
publicsector@cloudflare.com

Jenna Bodie, Named Account Executive

219.682.4579

jbodie@cloudflare.com
publicsector@cloudflare.com