June 2023

CLOUDFLARE

Protecting Critical Infrastructure against Ransom DDoS Attacks

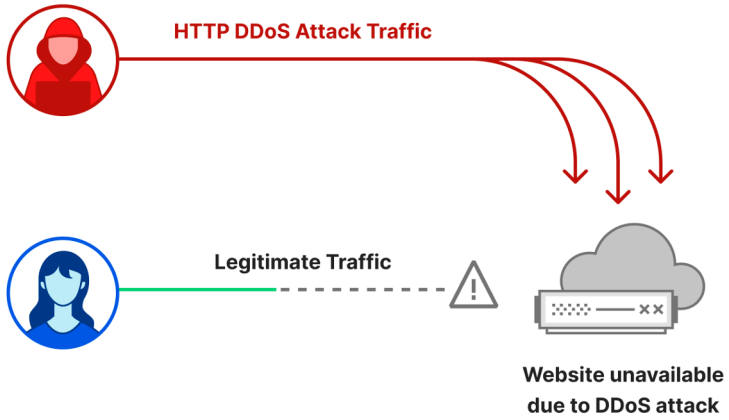
Omer Yoachimik
Senior Product Manager
DDoS Protection

Quick Recap

What is a DDoS attack?

DDoS = *Distributed Denial of Service*

- A type of cyber attack that aims to take down Internet properties and make them unavailable for users by sending it more Internet traffic than it can handle.
- These types of cyberattacks can be very efficient against unprotected websites and they can be very inexpensive for the attackers to execute.



GOVERNMENT & PUBLIC SECTOR | SECURITY

DDoS attacks block PM Trudeau's web site

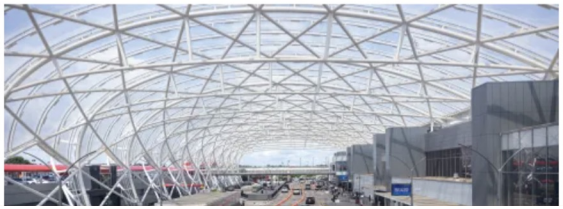
HOWARD SOLOMON APRIL 11, 2023

CNN US Live TV

Russian-speaking hackers knock multiple US airport websites offline. No impact on operations reported

By Greg Wallace, Sean Lyngaas, Pete Muntean and Michelle Watson, CNN

Updated 11:50 AM EDT, Mon October 10, 2022



SC MEDIA
A CyberRisk Alliance Resource
LOG IN REGISTER

Anonymous Sudan claims DDoS attacks against Microsoft Outlook

SC Staff June 8, 2023

HACKREAD

IoT Botnet DDoS Attacks Threaten Global Telecom

Search

CYBERSECURITY CONNECT

Home / Industry /

CYBER ATTACK THE MAIN FEAR FOR EUROVISION ORGANISERS

SC MEDIA
A CyberRisk Alliance Resource
LOG IN REGISTER

Passion botnet cyberattacks hit healthcare, as actors offer threat as DDoS-as-a-service

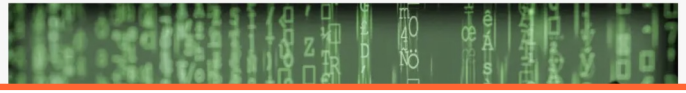
Jessica Davis February 2, 2023

THE JERUSALEM POST ISRAEL NEWS HEALTH & WELLNESS WORLD NEWS MIDDLE EAST BUSINESS & INNOVATION

Israeli cyber security website briefly taken down in cyberattack

The websites of multiple major universities in Israel were attacked by a group of hackers calling themselves 'Anonymous Sudan.'

By JERUSALEM POST STAFF **Published:** APRIL 4, 2023 11:29
Updated: APRIL 27, 2023 17:22



yahoo! Get App

Microsoft Azure Users Face Service Disruption Amid Reports Of DDoS Attack

Anusuya Lahiri

Fri, June 9, 2023 at 3:41 PM EDT · 1 min read

US government seizes 13 domains linked to DDoS attacks

The DDoS-attack-for-hire sites have been accessed by hundreds of thousands of users

Olivia Powell

05/22/2023

There have been
so many DDoS campaigns lately
that it's hard to even keep track! 😖

Setting the stage

The DDoS threat landscape

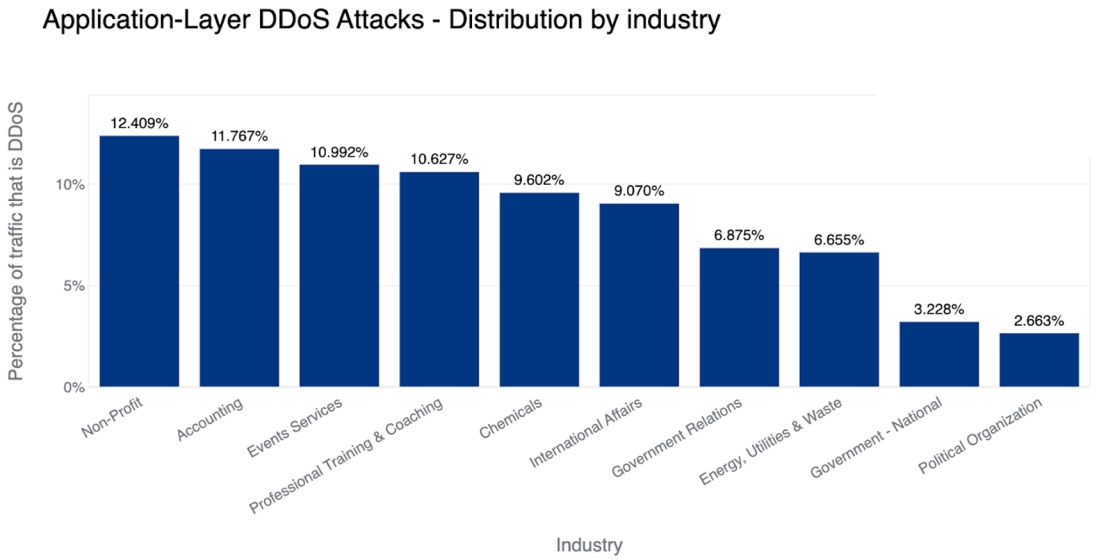
Global DDoS attack insights

- **The majority of attacks are short and small (*cyber vandalizim)***
  - 86% end within 10 minutes
  - 91% never exceed 500 Mbps
  - 1 out of 50 attacks exceeds 10 Gbps
  - 1 out of 1,000 attacks exceeds 100 Gbps
- **While still the outlier, large and hyper-volumetric attacks are growing**
  - Attacks >100 Gbps increased by 67% QoQ
  - New record broken (71M rps) which is 54% larger than the previous
  - Attacks in the 40-60 minute range increased by 63% QoQ

Based on L3/4 DDoS attacks in 2023 Q1.

🏭 Top attacked industries (L7 HTTP)

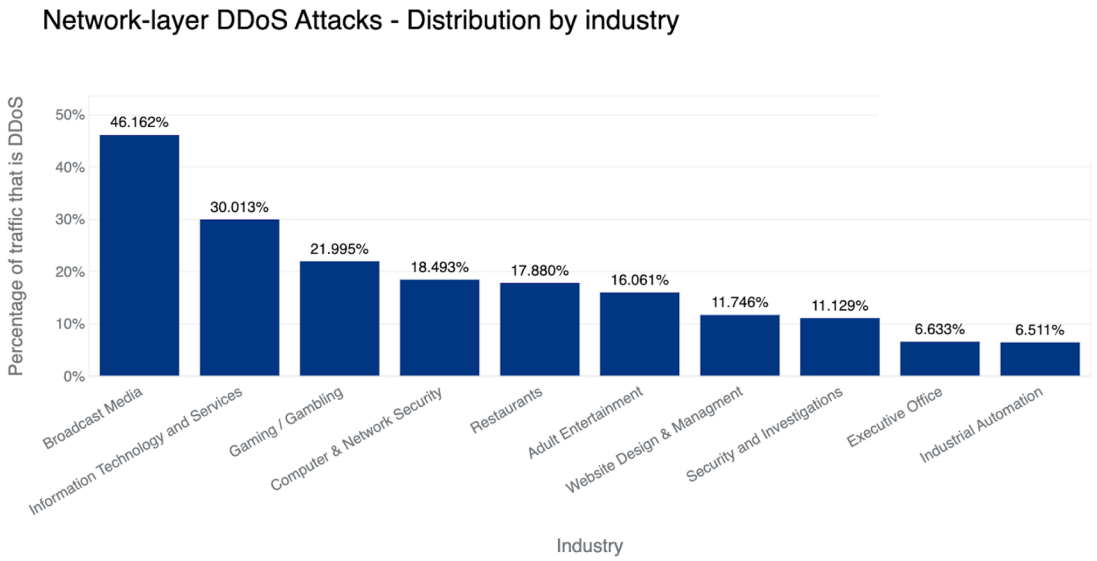
1. Nonprofits **12%**
2. Accounting **12%**
3. Events Services **11%**



Percentage of HTTP DDoS attack traffic out of all HTTP traffic to each customer industry for 2023 Q1.

🏭 Top attacked industries (L3/4)

1. Broadcast Media **46%**
2. IT & Services **30%**
3. Gaming / Gambling **22%**



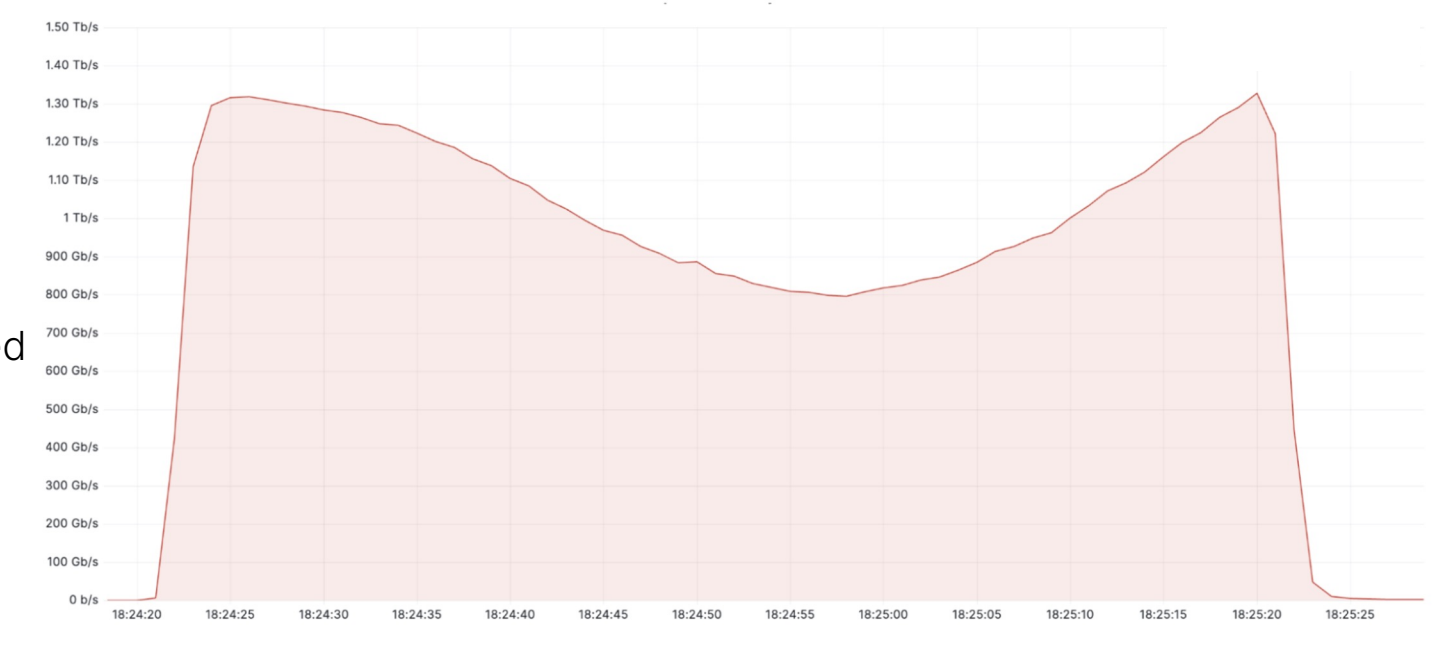
Percentage of network-layer DDoS attack traffic out of all network traffic to each customer industry in 2023 Q1.

🏭 Top attacked industries by region (L7 HTTP)

Percentage of HTTP DDoS attack traffic out of all HTTP traffic to each customer industry by region for 2023 Q1.

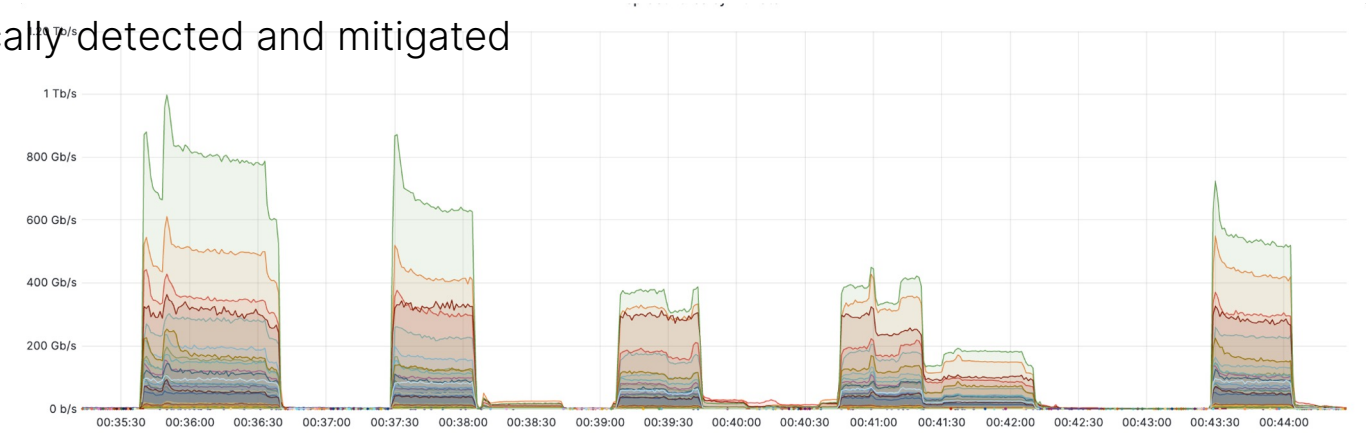
South American Telco attacked

- 1.3 Tbps
- Lasted one minute
- Multivector
- Mirai botnet
- Automatically detected and mitigated



A different South American Telco attacked again

- This time a little lower, only 1 Tbps
- Each blast lasted 1 minute
- A more sophisticated Mirai botnet - randomizes almost everything
- Multi vector: various kinds of GRE floods and UDP floods, Valve Source Engine traffic flood, Mirari TCP, Portmap flood, VXWorks traffic flood
- Automatically detected and mitigated



🌍 Top attacked countries

L3/4

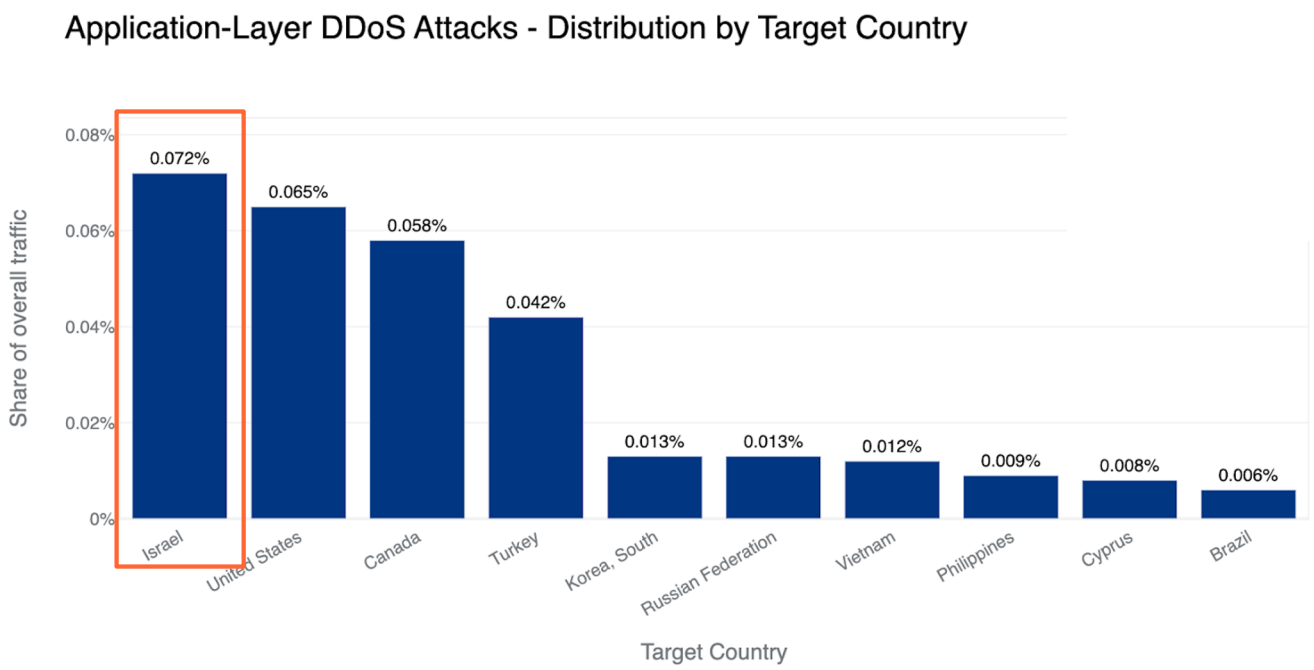
1. Finland **83%**
2. China **68%**
3. Singapore **49%**

L7 (HTTP)

1. Slovenia **19%**
2. Georgia **18%**
3. Saint Kitts and Nevis **7%**

Percentage of DDoS attack traffic out of all traffic to each customer billing country in 2023 Q1.

🇮🇱 Top attacked country by overall traffic



Percentage of DDoS attack traffic out of all of Cloudflare's traffic in 2023 Q1.

🌍 Top source countries

L3/4

1. Vietnam **25%**
2. Paraguay **24%**
3. Moldova **20%**

Based on ingesting Cloudflare data center

L7 (HTTP)

1. Finland **16%**
2. Virgin Islands **14%**
3. Libya **12%**

Based on client IP

Percentage of DDoS attack traffic out of all traffic from each client country or data center.

👾 Top attack vectors & emerging threats

Top vectors

1. DNS floods/reflections **30%**
2. SYN floods **22%**
3. UDP floods/reflections **21%**

Share of attack vectors out of all vectors.

Emerging threats

1. SPSS reflections **+1,565%↑**
2. DNS amplifications **+958%↑**
3. GRE floods **+835%↑**

The changes are quarter-over-quarter.

Emerging threats worth highlighting

Emerging threats worth highlighting

📣 The main threats worth your attention

Highly-randomized HTTP DDoS attacks

- Sophisticated threat actors
- Excel at immitating browser behavior (headers, ua, orders)
- Attackers randomizing or imitating legit JA3

Examples of targets:

- A major VoIP provider
- A dominant semiconductor co,
- Top tier payment & CC provider

DNS Laundering DDoS attacks

- “Laundering” queries off of legit DNS resolvers such as Google’s 8.8.8.8 and Cloudflare’s 1.1.1.1
- Random-prefix queries of real domains managed by the target DNS server

Example of targets:

- A large Asian financial institution
- A North American DNS provider

VPS-based DDoS botnets

- Botnets built of Virtual Private Servers (VPS) instead of Internet of Things (IoT) devices.
- Much smaller botnet fleet size, but each VPS-bot is up to 5x more powerful than IoT bots.

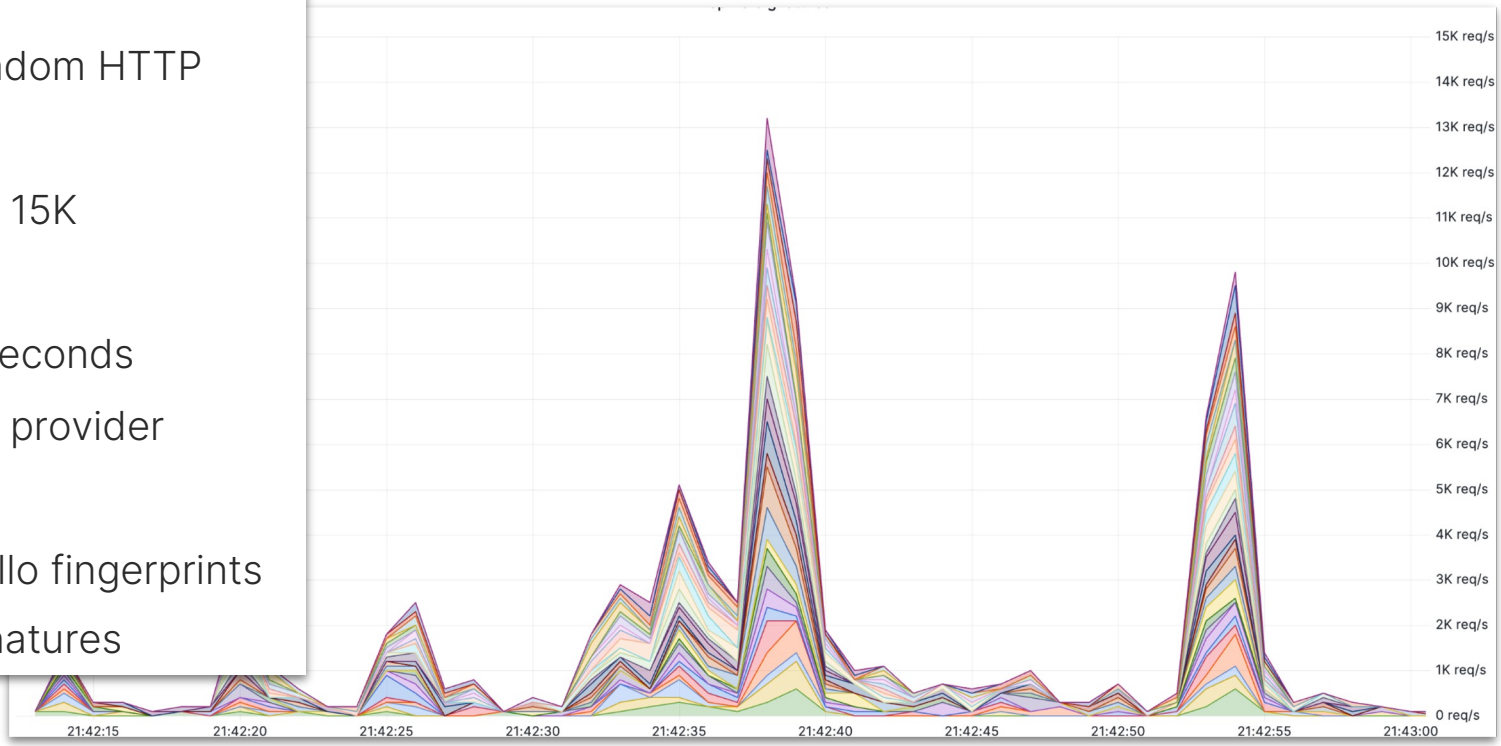
Examples of targets:

- Industry leading gaming platform provider

Example: Highly-randomized HTTP DDoS attacks

Attack stats:

- **Attack vector:** Random HTTP GET Flood
- **Botnet fleeet size:** 15K
- **Rate:** 13K rps
- **Shortest peak**: 3 seconds
- **Target**: Major VoIP provider
- **Randomization:**
  - 681 Client Hello fingerprints
  - 31 attack signatures



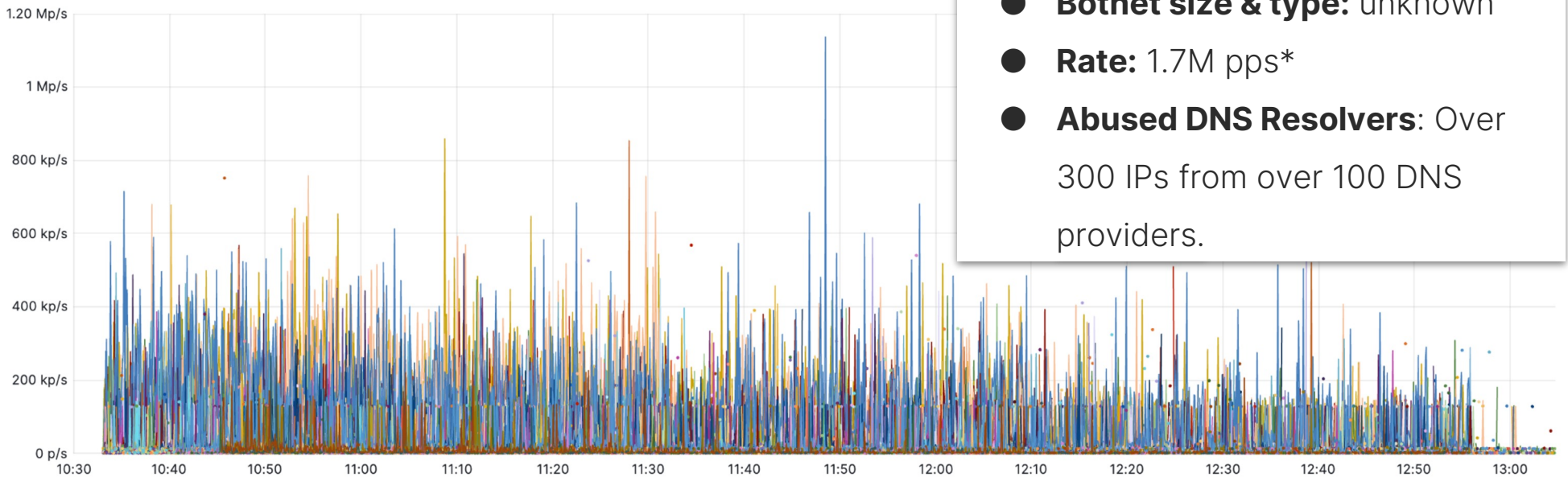
* Note: The max peak is not visible in this graph due to sampling

Emerging threats worth highlighting

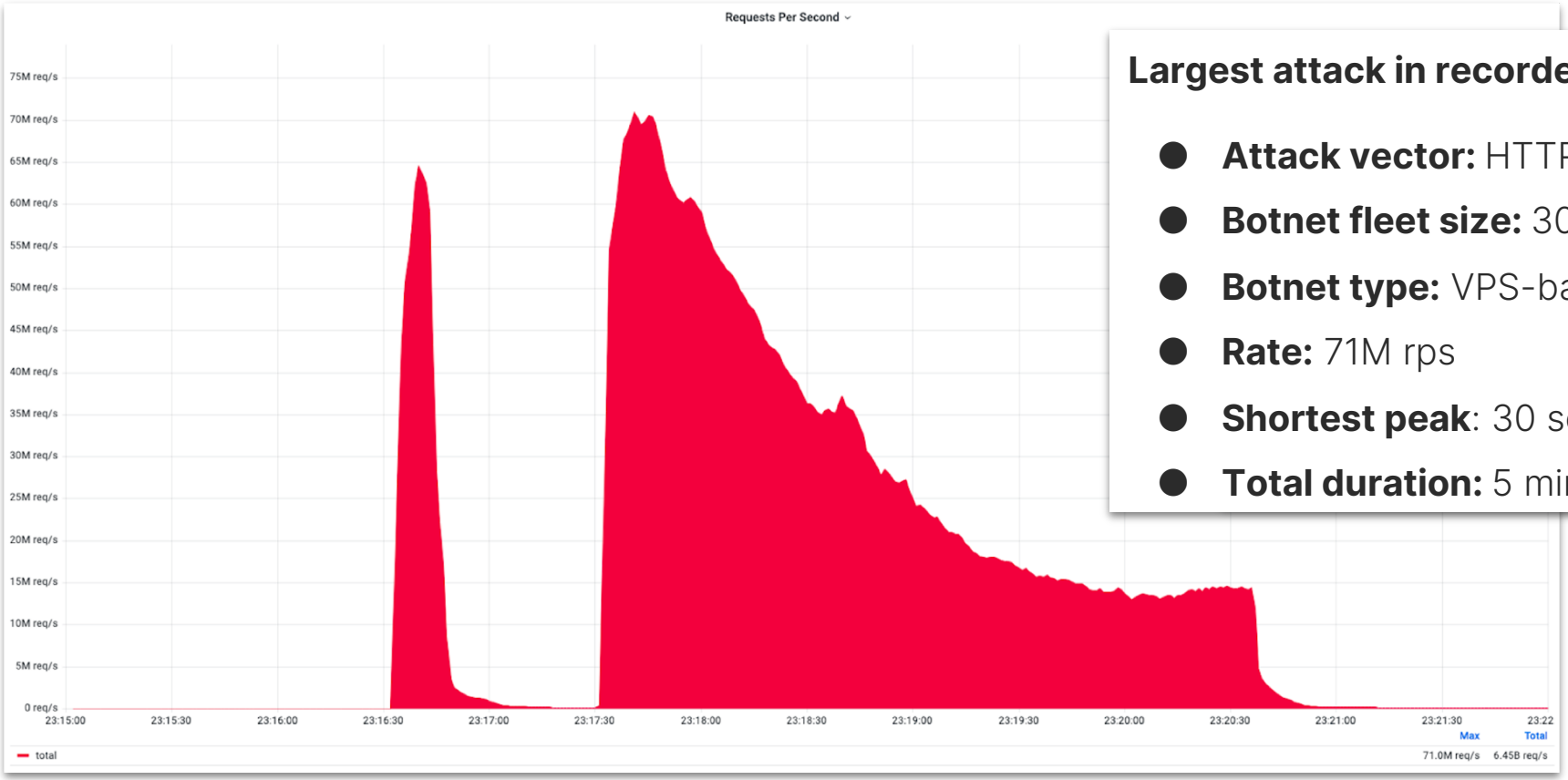
Example: DNS Laundering DDoS attacks

Attack stats:

- **Attack vector:** DNS reflection (Random-prefix Laundering)
- **Botnet size & type:** unknown
- **Rate:** 1.7M pps*
- **Abused DNS Resolvers**: Over 300 IPs from over 100 DNS providers.



Example: VPS-based DDoS botnets



Largest attack in recorded history

- **Attack vector:** HTTP/2 Flood
- **Botnet fleet size:** 30K
- **Botnet type:** VPS-based
- **Rate:** 71M rps
- **Shortest peak**: 30 seconds
- **Total duration:** 5 minutes

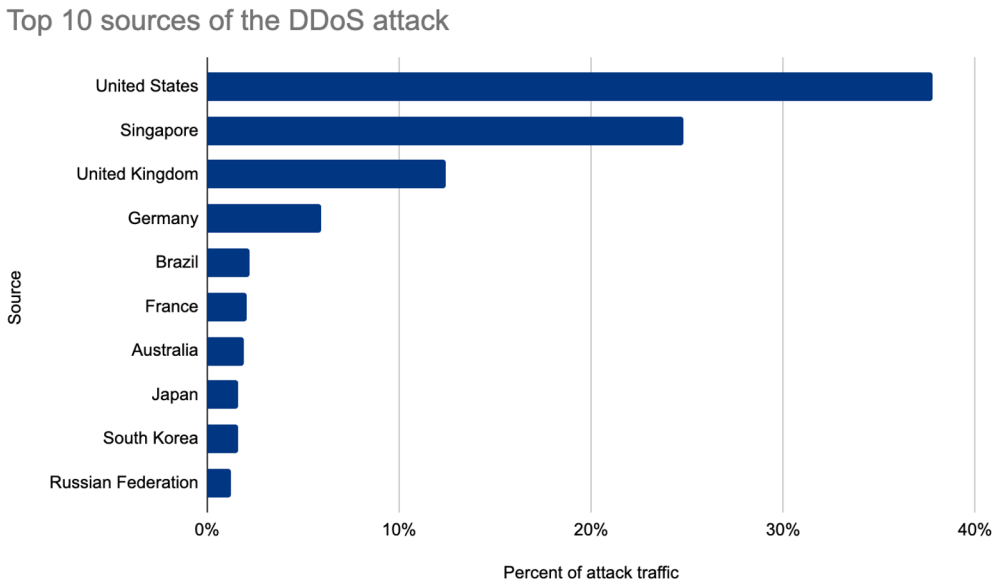
Top sources of the 71M rps DDoS attack

The top 3 sources:

1) USA 38%
2) Singapore 25%
3) United Kingdom 18%

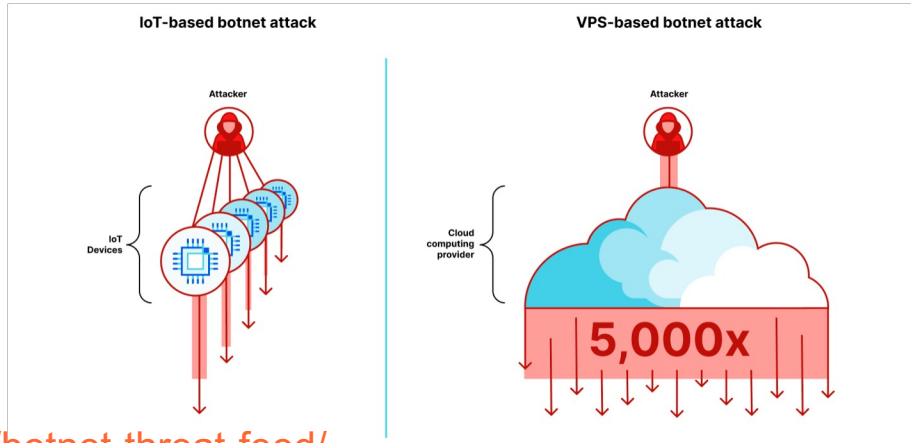
The top 10 countries accounted for 92% of the attack traffic.

The majority of the traffic came from a single network in the US.



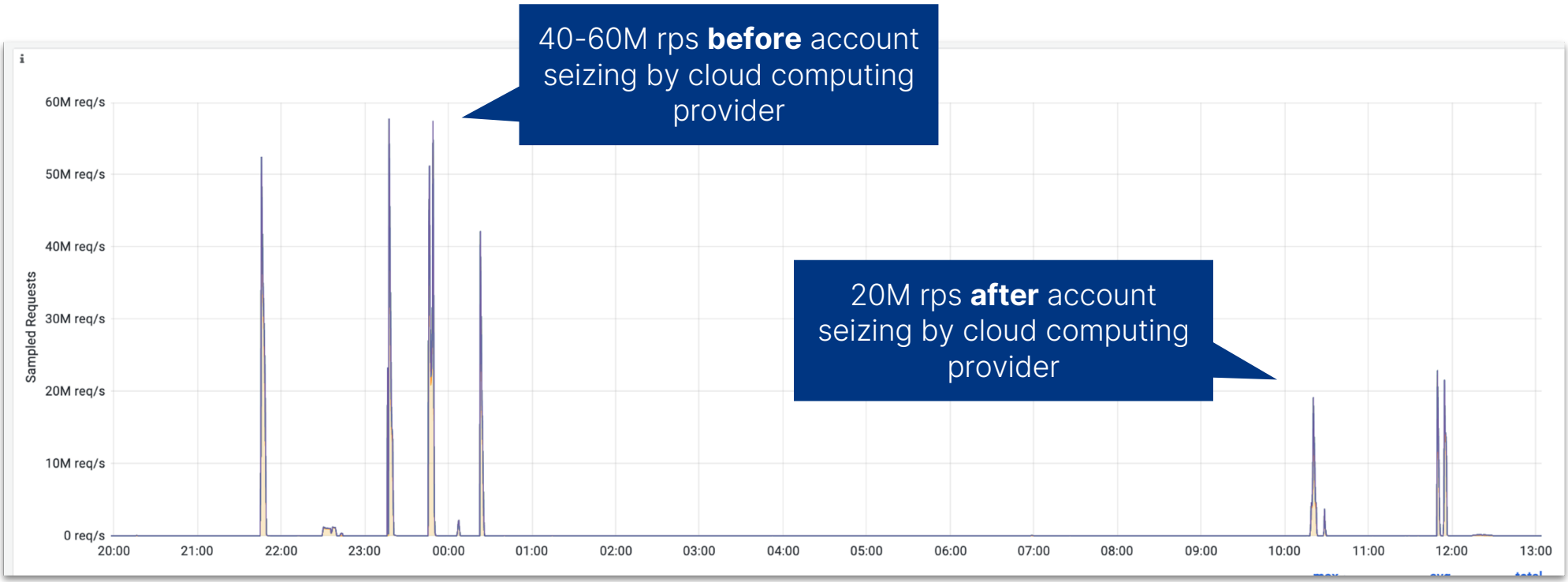
Working with the infosec community to takedown the botnet

- At least 50% of the botnet capabilities and force have been disabled.
- Cloud computing accounts associated with the attacks have been seized and disabled
- We have yet to see significant attacks originating from this botnet since, which could indicate a takedown or impact to the botnet capabilities



Free threat feed for ISPs:
https://www.cloudflare.com/lp/botnet-threat-feed/

Working with the infosec community to takedown the botnet



Fortune Global 500 company targeted by Ransom DDoS attack

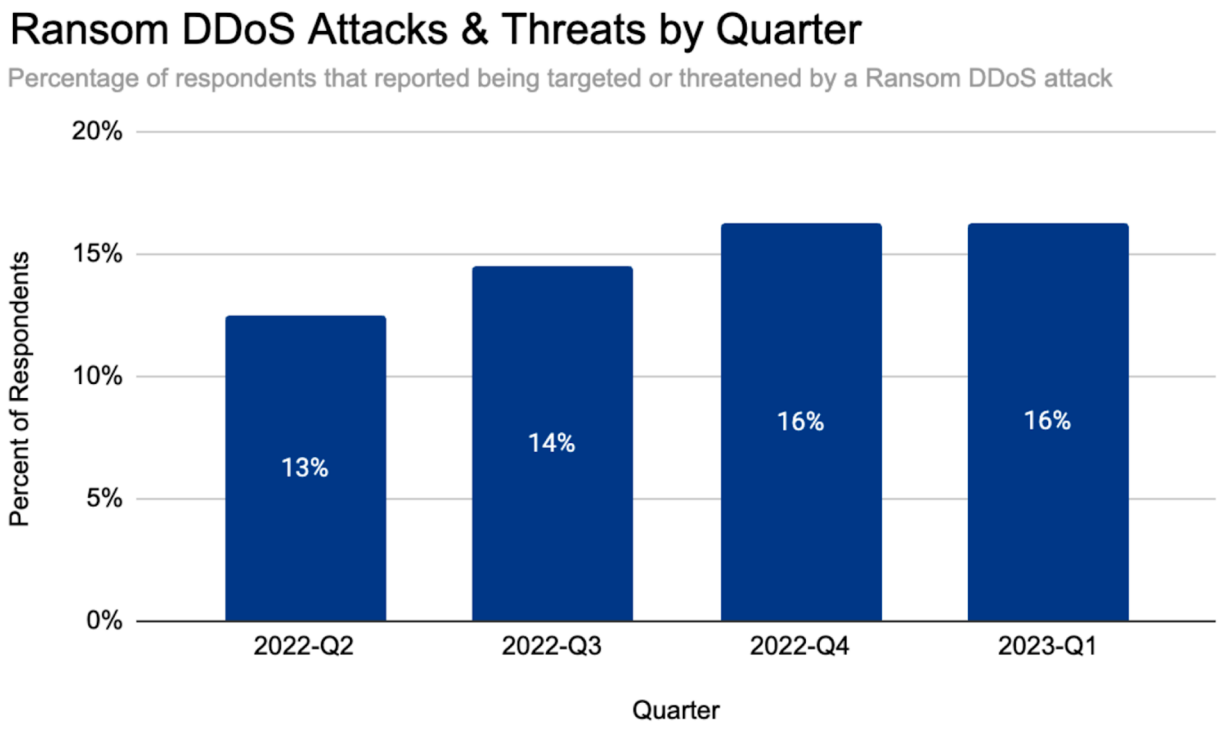
Fortune Global 500 company targeted by Ransom DDoS attack

Ransomware vs. Ransom DDoS?

	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

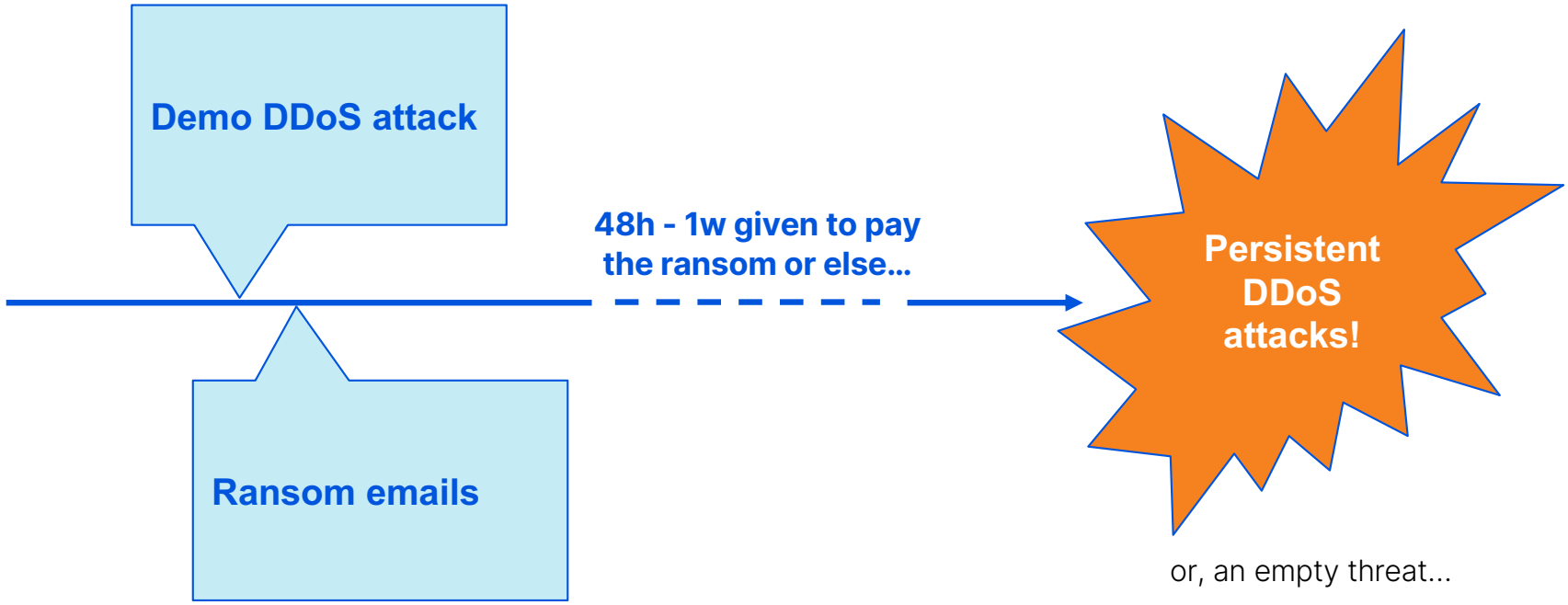
Fortune Global 500 company targeted by Ransom DDoS attack

Ransom DDoS Trend



Percentage of Cloudflare customers that experienced an HTTP DDoS attack and responded to a survey and reported being ransomed or threatened in advance.

Ransom DDoS Timeline



or, an empty threat...

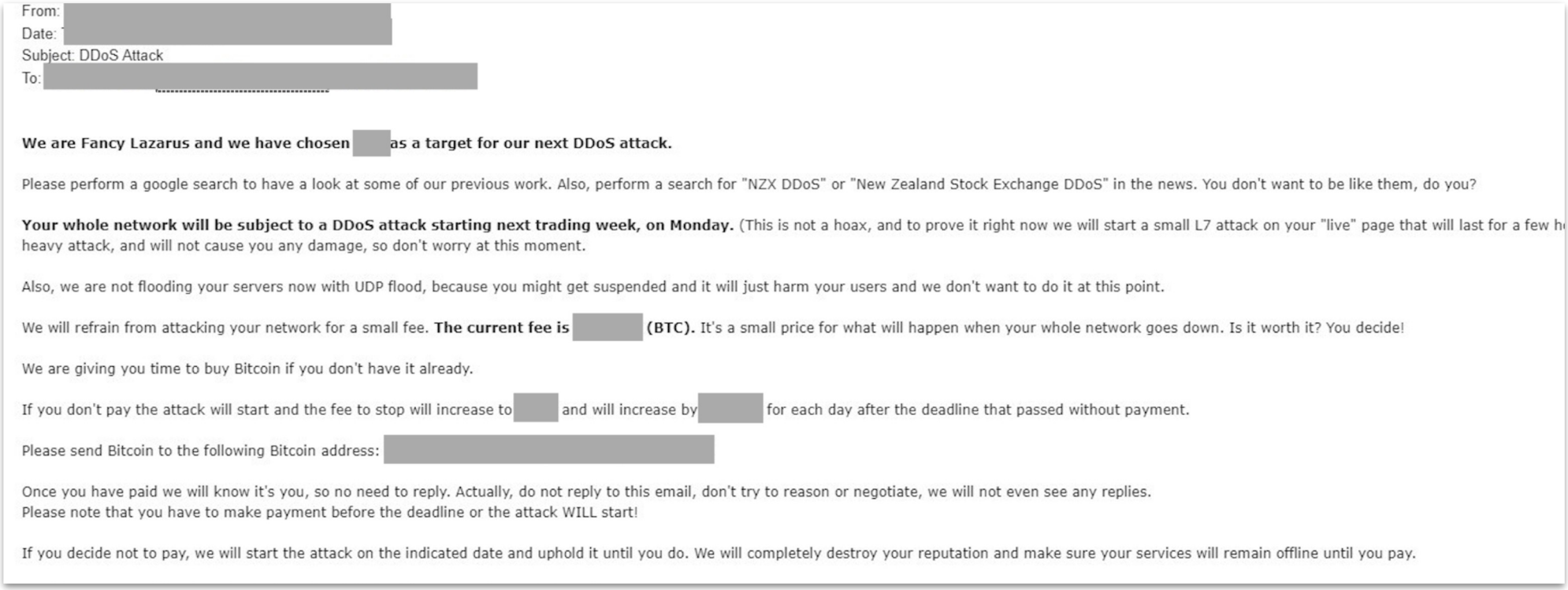
Pre-attack posture and readiness

- Alerts on data center CPU and bandwidth utilization
- Relied on ISP for out-of-path scrubbing
  - Haven’t used it in a while
  - ISP didn’t provide reporting
  - ISP didn’t know how to mitigate the attack
  - ISP clocked out when the workday ended (no follow-the-sun model)
  - Diversion impacted IPSec traffic
- No inline DDoS detection/alerts/visibility
- Staff wasn’t drilled, no DDoS runbooks

1. The demo attack

Target	The attack targeted one of their data centers
Duration	60 minutes
Size	80 Gbps (sustained)
Vector	Multivector: UDP, mDNS, SYN, other
Impact	Outage due to link saturation. It took the ISP 30 minutes to mitigate.

2. The ransom email (example)



From: [redacted]
Date: [redacted]
Subject: DDoS Attack
To: [redacted]

We are Fancy Lazarus and we have chosen [redacted] as a target for our next DDoS attack.

Please perform a google search to have a look at some of our previous work. Also, perform a search for "NZX DDoS" or "New Zealand Stock Exchange DDoS" in the news. You don't want to be like them, do you?

Your whole network will be subject to a DDoS attack starting next trading week, on Monday. (This is not a hoax, and to prove it right now we will start a small L7 attack on your "live" page that will last for a few h
heavy attack, and will not cause you any damage, so don't worry at this moment.

Also, we are not flooding your servers now with UDP flood, because you might get suspended and it will just harm your users and we don't want to do it at this point.

We will refrain from attacking your network for a small fee. **The current fee is [redacted] (BTC).** It's a small price for what will happen when your whole network goes down. Is it worth it? You decide!

We are giving you time to buy Bitcoin if you don't have it already.

If you don't pay the attack will start and the fee to stop will increase to [redacted] and will increase by [redacted] for each day after the deadline that passed without payment.

Please send Bitcoin to the following Bitcoin address: [redacted]

Once you have paid we will know it's you, so no need to reply. Actually, do not reply to this email, don't try to reason or negotiate, we will not even see any replies.
Please note that you have to make payment before the deadline or the attack WILL start!

If you decide not to pay, we will start the attack on the indicated date and uphold it until you do. We will completely destroy your reputation and make sure your services will remain offline until you pay.

Example of a ransom email from a different customer.

3. Deadline expiry

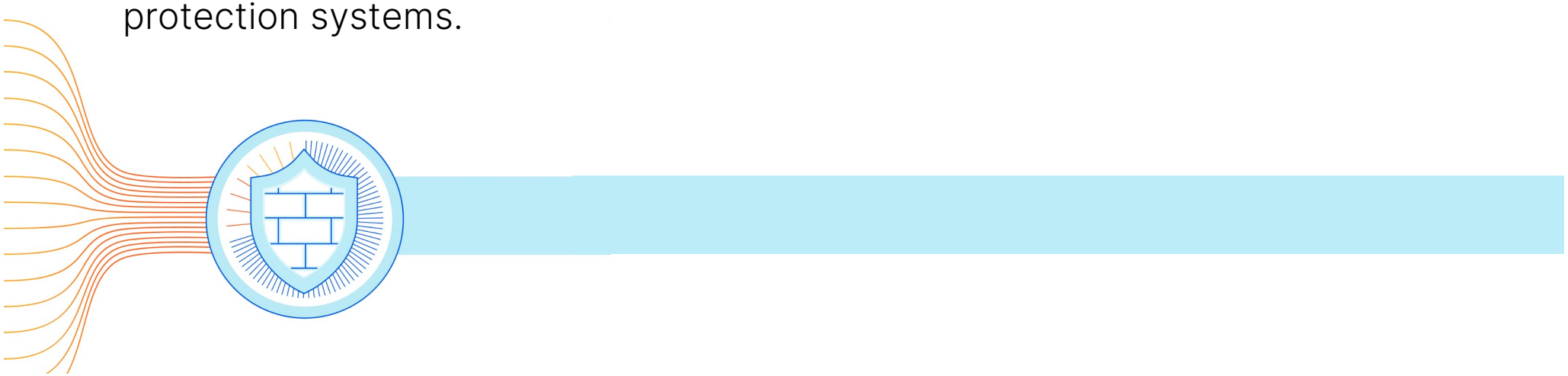
- Onboarded them to our BGP-based routing protection
- Gained real-time visibility and alerting
- Gained (self-service) control over mitigation and firewall
- Tailored mitigation strategy
- Access to follow-the-sun SOC and support

The promised attack never came - empty threat or deterred by detecting inline mitigation?

Lessons Learned from a Fortune Global 500 Company

Lessons Learned #1 - Use an automated & always-on solution

1. Don’t rely on reactive on-demand SOC-based solutions that require human analysis.
2. Don’t be tempted to use on-demand “you get all of the pain and none of the benefits.”
3. Use a cloud service that has sufficient network capacity and automated protection systems.



Lessons Learned #2 - Map your threat model & increase visibility

1. Work together with your DDoS protection vendor to tailor mitigation strategies to your workload.
2. Enforce, as much as possible, a combination of a positive & negative security model.
3. Enable critical alerts and logging — e.g. CPU, bandwidth, DDoS detections.

Lessons Learned #3 - Prepare & raise organizational awareness

1. Build and test emergency response runbooks — who to page, what to do, who to update, etc.
2. Educate and test your employees (even the non techies) — e.g. send fake ransom emails.
3. Encourage reporting of potential security incidents by employees.

Wrapping up & key takeaways

📝 Summary of attack landscape

- Attack durations have increased, volumetric attacks surged and ransom attacks are persisting → While human launch the attacks, bots execute the. So to play to win, you must fight bots with bots
- Sophisticated and coordinated attacks have been observed in the fourth quarter as well as the beginning of the current quarter → We have seen an increase in sophisticated attacks that fall outside the typical cyber vandalism
- Attackers can be very persistent in learning your network topology and identifying weak points → Be aware of smokescreen threats

Main takeaways from the DDoS victim

1. Use an automated & always-on solution
2. Map your threat model & increase visibility
3. Prepare & raise organizational awareness

Best practices

**Mitigate = Block, Rate-limit, Challenge, etc — based on what is most appropriate case by case.*

	Best practice	Examples
1	In-line, automated DDoS detection and mitigation with sufficient capacity, e.g. *2x your largest peaks + 2x largest attack on record*	Dynamic stateless fingerprinting ML-based classification and anomaly detection Traffic profiling and Stateful mitigation
2	Mitigate traffic you never want to see from the outside world	Mitigate certain countries or protocols
	Positive security mode: ensure that traffic you want gets in, always.	Only opening ports that are in use Using Schema Validation for API traffic
3	Leverage Threat Intelligence to mitigate or flag traffic	Bot scores that can be used within firewall and rate-limiting rules
4	Optimize configurations, move the load to the edge and ensure your origin is locked down	Auto-reduce HTTP/2 multiplexing ceiling when under attack, enabling WAF Leverage a digital waiting room Optimize caching, delegate load to the ‘cloud’

Thank you

Stay in touch

@omeryoahimik

omer@cloudflare.com

/omeryoahimik

Read more blog.cloudflare.com/ddos-threat-report-2023-q1/.
New reports are published on the second week of a new quarter.