CLOUDFLARE

Cyber Threat Landscape

Vince Voci
Director, Global Government
Relations & Partnerships

Agenda

1. Cloudflare Overview & 2025 Year In Review
2. Software Supply Chain Security
3. Cybercrime-as-a-Service
4. Internet Outages
5. DDOS Attacks

Cloudflare's **global network** powers our threat intelligence

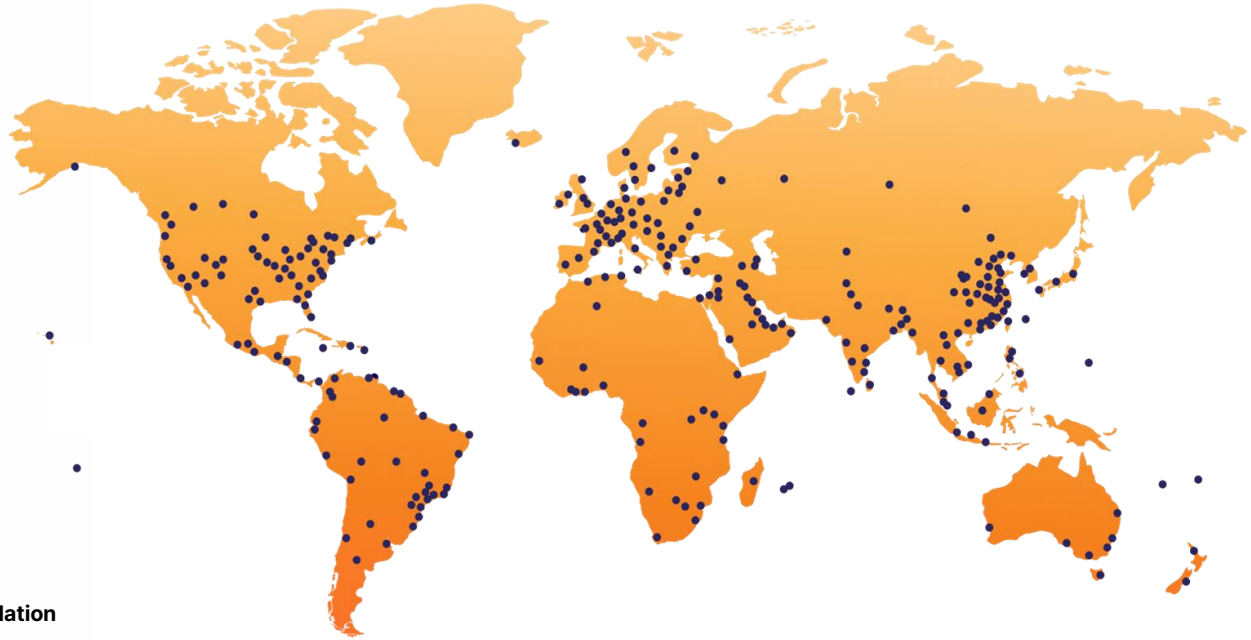
335+ cities
in 125+ countries

w/180+ cities
for AI inference powered by GPUs

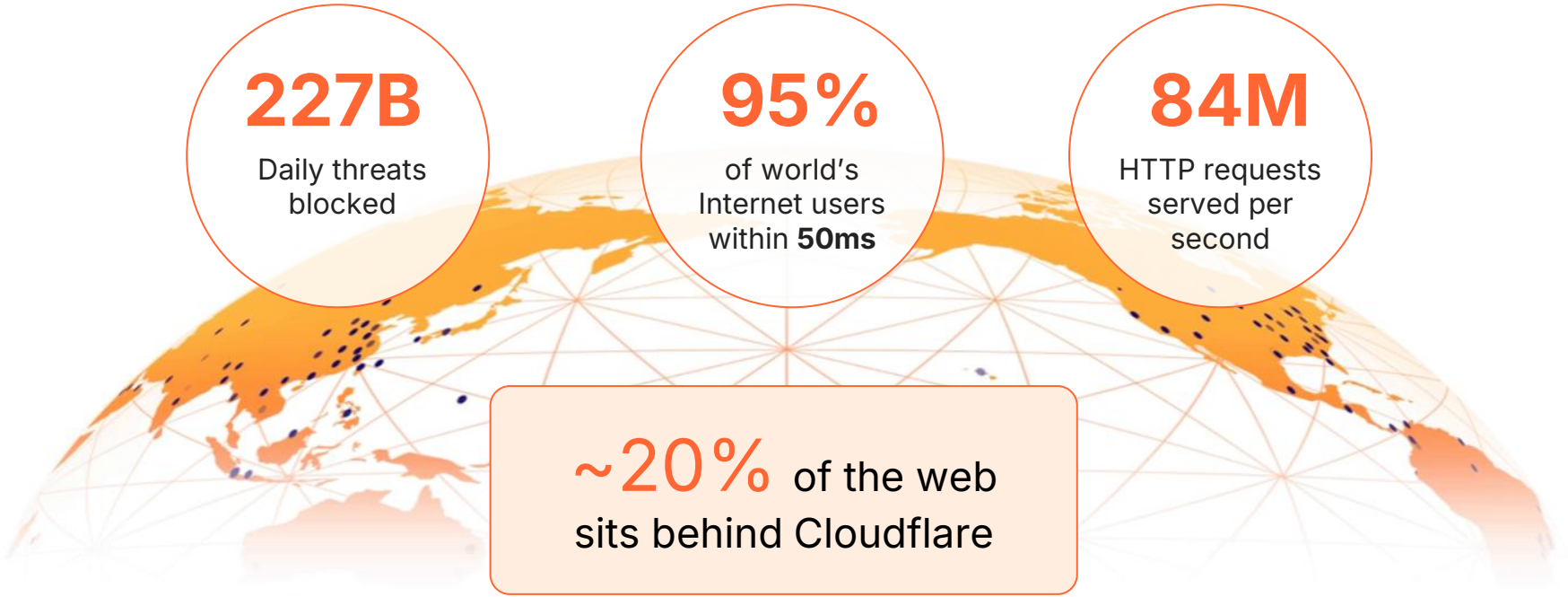
13,000
Global network interconnections, including major ISPs, cloud services, and enterprises

449 Tbps
of network capacity (and growing)

~50 ms
from 95% of the world's Internet-connected population



Insight into threats at massive scale



CLOUDFLARE

2025 Year in Review

Traffic

19%
Growth in Internet traffic

Connectivity

174
Major Internet disruptions observed

Security

71%
of global bot traffic comes from the top 10 countries/regions

Security

31 Tbps
peak network-layer DDoS attack

Email Security

5.6%
of emails are malicious

Email Security

52%
of malicious emails contained a deceptive link

Email Security

.christmas
Originated the largest share of malicious and spam email

CLOUDFLARE

Software Supply Chain Security

Salesloft Drift Compromise

GRUB1

- **Who:** Actor based in Russia
- **What:** Focused on credential and data harvesting
- **When:** July and August 2025
- **Why:** Unknown, possibly financially motivated
- **Sophistication:** Unsophisticated
- **Effectiveness:** Highly Effective

CLOUDFLARE

The “Side Door” Entry

What happened?	Key Concept	The Result
Salesloft Drift is a customer support tool of Salesforce. It is used by companies to manage customer support between clients and vendors.	Think of this like giving a contractor a key to your office building.	The attackers used this trusted access to enter organizations customer support database (Salesforce) and copy records.
Malicious actors targeted a **trusted third-party tool**, which roughly 100 organizations.	The hackers didn't pick the lock; they stole the contractor's key to walk right in.	Customer Records **DID** Include: ● The subject line of the Salesforce case ● The body of the case, which included freeform text ● Customer contact information
Attackers stole a **digital key** that organizations had given to the Drift tool		Customer Records **Did Not** Include: ● Passwords, tokens, keys, or logs

Timeline of the Cloudflare Breach

2025 August

August 9
First signs of reconnaissance

August 12
Initial compromise of Cloudflare
.

August 13
Expanding reconnaissance.

August 14
Understanding our Salesforce environment.

August 16
Preparing for the operation

August 17
Final exfiltration and coverup.

August 20
Vendor action ahead of notification

August 23
Salesforce and Salesloft notifications to Cloudflare

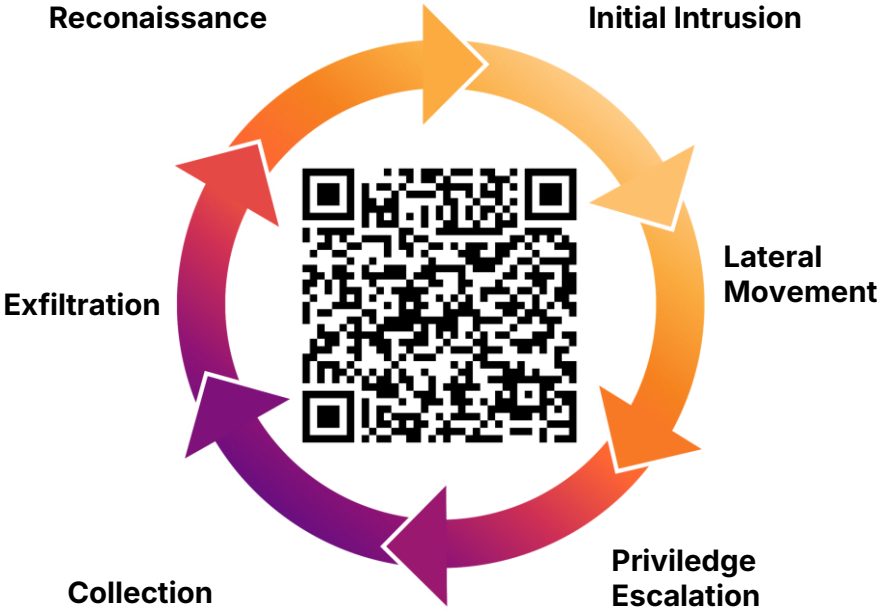
August 25
Cloudflare initiates response activity.

August 26–29
Scaling the response and proactive measures

September

September 2
Customers notified and blog posted.

The Takeaways



- Software Supply Chain
  - Becoming major threat vector
  - Organizations are responsible for the technology stack
  - Extensive risk across the multi-vendor ecosystem
  - Single breach leads to hundreds or thousands of downstream impacts
- Recommendations
  - Implement frequent credential rotation
  - Enforce principles of least priviledge
  - Enhance monitoring and controls

Cybercrime-as-a-Service

Disrupting RaccoonO365

Who is RaccoonO365?

- **Who:** Joshua Ogundipe, actor based in Nigeria, and working with at least four others.
- **What:** Focused on cybercrime
- **When:** February to September 2025
- **Why:** Financially motivated
- **Sophistication:** Unsophisticated
- **Effectiveness:** Highly Effective
- **Status:** Arrested by the Nigerian Police in December 2025.

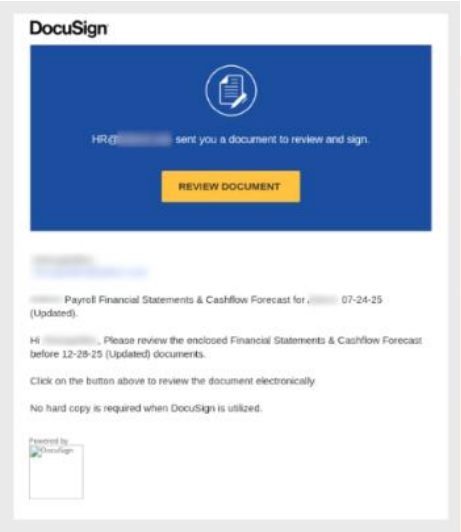
CLOUDFLARE

WHAT is RaccoonO365?

- **Sells phishing kits and other services to steal sensitive information** from Microsoft customers
- **Leveraged by hundreds of threat actors** to target every industry, granting them initial access to perpetrate additional cybercrimes
- **Since July 2024, kits have been used to steal at least 5,000 Microsoft credentials** from 94 countries.
- There was an **extensive tax themed phishing campaign targeting over 2,300 organizations** in the US.

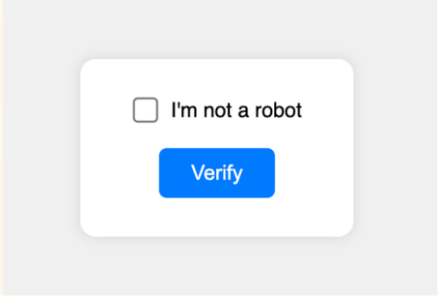
HOW does RaccoonO365 work?

STEP 1
Initial lure



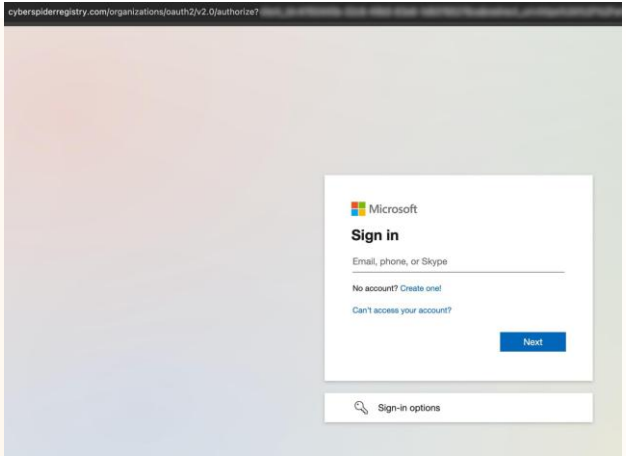
Phishing campaigns impersonate trusted brands like DocuSign, SharePoint, Adobe, and Maersk

STEP 2
Human verification and detection evasion



CAPTCHA page to block automated security tools and restrict access to human targets

STEP 3
Credential theft



Page acts as AITM to proxy authentication flow to Microsoft, allowing attacker to capture password and session cookie, effectively bypassing MFA

CLOUDFLARE

Coordinated disruption operation

What happened?

1 CORE INFRASTRUCTURE

- Identified RaccoonO365's core infrastructure

2 PARTNERSHIP

- Operationalized partnership with key players (e.g., MSFT)

3 LEGAL STRATEGY

- Enacted legal strategy – Civil RICO and IP Infringement

4 DISRUPTION

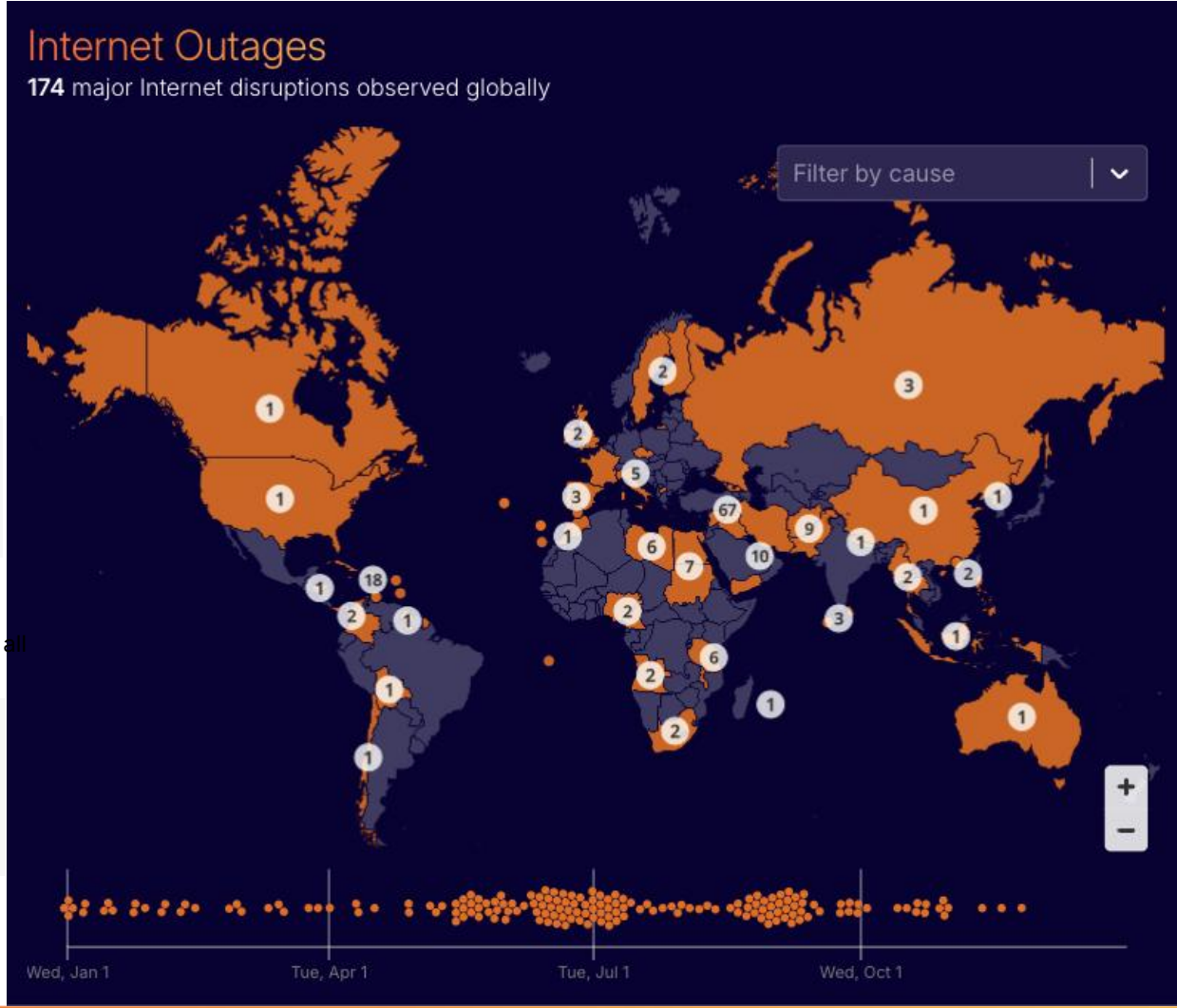
- Systematically dismantled RaccoonO365's presence on Cloudflare's platform

Internet Outages

What we know about Iran's Internet shutdown

Internet Outages

1. **Government Directed - 83**
   - A variety of factors, including political unrest, military operations, or elections, have directed government bodies to suspen Internet service.
2. **Power Outage - 25**
   - Intentional or unintentional power outages have impacted Internet connectivity.
3. **Cable Cuts - 19**
   - Nearly 900 subsea cables provide nearly 99% of all international data traffic.
4. **Technical Problems - 14**
   - Several technical incidents at cloud platforms, including Cloudflare, impacted the availability of websites and applications

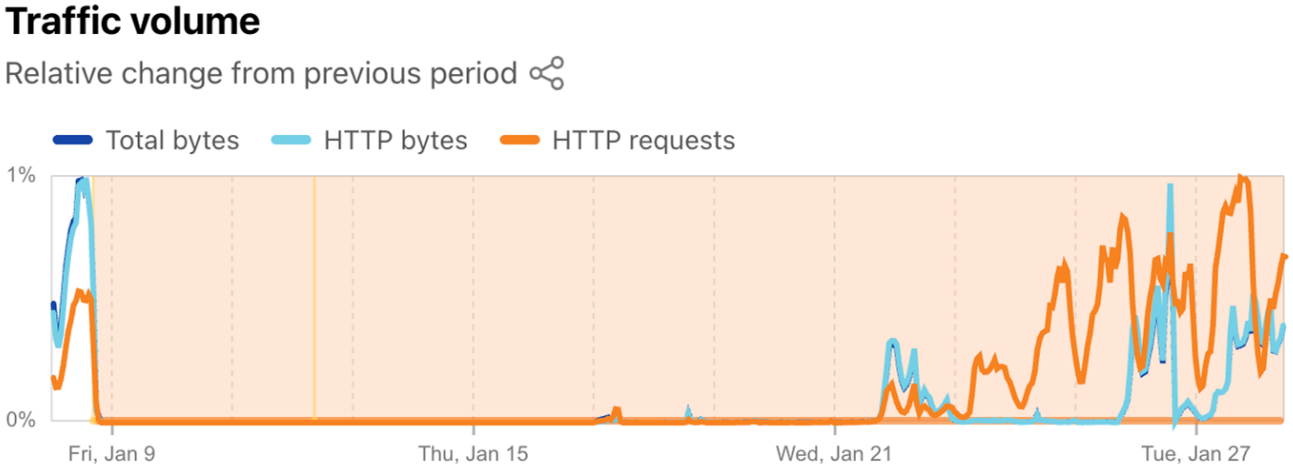


CASE STUDY

CLOUDFLARE

What we know about Iran's Internet shutdown

- Beginning in December 2025, protests erupted in multiple cities across Iran. Protestors were originally motivated by poor economic conditions, but later demanded a change in government leadership.
- From roughly January 8 - 21, the entire country was almost entirely cut off from the global Internet.
- The Iranian government has a history of Internet shutdowns during periods of protests.

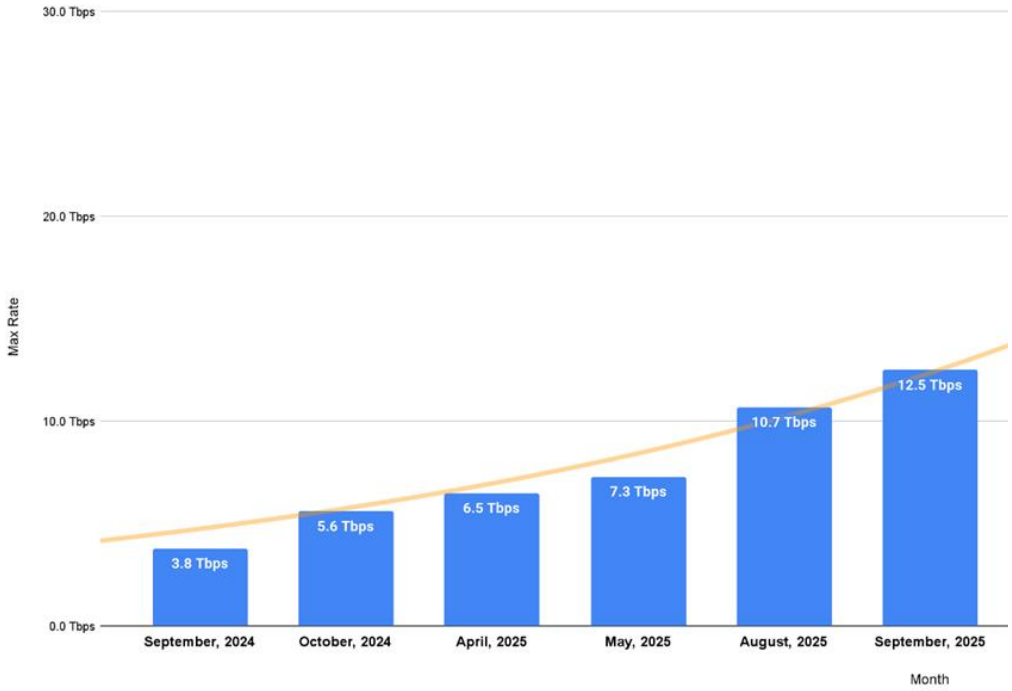


Distributed Denial of Service (or DDOS) Attacks

2025 Parliamentary Elections in Moldova

Alarming Rise in Hyper-volumetric DDoS Attacks

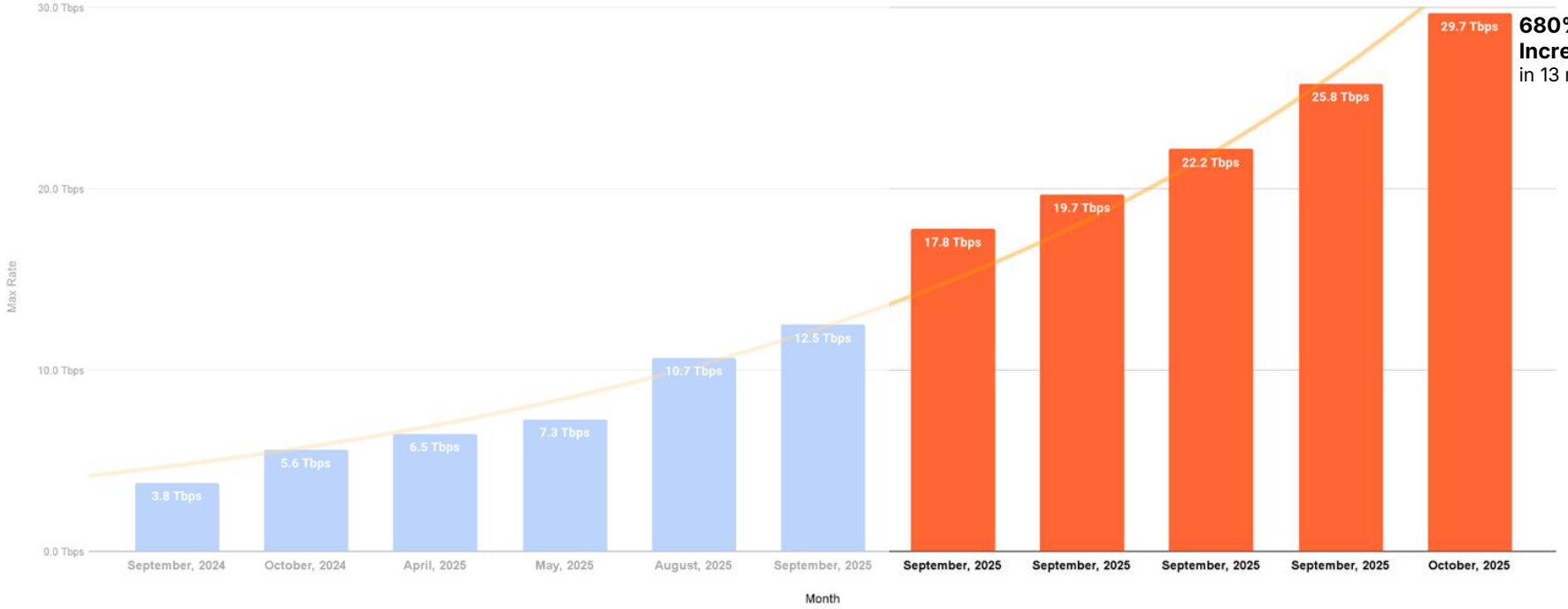
+8.7 Tbps
in 12 Months



Alarming Rise in Hyper-volumetric DDoS Attacks

+8.7 Tbps
in 12 Months

+17.2 Tbps
in Q4 2025



680% Increase
in 13 months

CLOUDFLARE

Analysis of the 29.7 Tbps DDoS Attack

"Aisuru" Botnet

400K-500K compromised consumer-grade IoT devices

Traffic Flood

Carpet bombing thousands of ports with randomized headers

Targeted Industries

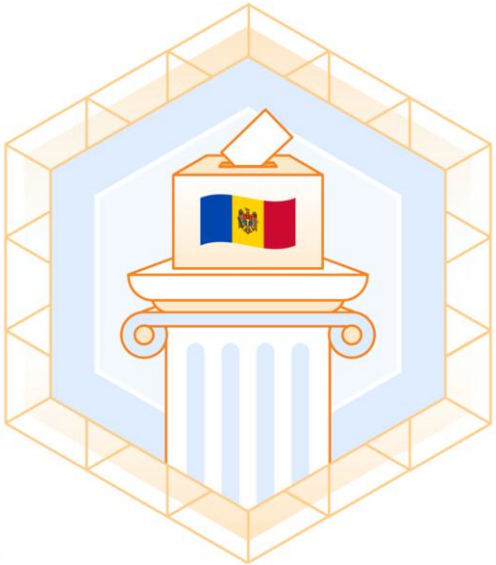
Primarily targeting US-based ISPs/Telcos and Gaming Industry

Cloudflare's Assessment: Recent attacks appear to be validating 20+ Tbps capability before deploying against unprotected targets. Most Enterprise defenses are sized for <20 Tbps.

CASE STUDY

CLOUDFLARE

Elections in Moldova



Free service provided

- CDN
- DDOS protections
- Cloudflare Pages
- Web Application Firewall
- Abuse reporting
- Brand protection

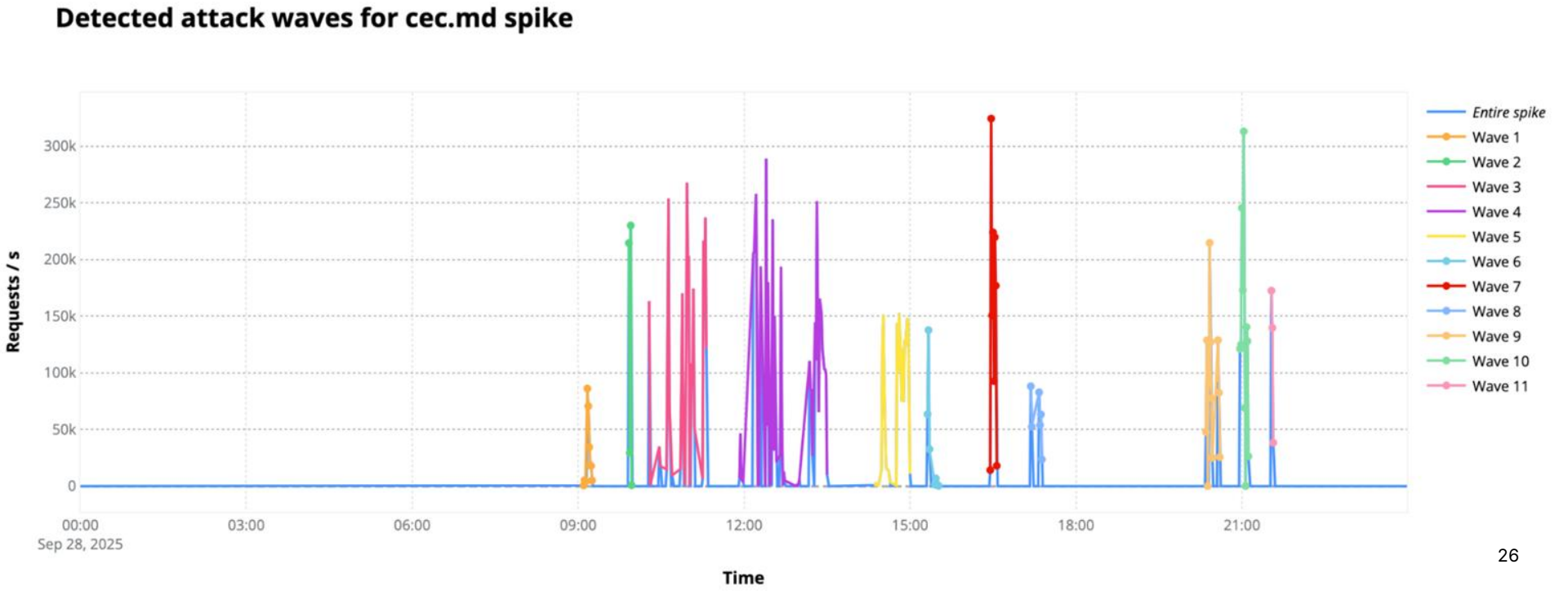
Cyberattacks on Moldovan Central Election Commission.

- 11 attacks chunks over twelve hours.
- 898 million malicious requests deflected.
- Hundreds of millions of malicious requests aimed at Moldovan election-related, civil society and news websites.

> Cloudflare's support was essential for Moldova's parliamentary elections, ensuring uninterrupted access to real-time results for citizens at home and abroad. Their resilient infrastructure allowed us to withstand heavy DDoS attacks and protect the integrity of the democratic process."

– Anatolie Golovco, Cybersecurity and Digital Transformation Expert in the Office of the Prime Minister of Moldova

Cyberattacks to the Moldova Election Commission



Thank you!

Stay in Touch:

Cloudflare Radar:

Cloudflare Threat Intelligence: