DDoS Attacks 2026 Trends & Mitigation

An Evaluation Including FastNetMon Research

presented by Virgil Truica

FASTNETMON

Agenda

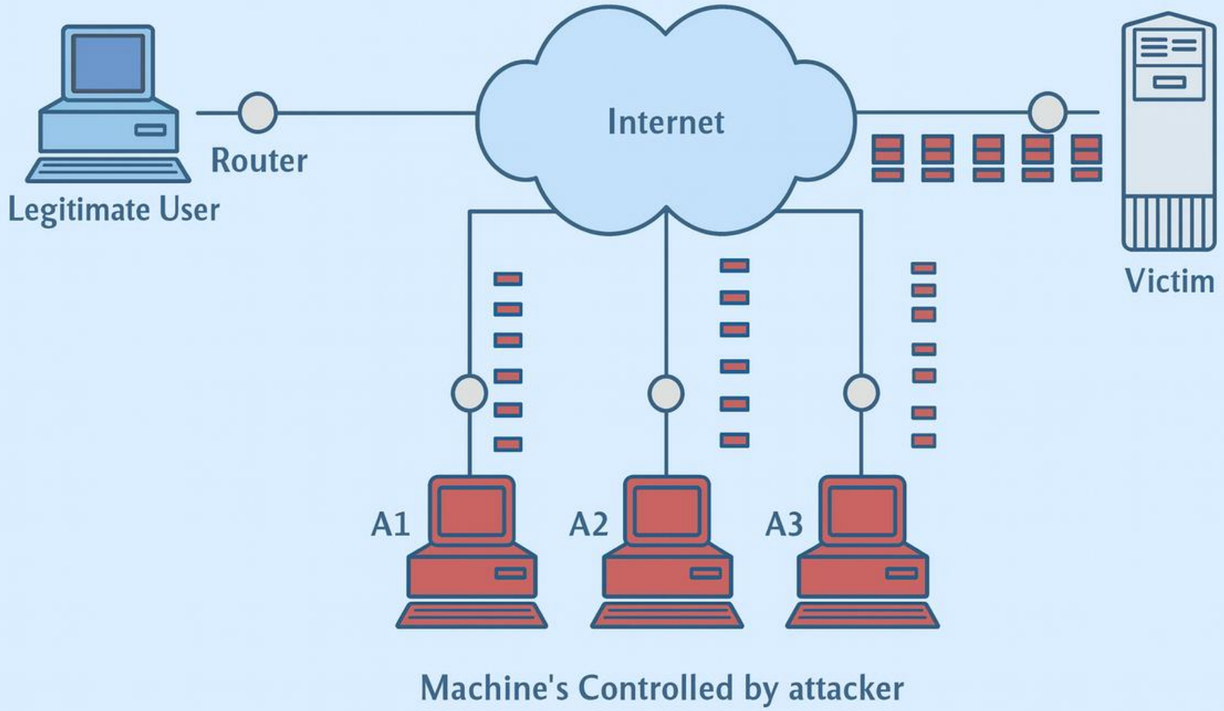
What we'll cover

1. DDoS Attack **Evolution & Milestones**
2. Modern Attack **Taxonomy & Trends**
3. DDoS **Statistics & Global Impact**
4. **Mitigation Solutions** Landscape
5. Strategic **Recommendations & Predictions**

FASTNETMON

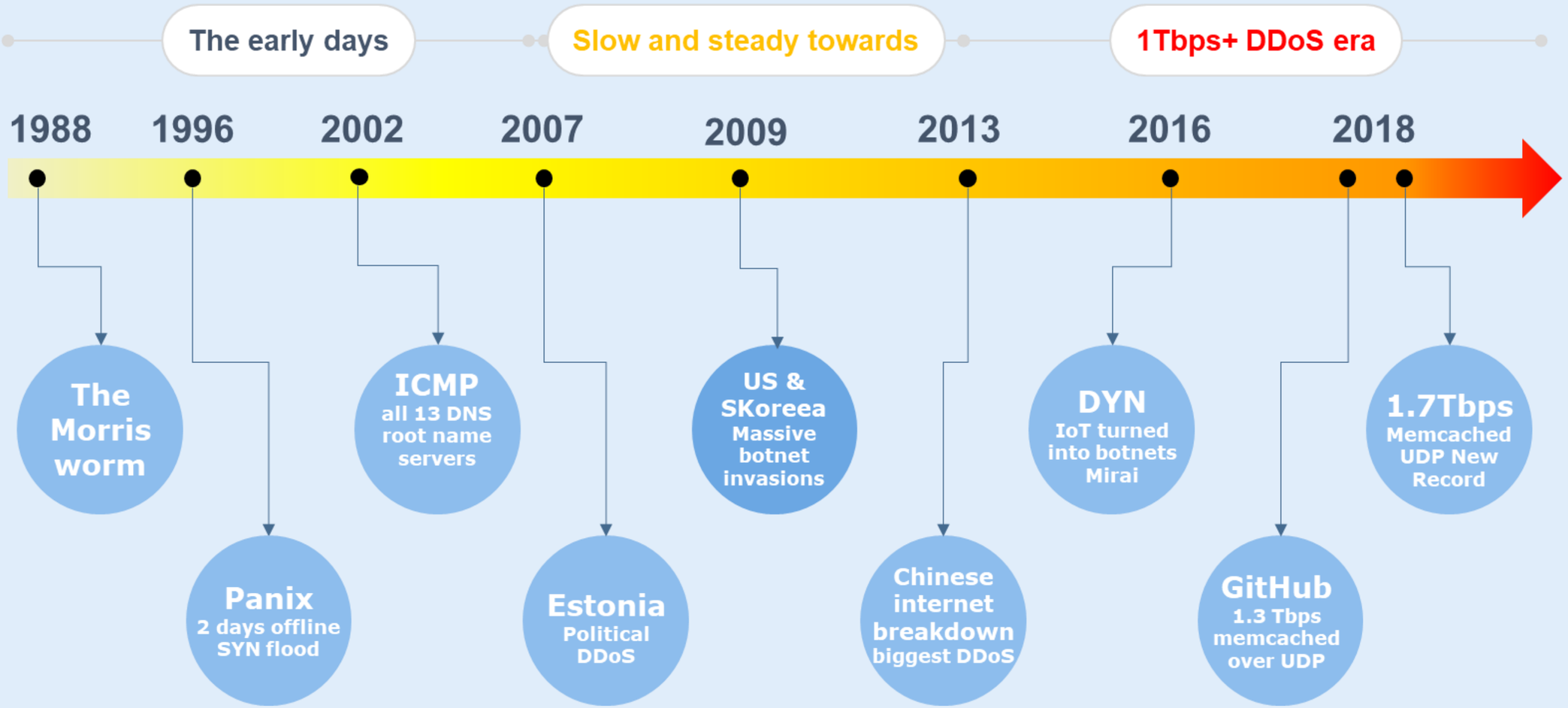
What is a DDoS Attack?

A **DDoS (Distributed Denial-of-Service)** attack **floods** a server or network with “**fake” traffic** from multiple sources, making it **slow** or completely **unreachable** for real users.

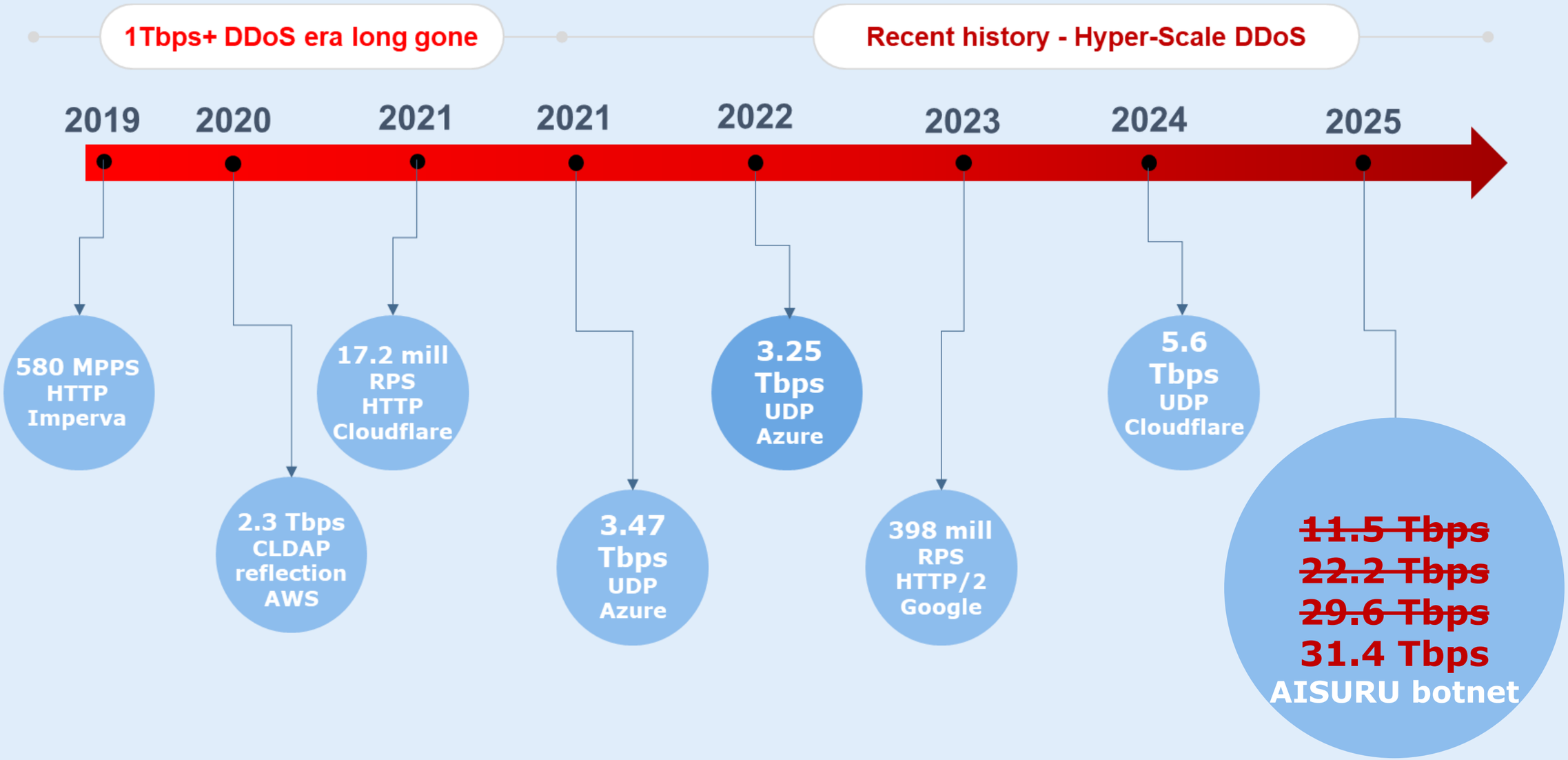


FASTNETMON

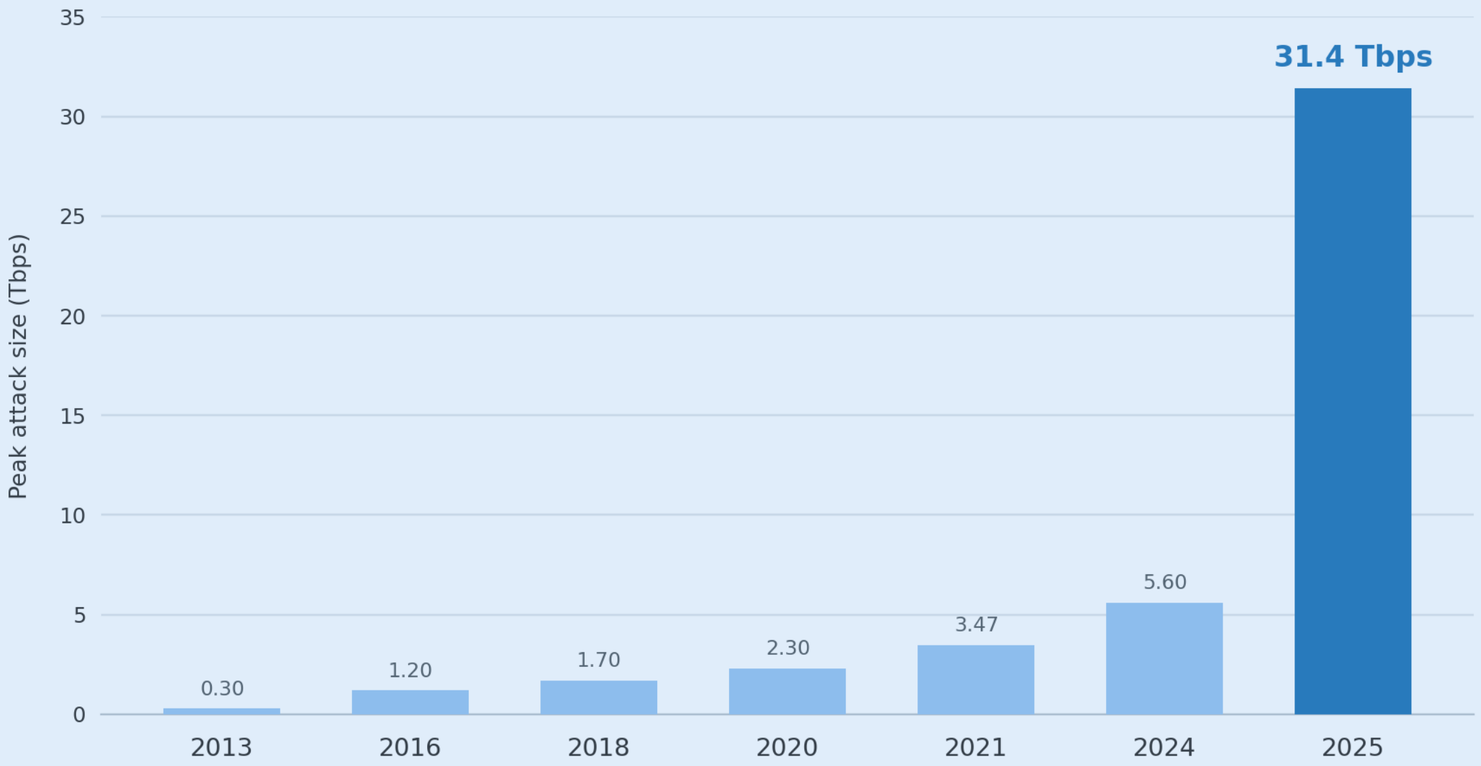
Recap & Evolution (1988–2018)



Recap & Evolution (2019 – 2026)



DDoS: from Gbps to 30+ Tbps



31.4 Tbps

Largest publicly reported DDoS attack

5.6×

the 2024 record

FASTNETMON

Not All DDoS Attacks Are Created Equal

Volumetric / Amplification	Transport / State-Exhaustion	Application / Resource Abuse	Stealth / Modulation Techniques
DNS amplification	SYN flood	HTTP GET/POST flood	IPv6 Reflection
Authoritative DNS query flood — dominant in 2026	TCP Reset flood	Slowloris / slow POST	Webtransort & WebRTC Abuse
CLDAP	HTTP/2 Rapid Reset	GraphQL introspection	Protocol Obfuscation
SSDP / UPnP	HTTP/2 Continuation	Websocket flood	Fragmented Payloads
Memcached	IP fragment overlap	gRPC ping-pong	Multi-vector rotation
...and more	...and more	...and more	...and more

The DDoS Mix Shifted in 12 Months

DNS FLOODS

Almost 1 in 3

of L3/L4 attacks · Q2 2025

→

40%

of network-layer attacks · Q2 2026

CLDAP

Outside top 5

attack vectors · Q2 2025

→

RESURGENCE

#3 VECTOR

Q2 2026 · +580% versus Q1

ATTACKS >1 Tbps

106

attacks in Q1 2026

→

>7.5 x Q1

805

attacks in Q2 2026

The protocols are familiar. The scale, frequency and attack mix are not.

Source: Cloudflare DDoS Threat Reports, Q2 2025 and H1 2026

FASTNETMON

Three Observations From The Frontlines:

Carpet Bombing - the Norm

Attack traffic is spread across entire prefixes, evading per-host thresholds while overwhelming shared infrastructure.

Botnets Rebuild Quickly

Aisuru and KimWolf were disrupted, but new botnets immediately began competing for the same vulnerable devices.



Multi-vectored DDoS

Attackers increasingly combine multiple attack vectors - volumetric, transport, and application-layer to overwhelm systems and evade single-layer defenses.

FASTNETMON

Top 20 Locations of Botnet C&Cs

Spamhaus Intelligence Report, Jan–Jun 2026

Rank	Country	Jul - Dec 2025	Jan - Jun 2026	% Change
#1	United States	5,040	4,244	-16%
#2	Netherlands	2,104	1,595	-24%
#3	China	3,371	1,409	-58%
#4	Germany	1,528	1,170	-23%
#5	Singapore	1,191	645	-46%
#6	United Kingdom	667	539	-19%
#7	France	533	525	-2%
#8	Russia	722	471	-35%
#9	Cyprus	-	286	New entry
#10	Sweden	437	264	-40%
#11	Finland	197	254	+29%
#12	Moldova	-	231	New entry
#13	Canada	206	219	+6%
#14	Seychelles	647	209	-68%
#15	Latvia	-	188	New entry
#16	Turkey	271	187	-31%
#17	Japan	269	175	-35%
#18	Vietnam	321	174	-46%
#18	Switzerland	-	174	New entry
#20	UAE	-	143	New entry

FASTNETMON

Top 10 Networks Hosting C&Cs Botnets

Spamhaus Intelligence Report, Jan–Jun 2026

Rank	Jul - Dec 2025	Jan - Jun 2026	% Change	Network	Country
#1	1428	1017	-29%	digitalocean.com	United States
#2	-	931	New entry	stark-industries.solutions	United Kingdom
#3	729	589	-19%	colocrossing.com	United States
#4	1502	588	-61%	alibaba-inc.com	China
#5	511	382	-25%	virtualine.org	United Kingdom
#6	346	374	+8%	contabo.de	Germany
#7	543	335	-38%	amazon.com	United States
#8	879	302	-66%	tencent.com	China
#9	-	291	New entry	cloudzy.com	United States
#10	362	273	-25%	as210558.net	Germany

FAST NETMON

Conclusions

Geography Is Stable, Infrastructure Is Not.

The leading countries remain broadly similar, while C&C activity moves rapidly between hosting networks.

Hosting Networks Remain a Primary Target.

Fast provisioning and scalable infrastructure make cloud and hosting providers attractive to botnet operators.

Moldova Is Now Part of the Global Picture

Moldova and Cyprus entered the Top 20 at #12 and #9, showing that no market is too small to host infrastructure abused by global botnets.

FASTNETMON

Where DDoS attacks are concentrated

MOST TARGETED REGIONS

01	North America
02	Asia-Pacific
03	Europe
04	Middle East
05	Latin America

MOST TARGETED COUNTRIES

01	China
02	United States
03	India
04	United Kingdom
05	Turkey

Consensus across Cloudflare, NETSCOUT, Radware, StormWall, Gcore and Akamai reporting.

Industries under the greatest DDoS pressure

01 **Financial Services**

02 **Technology & Cloud**

03 **Telecommunications & Service Providers**

04 Government & Public Sector

05 Media, Gaming & Entertainment

Consensus across Cloudflare, NETSCOUT, Radware, StormWall, Gcore and Akamai reporting. Rankings indicate recurring prominence, not averaged market share.

DDoS pressure in Moldova

NETSCOUT ATLAS · January–June 2026

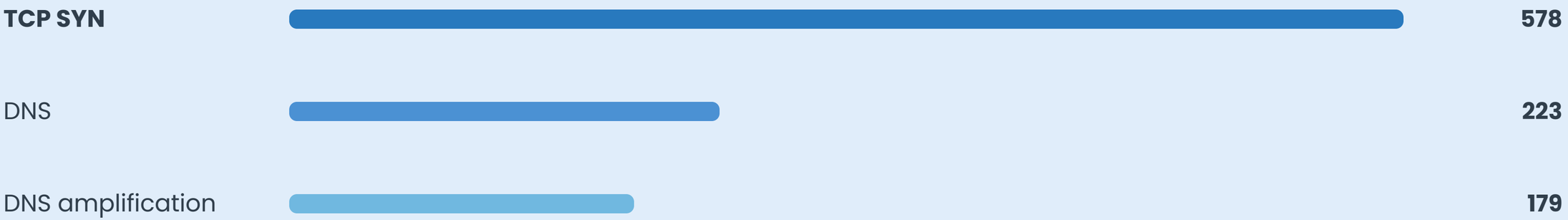
1,223
attacks observed

37.6 min
average duration

9
vectors in one attack

420
hosting and telecom attacks

Most observed attack vectors



420 combines hosting and data-processing providers, wireless carriers and wired carriers. Figures represent NETSCOUT visibility, not Moldova’s complete national attack volume.

From election security to government disruption

Two incidents show the national impact of DDoS attacks

28 SEPTEMBER 2025

Parliamentary election

898M

malicious requests

12+ hours

11 coordinated waves

Peak: 324,333 requests per second

CEC services remained available

11 SEPTEMBER 2026

Government websites

Affected services

Presidency

Government

Public Services Agency

Temporary access problems and service unavailability

STISC activated mitigation and restoration measures

In Moldova, DDoS is both an operational threat and an instrument of geopolitical pressure.

The Real Cost of DDoS Attacks: Industry Estimates

Business Tier	Estimated impact	Downtime Exposure	Long-Term Impact
SMBs	**~$120,000** Per attack	**$8K–$74K / hour**	**20% forced out of business post-attack**
Mid-SMEs	**~$254K** Per attack	**Up to $360K / hour**	**Revenue and SLA impact** Customer churn extend the impact
Enterprises	**Can exceed $2M** for a major incident	**Hundreds of thousands** per hour	**Amplified damage over prolonged outages**

Data: MazeBolt, Checkpoint, Perimeter81, Radware 2026 Cyber Survey, industry cost research

FASTNETMON

Affordable DDoS Protection – Start Simple, Scale Smart

DDoS Mitigation for Every Budget

Blackholing

- Manual, reactive, and low-effort.
- Customer impact & Network impact.

Free, automated blackholing

- Open Source DDoS detection tools
- **FastNetMon** Community Edition - free, automated DDoS detection + blackholing.

BGP FlowSpec mitigation

- Software solutions deployed on-premise or cloud
- Requires NetFlow / sFlow / IPFIX + BGP
- **FastNetMon Advanced, Nokia Deepfield, Wanguard, Genie Networks, CoreTech, Kentik**

FASTNETMON

Enterprise & Hybrid DDoS Mitigation Options

DDoS Protection for Demanding Environments

On-Premise Appliances

- On-premise mitigation with full control
- Limited to appliance/network capacity
- **Arbor, Radware, Corero, A10, NSFocus, NexusGuard, RioRey**
- New: **FastNetMon FastACL, CoreTech, Stormwall**

Cloud Scrubbing Providers

- Fully managed, on-demand
- Handles large-scale attacks
- Adds latency, typically
- **Cloudflare, Akamai, Radware, Arbor Cloud, Gcore, Inter.link, StormWall, Voxility, GSL, NaWas**, **Nexus Guard** and others

Hybrid Strategy

- Combine on-premise & cloud protection
- Optimized cost vs. coverage
- Ideal for enterprises with critical uptime
- **FastNetMon** - DDoS detection and traffic diversion over cloud

FASTNETMON

The Internet Is Growing. So Are the Threats.

- **39 billion IoT devices by 2031** → exponential attack surface
- **Broadband connections - from 1.69 billion to 2 billion by 2031** → more capacity available to legitimate users and botnets
- **Mobile data traffic: 146 EB to 328 EB per month by 2031** → demanding significantly larger uplinks and port capacities.
- **AI is lowering the barrier to sophisticated DDoS attacks** → Reconnaissance, attack configuration, and multi-vector orchestration can be automated now.
- **More capacity. More automation. Less time to react.**

FASTNETMON

Security Is a Shared Duty

- **Share intelligence:** exchange attack data and mitigation lessons
- **Promote security awareness:** educate employees, partners, and users
- **Secure the edge**: Networks must push for stricter filtering at ingress points
- **Demand safer products:** push vendors to ship devices with better default security and updates.
- **Be proactive, not reactive**
- **Keep the dialogue active:** NOGs, RIPE, EPF, Peering & Securiy events ....

FASTNETMON

Thank you!



Virgil Truica

Happy father, DDoS security advocate, and 18 years of experience within the International Telecom industry.

virgil@fastnetmon.com / virgil@salesflow.tech
linkedin.com/in/virgiltruica
+40 742 991 619