



# DDoS Attacks 2025 Trends & Mitigation

The Era of Hyper-Scale Attacks

*presented by Virgil Truica*

# Agenda

What we'll cover

1

DDoS Attack **Evolution & Milestones**

2

Modern Attack **Taxonomy & Trends**

3

DDoS **Statistics & Global Impact**

4

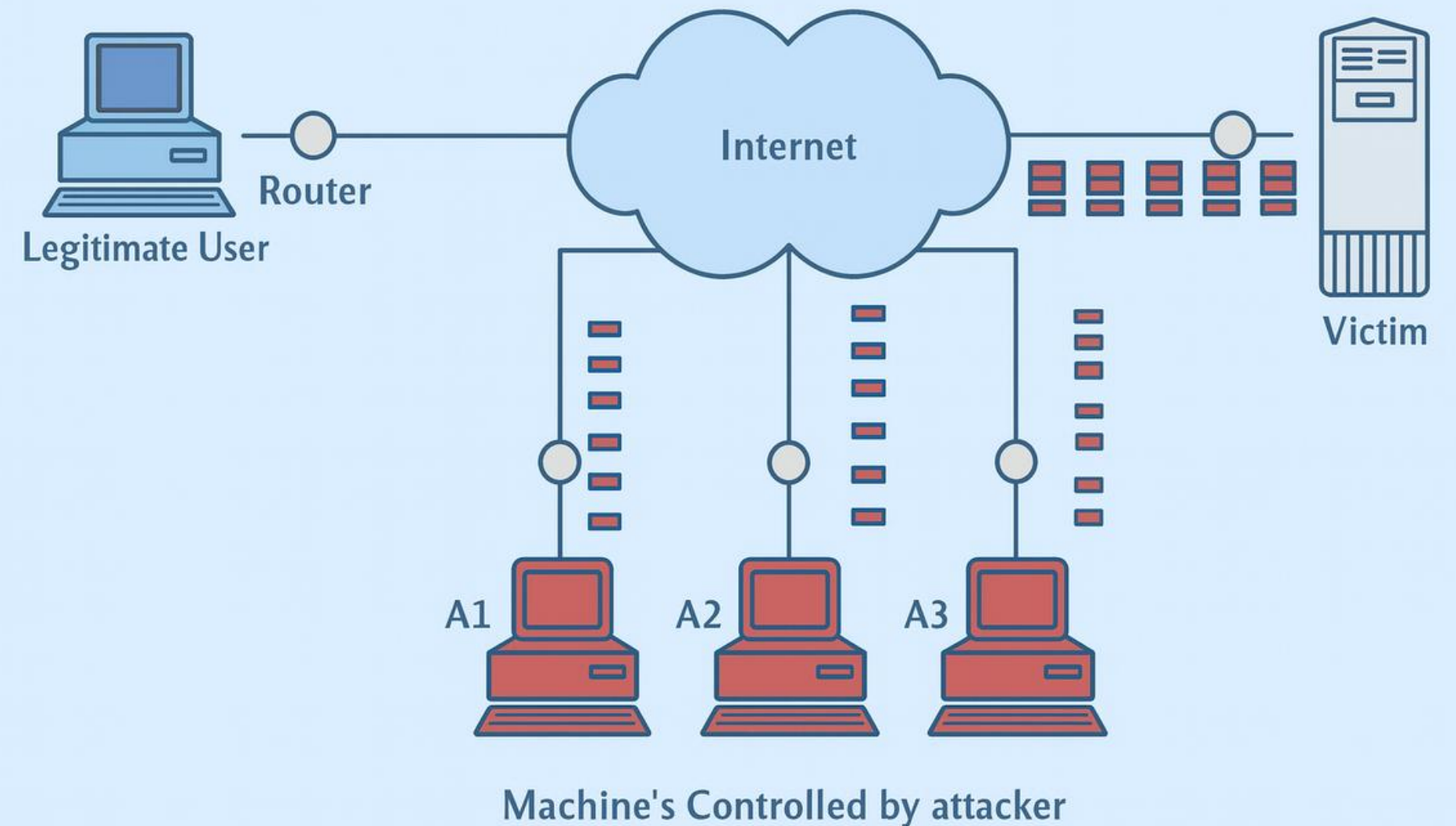
**Mitigation Solutions** Landscape

5

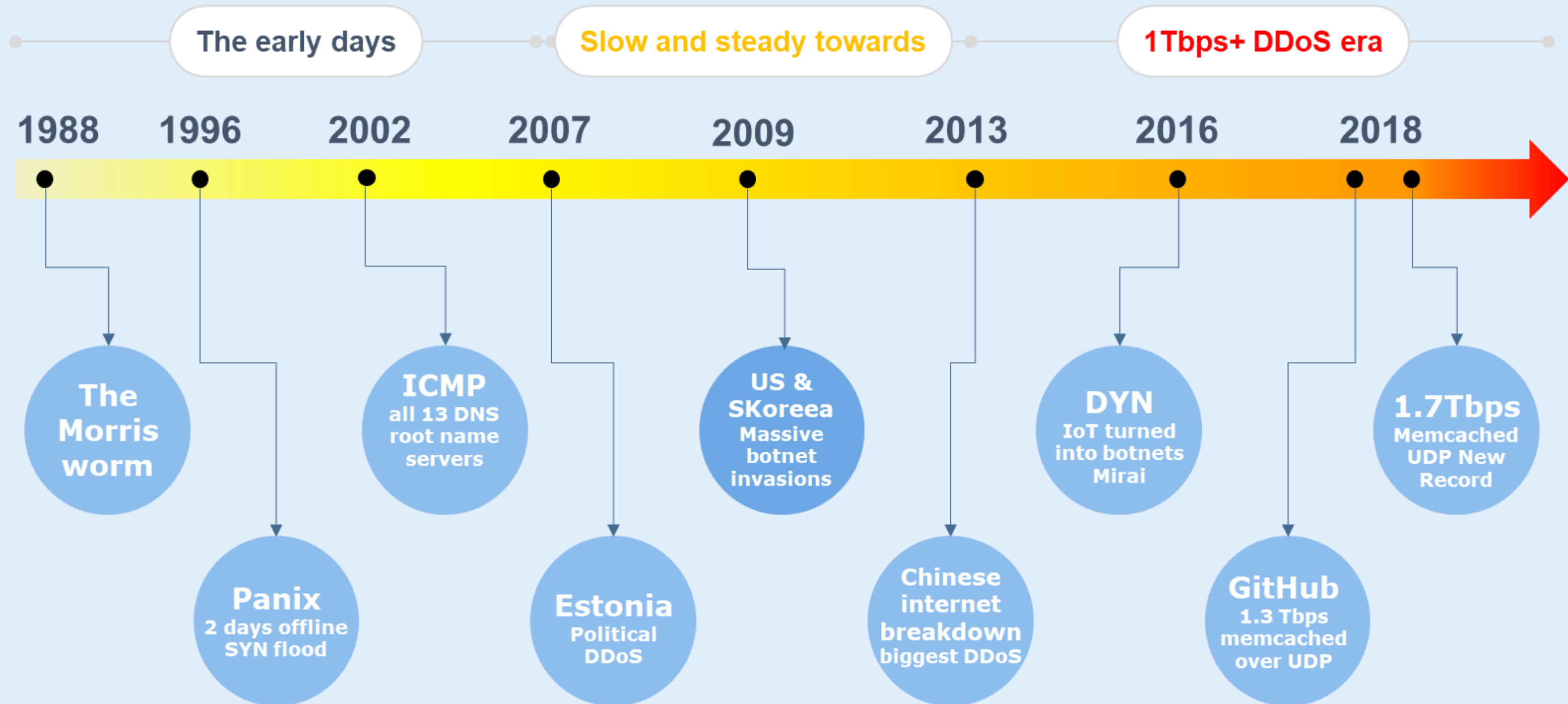
Strategic **Recommendations & Predictions**

# What is a DDoS Attack?

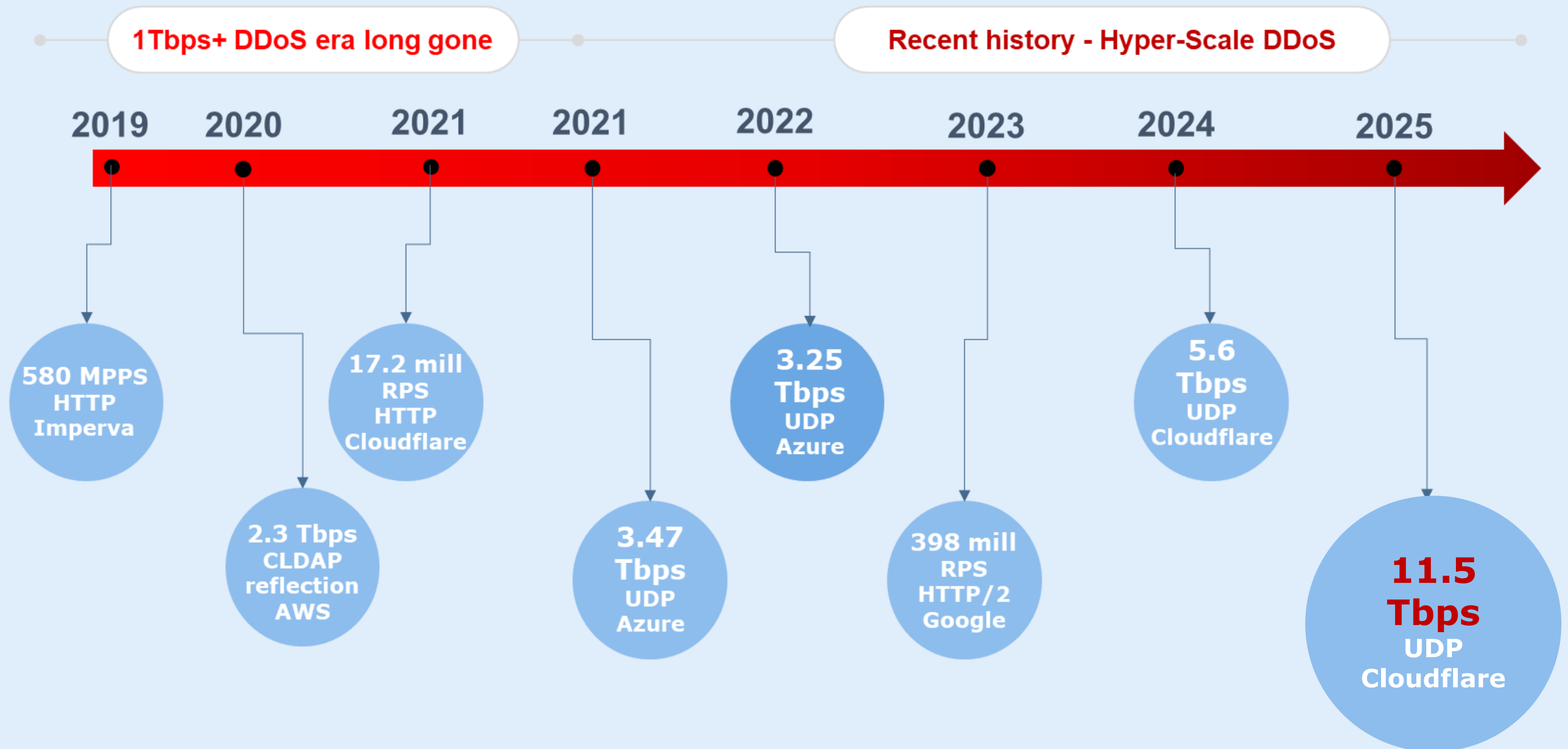
A **DDoS (Distributed Denial-of-Service)** attack **floods** a server or network with “**fake**” traffic from multiple sources, making it **slow** or completely **unreachable** for real users.



# Recap & Evolution (1988–2018)



# Recap & Evolution (2019 - 2025)







# 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                 |
| NTP MONLIST                | 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                     |

# Emerging DDoS Vectors in 2025

- **CLDAP:** +3,488% growth in 2025
- **ESP Reflection:** +2,301% growth in 2025
- **Memcached:** +314% growth, up to 51,000 amplification
- **DNS Amplification:** 55% of all amplified traffic
- **HTTP/2 Rapid Reset:** reached 398M requests/sec

# Three Observations From The Frontlines:

## Shift in Attack Patterns

Carpet bombing DDoS (targeting entire subnets) is gaining traction because it's harder to detect and block.

## Pressure on Infrastructure

Carpet bombing increases false positives, especially for ISPs and carriers. It stresses edge devices, firewalls, and scrubbing centers due to wide coverage and unpredictable targets.



## Multi-vectored DDoS

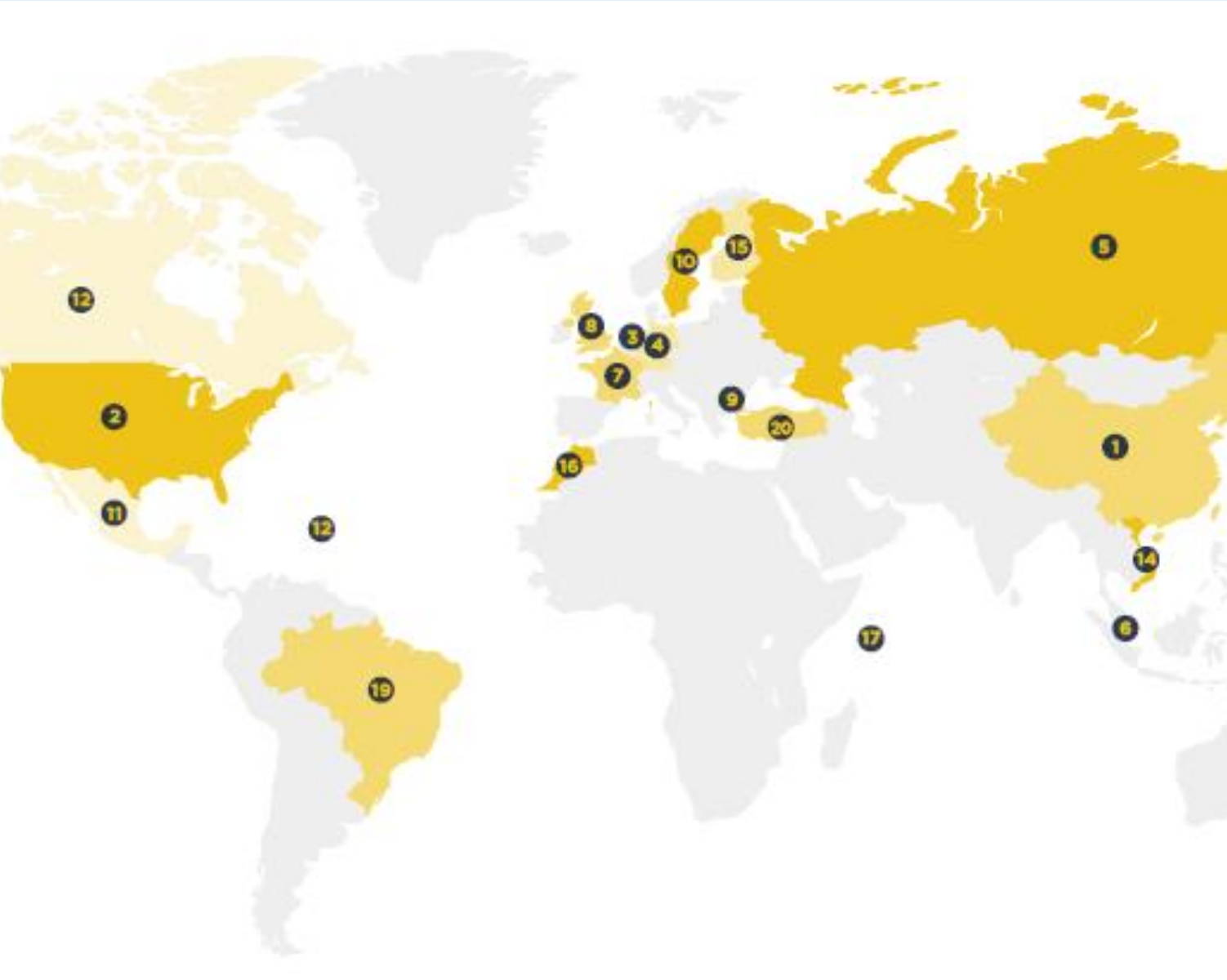
Attackers increasingly combine multiple attack vectors - volumetric, transport, and application-layer to overwhelm systems and evade single-layer defenses.



# Top 10 Locations of Botnet C&Cs

Spamhaus Intelligence Report, Jan–Jun 2025

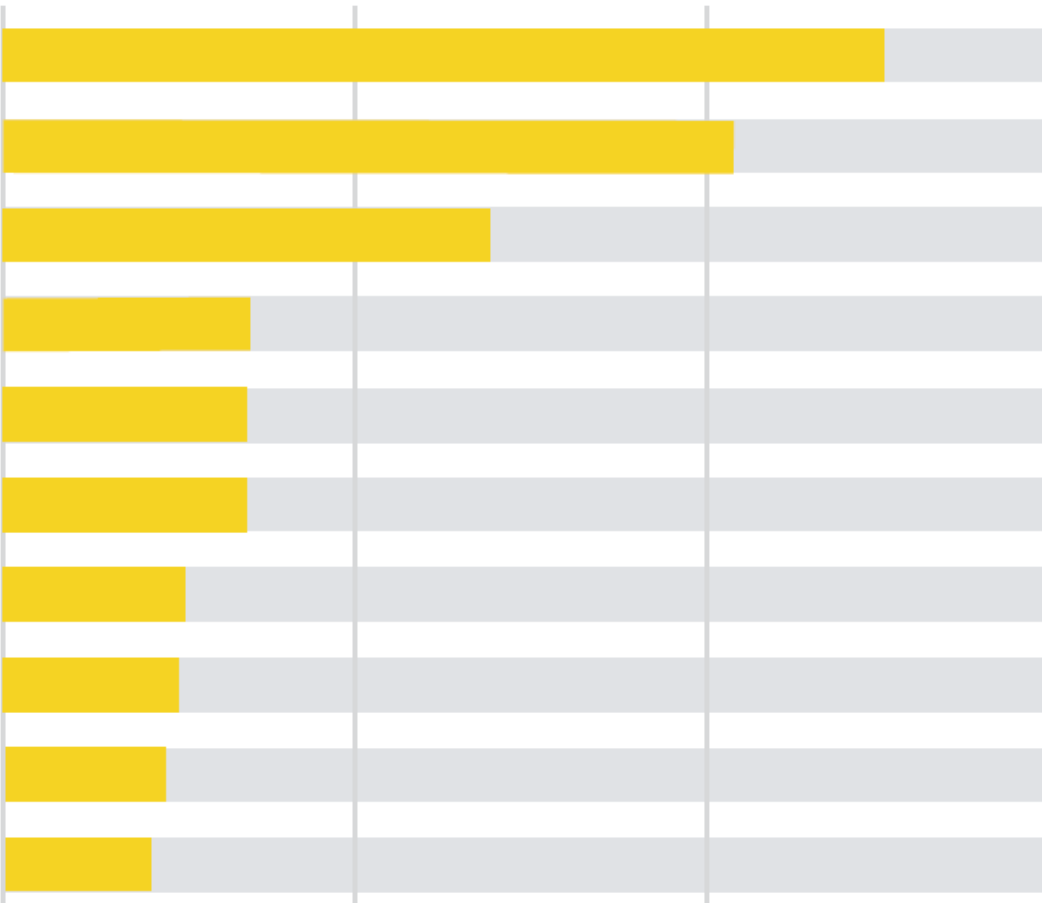
| Rank | Country        |                                                                                     | Jul - Dec<br>2024 | Jan - Jun<br>2025 | % Change |
|------|----------------|-------------------------------------------------------------------------------------|-------------------|-------------------|----------|
| #1   | China          |    | 3,535             | 3,533             | 0%       |
| #2   | United States  |    | 2,286             | 3,512             | 54%      |
| #3   | Netherlands    |    | 782               | 1,406             | 80%      |
| #4   | Germany        |  | 657               | 1,307             | 99%      |
| #5   | Russia         |  | 1,125             | 1,022             | -9%      |
| #6   | Singapore      |  | 382               | 712               | 86%      |
| #7   | France         |  | 279               | 470               | 68%      |
| #8   | United Kingdom |  | 317               | 329               | 4%       |
| #9   | Bulgaria       |  | 544               | 327               | -40%     |
| #10  | Sweden         |  | 275               | 284               | 3%       |



# Top 10 Networks Hosting C&Cs Botnets

Spamhaus Intelligence Report, Jan–Jun 2025

| Rank | Jul - Dec<br>2024 | Jan - Jun<br>2025 | %<br>Change | Network          | Country       |                                                                                       |
|------|-------------------|-------------------|-------------|------------------|---------------|---------------------------------------------------------------------------------------|
| #1   | 172               | 277               | 61%         | alibaba-inc.com  | China         |    |
| #2   | 85                | 213               | 151%        | tencent.com      | China         |    |
| #3   | 29                | 135               | 366%        | digitalocean.com | United States |    |
| #4   | 23                | 76                | 230%        | colocrossing.com | United States |   |
| #5   | 23                | 74                | 222%        | amazon.com       | United States |  |
| #6   | 47                | 72                | 53%         | huawei.com       | China         |  |
| #7   | -                 | 52                | New entry   | railnet          | United States |  |
| #8   | 24                | 43                | 79%         | contabo.de       | Germany       |  |
| #9   | 11                | 40                | 264%        | m247.com         | Romania       |  |
| #10  | -                 | 36                | New entry   | microsoft.com    | United States |  |



# Conclusions

Cloud is ground zero.

Mainstream IaaS providers host the majority of active botnet infrastructure.

China and US dominate.

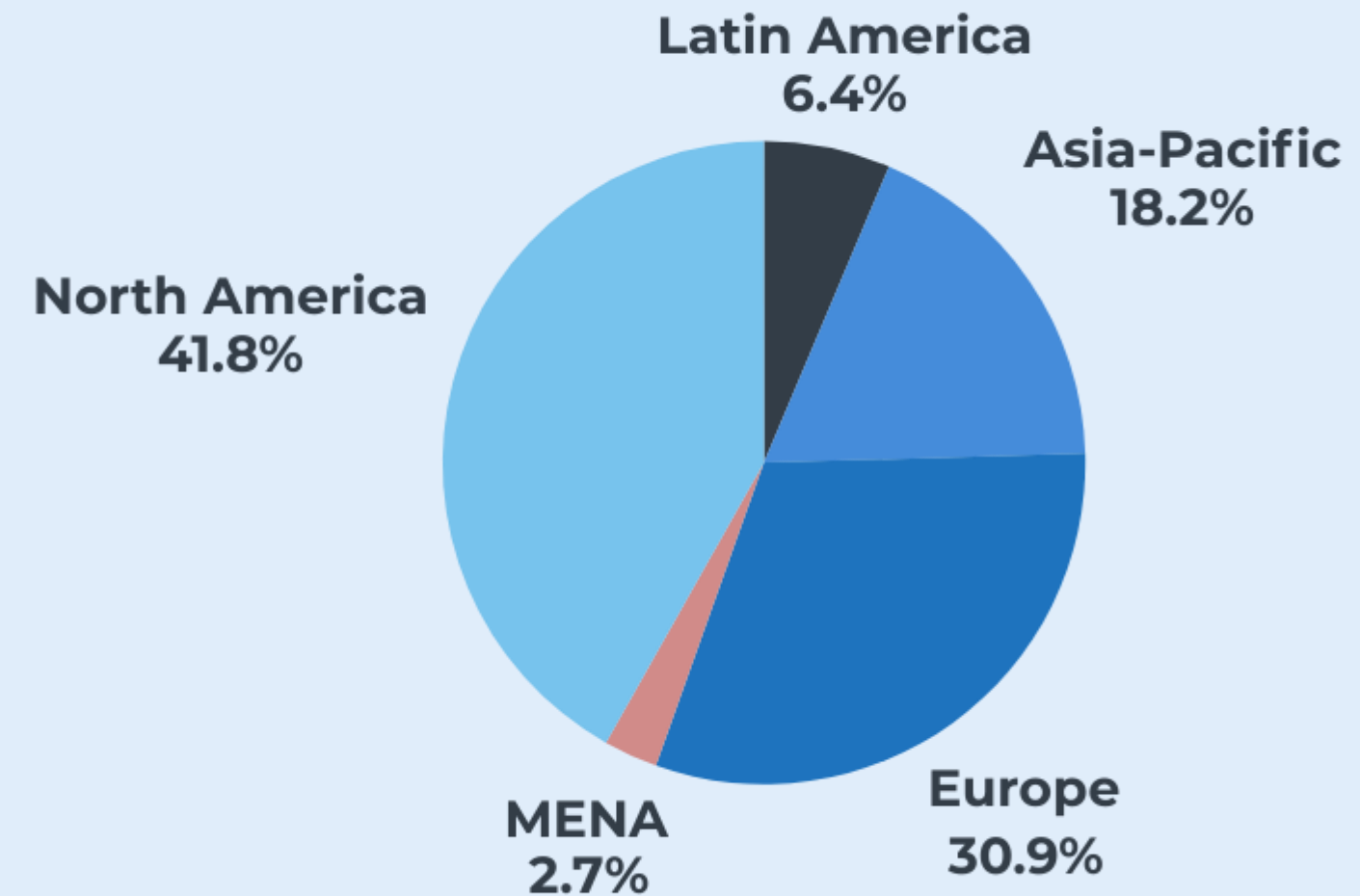
They lead in both C&C volume and network-level growth.

High turnover & new entries.

Networks like Railnet and M247 reflect the rapid expansion of attacker infrastructure.

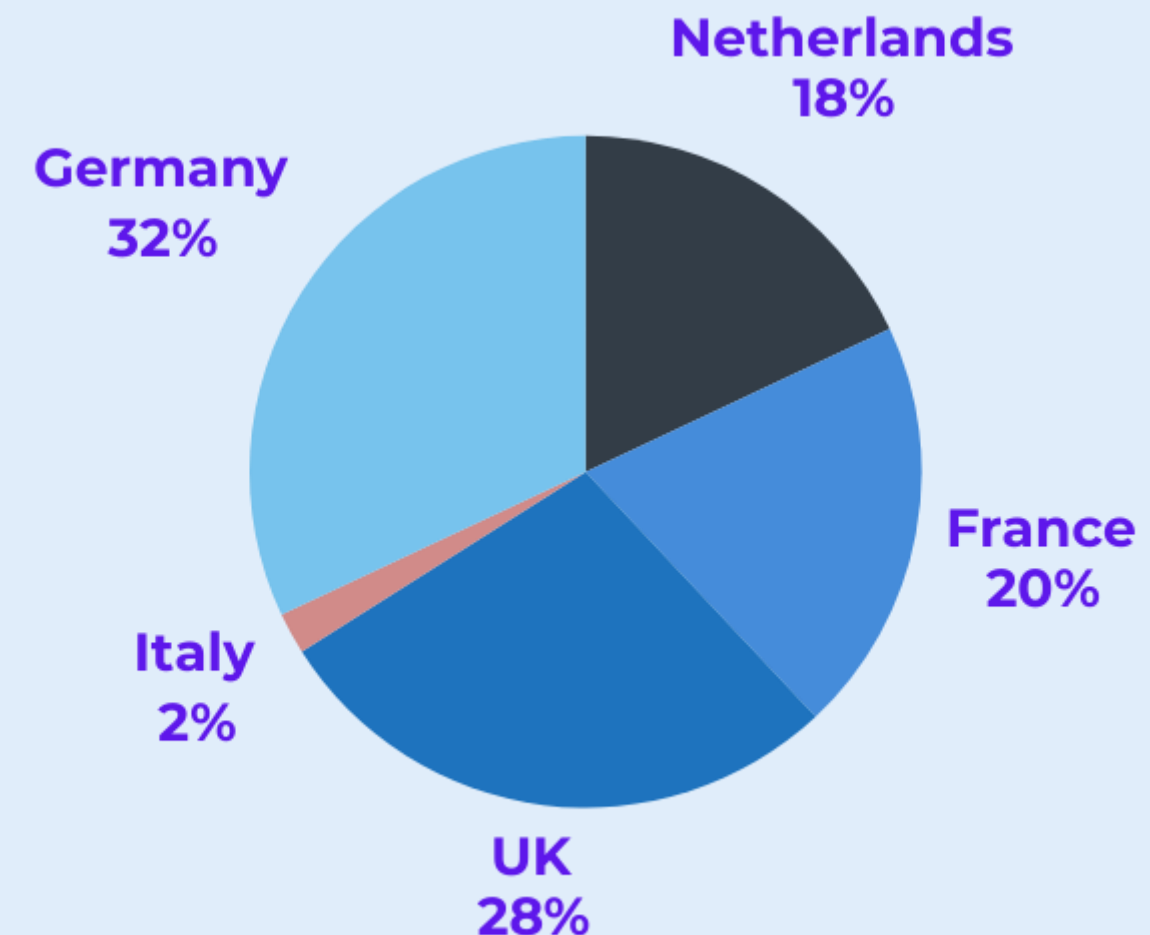
# Most targeted global regions

Data aggregated from multiple DDoS  
vendor reports, 2024–2025



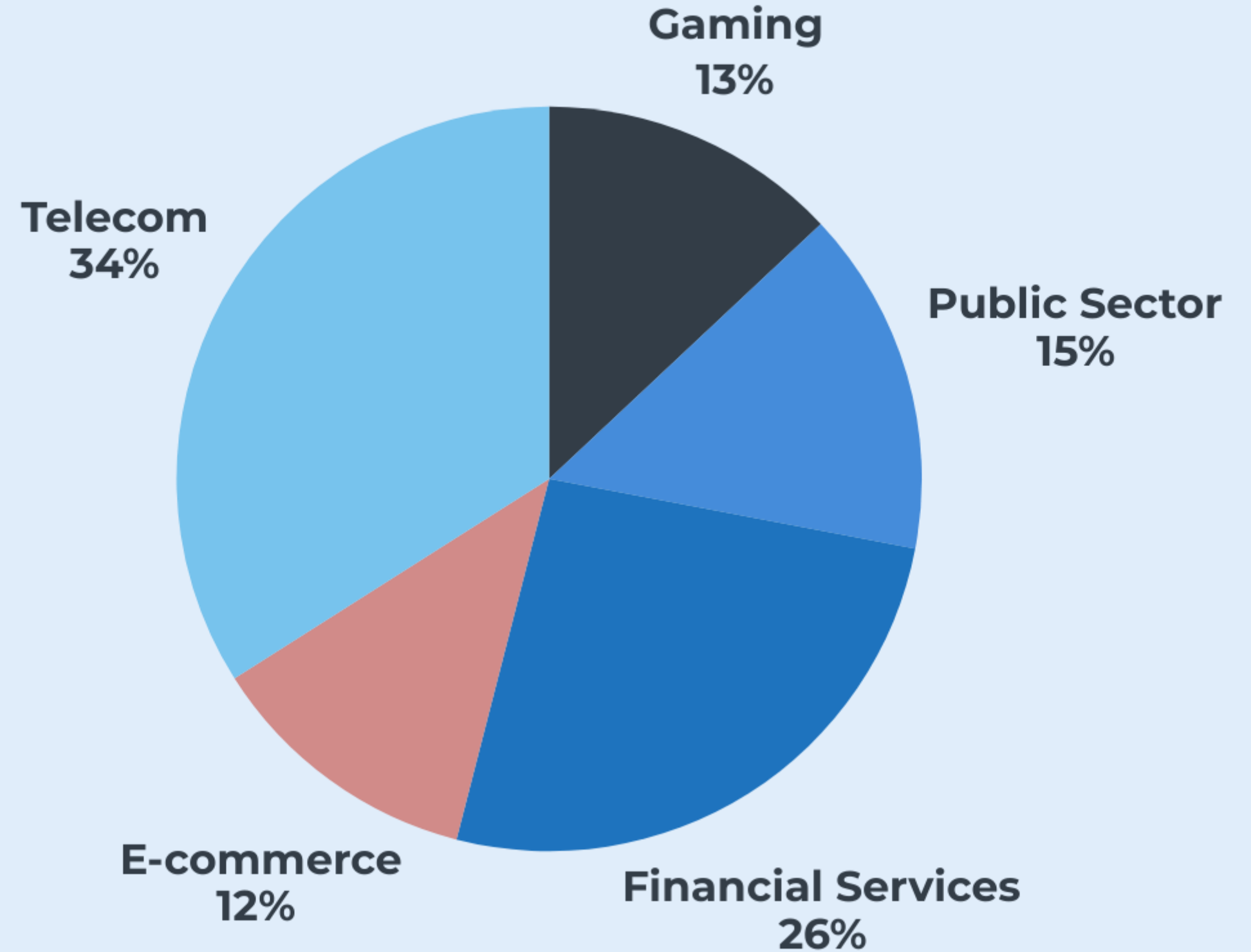
# Most targeted European countries

Data aggregated from multiple DDoS vendor  
reports, 2024–2025



# Most attacked industries

Telecoms and financial services face sustained DDoS pressure - many hit daily, some multiple times per day.





# The Real Cost of DDoS Attacks (2025 Estimates)

| Business Tier | Avg Cost per Attack | Downtime Cost        | Long-Term Impact                         |
|---------------|---------------------|----------------------|------------------------------------------|
| SMBs          | ~\$120,000          | \$8K–\$74K per hour  | 20% forced out of business post-attack   |
| Mid-SMEs      | ~\$254K             | ~\$360K per hour     | 1.3% loss in market value in month after |
| Enterprises   | ~\$2M               | ~\$408K per incident | Amplified damage over prolonged outages  |

Data: MazeBolt, VikingCloud, Checkpoint, Perimeter81, 2024–2025



# 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
- Vendors: **FastNetMon Advanced, Nokia Deepfield, Wanguard, Genie Networks, Arbor, Kentik**





# Enterprise & Hybrid DDoS Mitigation Options

DDoS Protection for Demanding Environments

## Hardware Appliances

- On-premise mitigation with full control
- Limited to appliance/network capacity
- **Arbor, Radware, Corero, F5, A10, NSFocus, NexusGuard, RioRey**
- New: **CoreTech, Aurologic**

## Cloud Scrubbing Providers

- Fully managed, on-demand
- Handles large-scale attacks
- Adds latency, typically
- **Cloudflare, Akamai, Radware, Arbor Cloud, Gcore, Imperva, Inter.link, Stormwall, Voxility, GSL**, 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



# The Internet Is Growing. So Are the Threats.

- **34 billion IoT devices by 2030** → exponential attack surface
- **Broadband connections - from 1.6 billion to 2 billion by 2030** → more capacity connected
- **Mobile data traffic may exceed 280 EB/month** → demanding significantly larger uplinks and port capacities.
- **Exponential increase in DDoS attack size**

# Security Is a Shared Duty

- **Share intelligence:** exchange attack data and mitigation tactics
- **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**
- **Engage in open dialogue:** NOGs, RIPE, EPF, Peering & Security events ....

# Thank you!



Virgil Truica

Happy father, DDoS security advocate, and 16 years of experience within the International Telecom industry.

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