



AI used by Cyber Criminals in DDoS Botnets Today

Threat Intel & Lessons Learned to Defend Against DDoS

By Virgil Truica
Research with FastNetMon
October 27th 2026



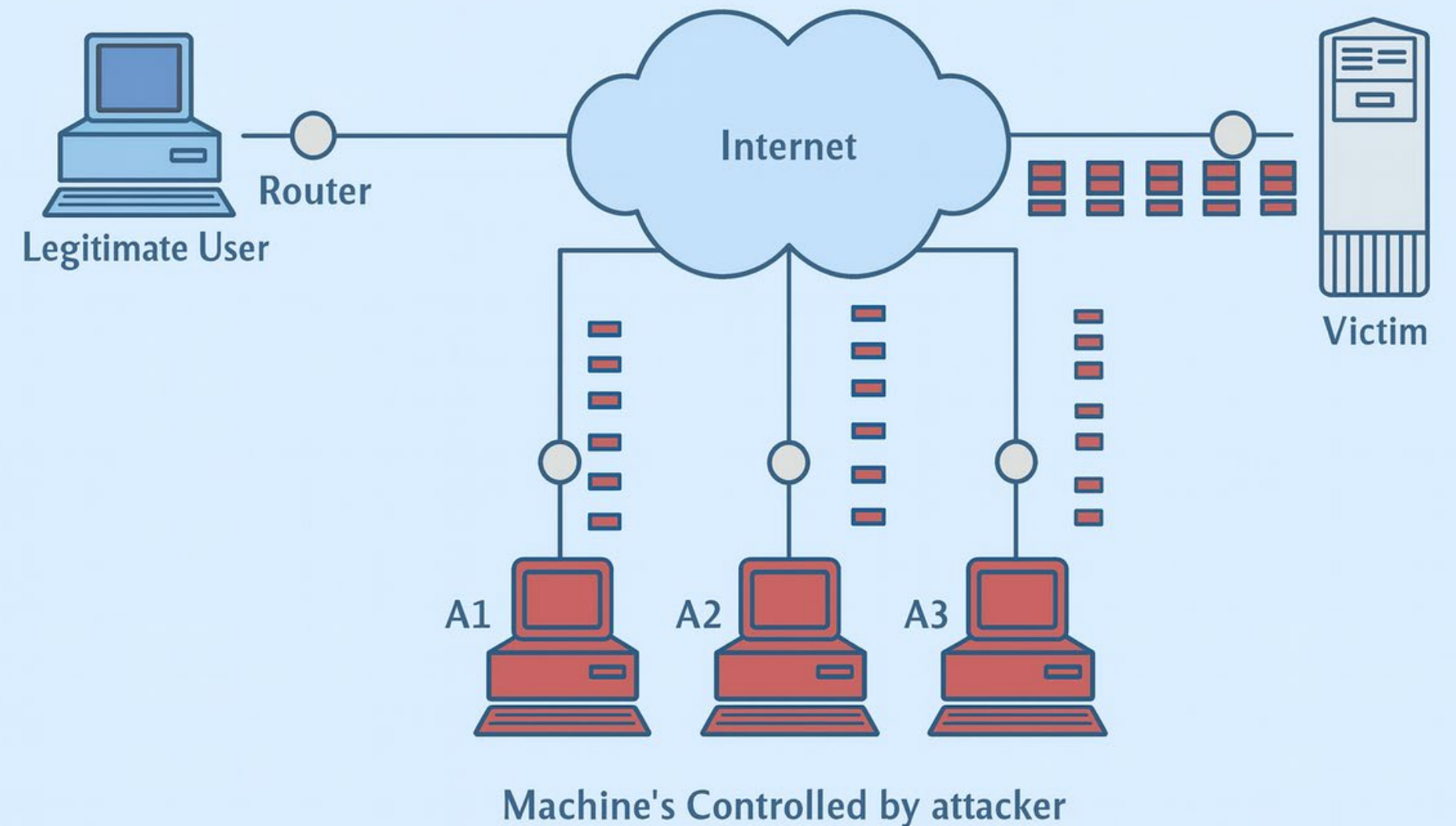
Agenda

Topics Covered

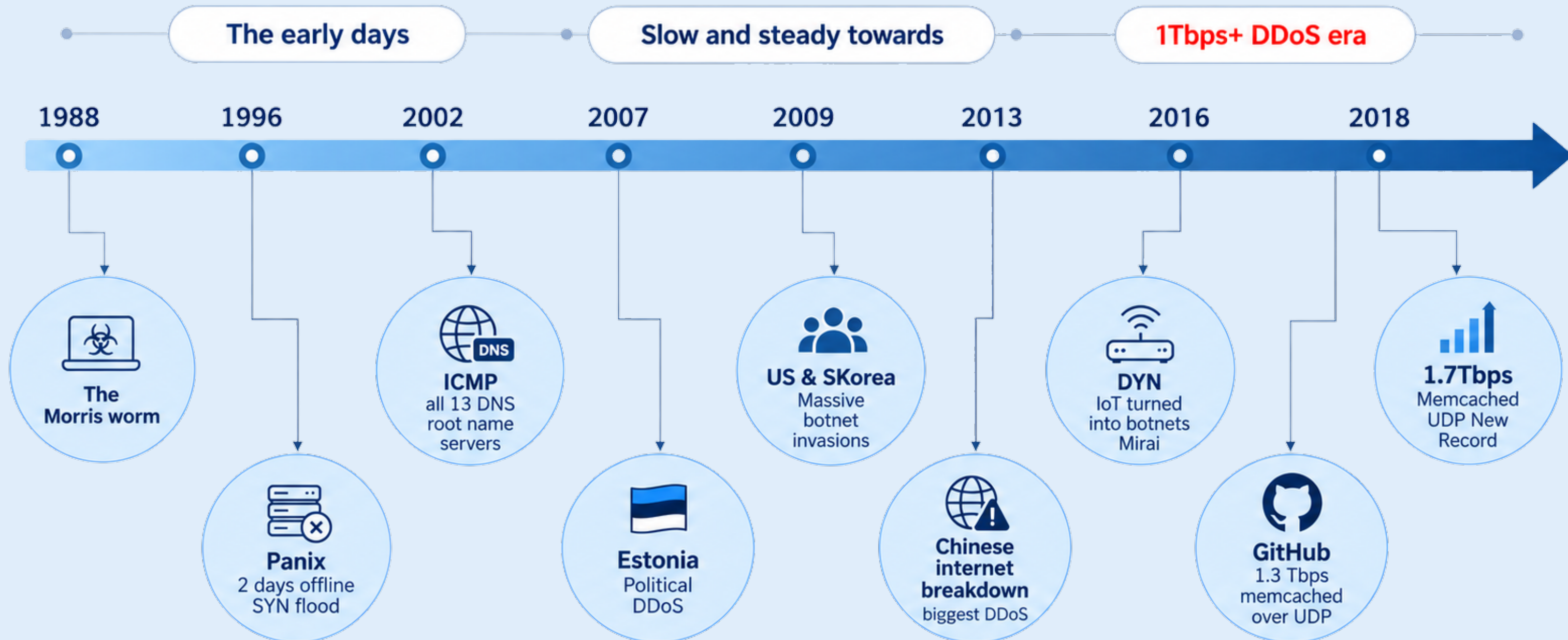
- 1 What's happening in the L3 & L4 DDoS landscape?
- 2 Underlying botnet architecture and economics
- 3 Why is DDoS still a problem?

What is a DD oS Attack?

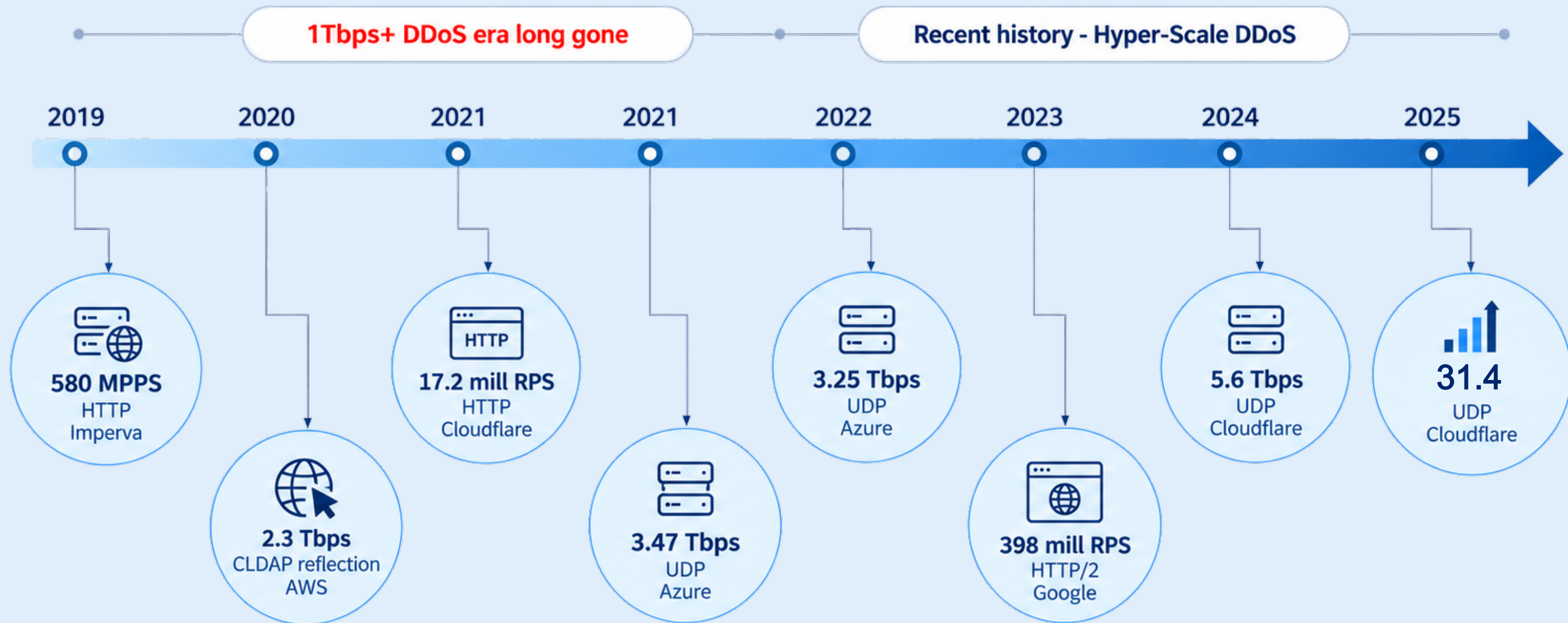
A DDoS (Distributed Denial -of-Service) attack **floods** a server or network with “**fake**” traffic from multiple sources, making it **slow** or completely **unreachable** for real users.



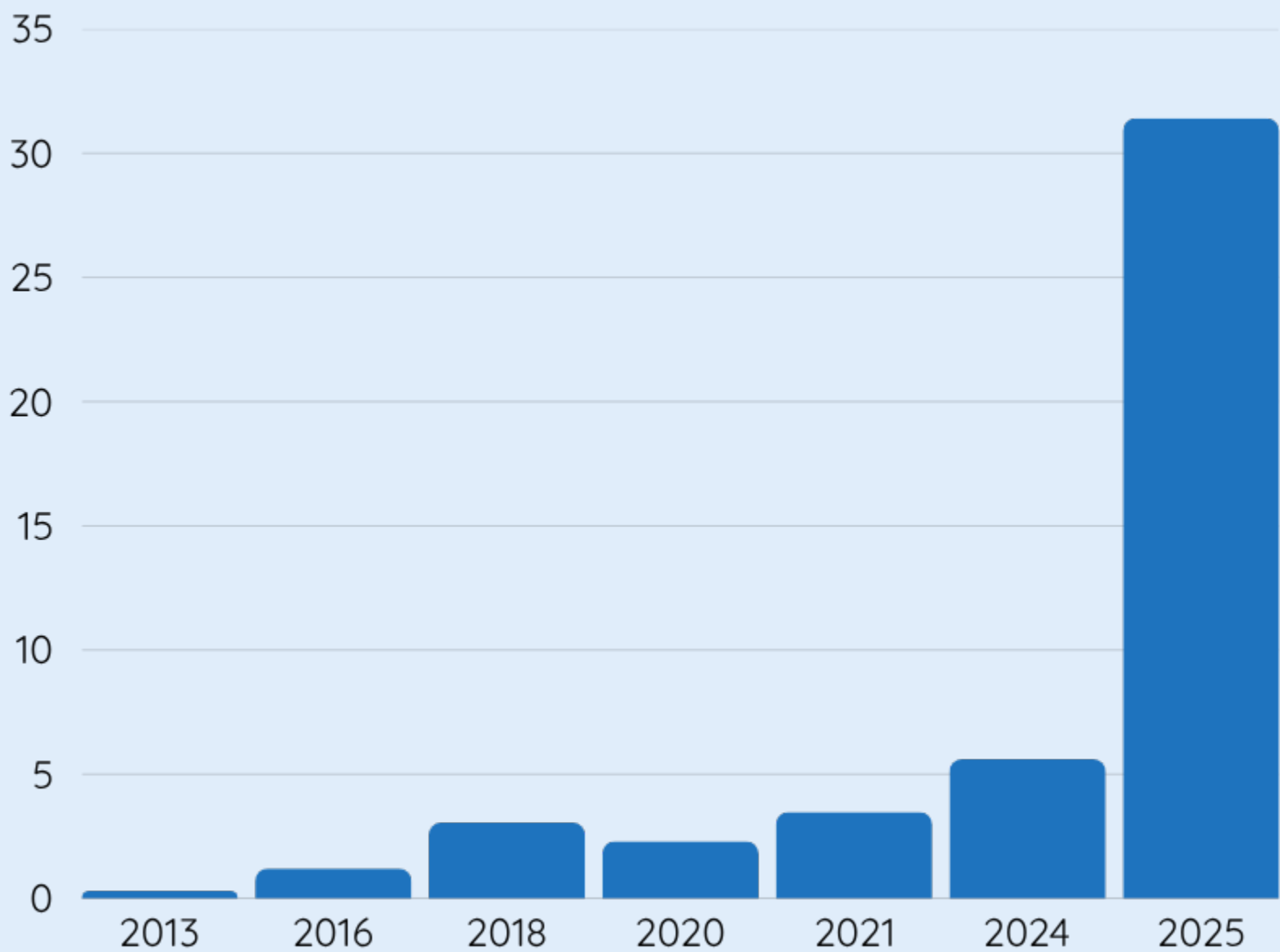
History of DDoS: from Gbps to 30+ Tbps



History of DDoS: from Gbps to 30+ Tbps

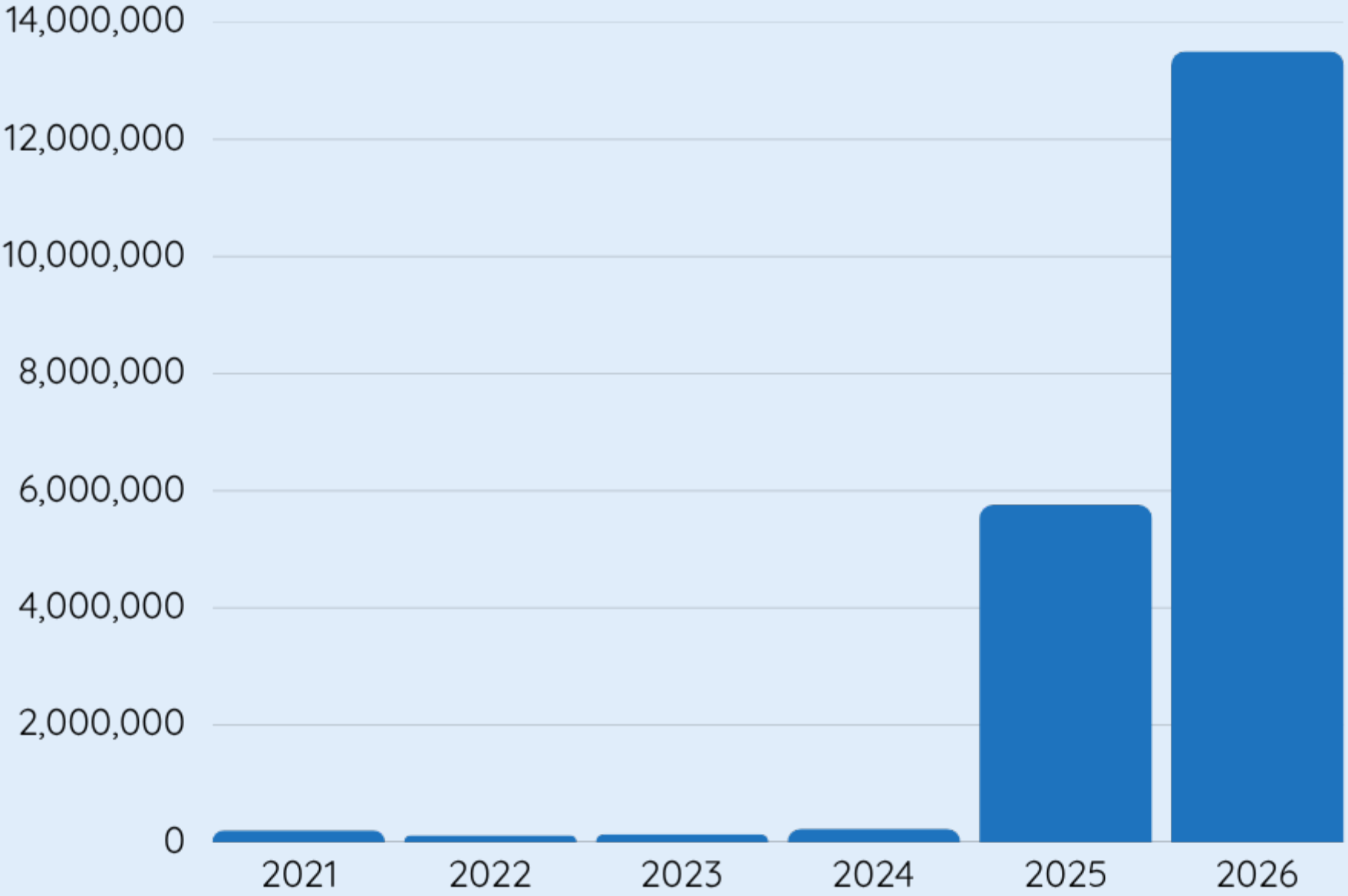


State of DDoS: from Gbps to 30+ Tbps

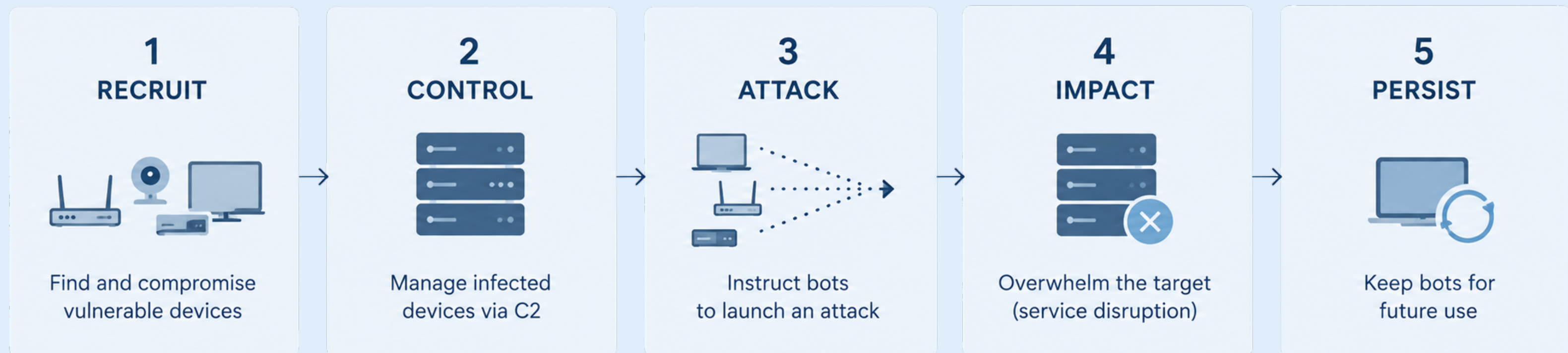


Year	Attack reported	Peak Tbps
2013	Spamhaus	0.30
2016	Mirai / Dyn era	1.20
2018	GitHub memcached	1.35
2018	Memcached record	1.70
2020	AWS CLDAP reflection	2.30
2021	Microsoft Azure	3.47
2024	Cloudflare UDP	5.60
2025	Cloudflare	7.30
2025	Cloudflare	11.50
2025	Aisuru / Cloudflare	29.70
2025	Cloudflare	31.40

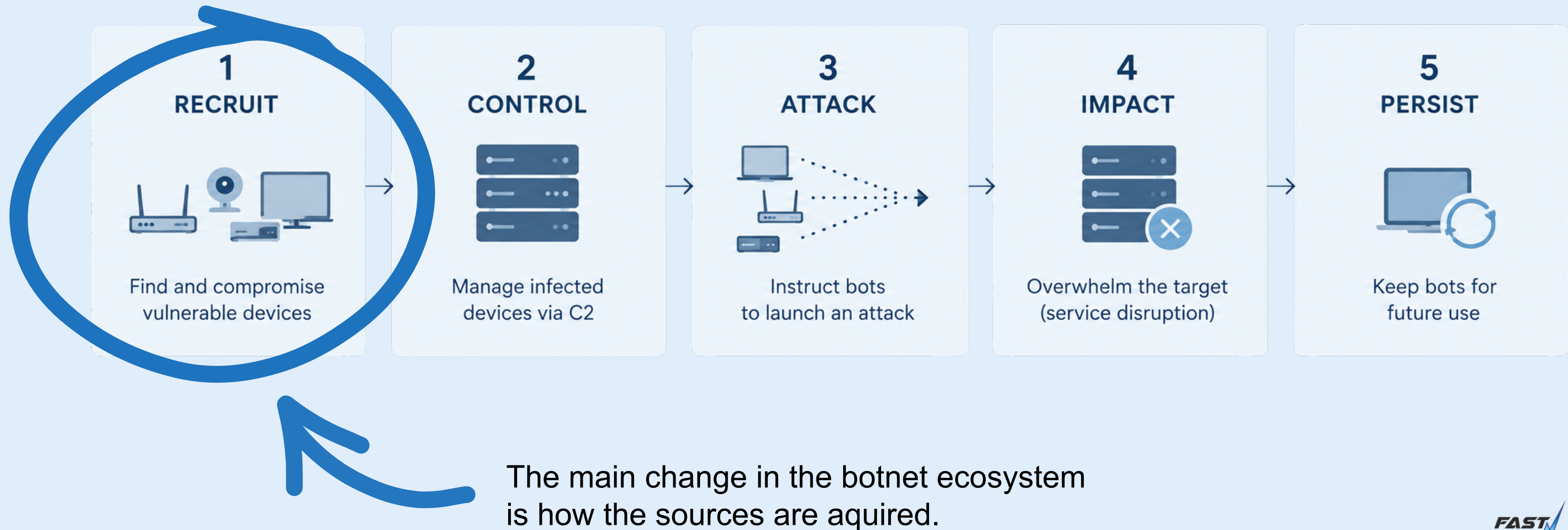
Botnets went from thousands to millions of active sources



Anatomy of a Botnet



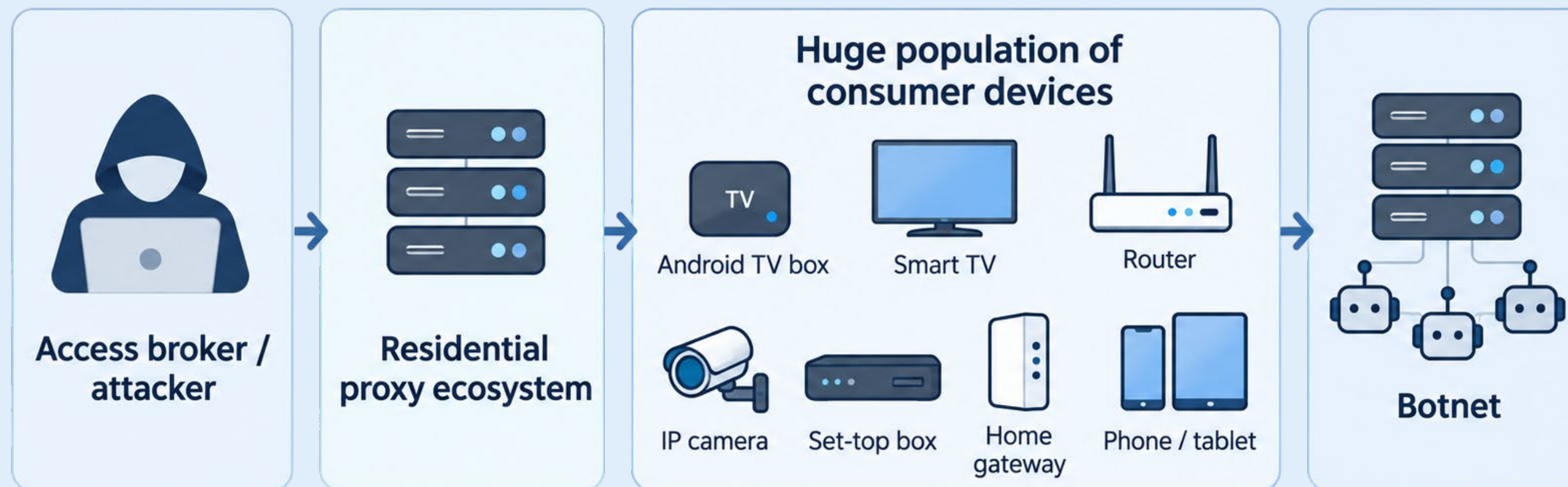
Anatomy of a Botnet



The old model: scan → exploit → infect



A new supply of bots: residential proxies

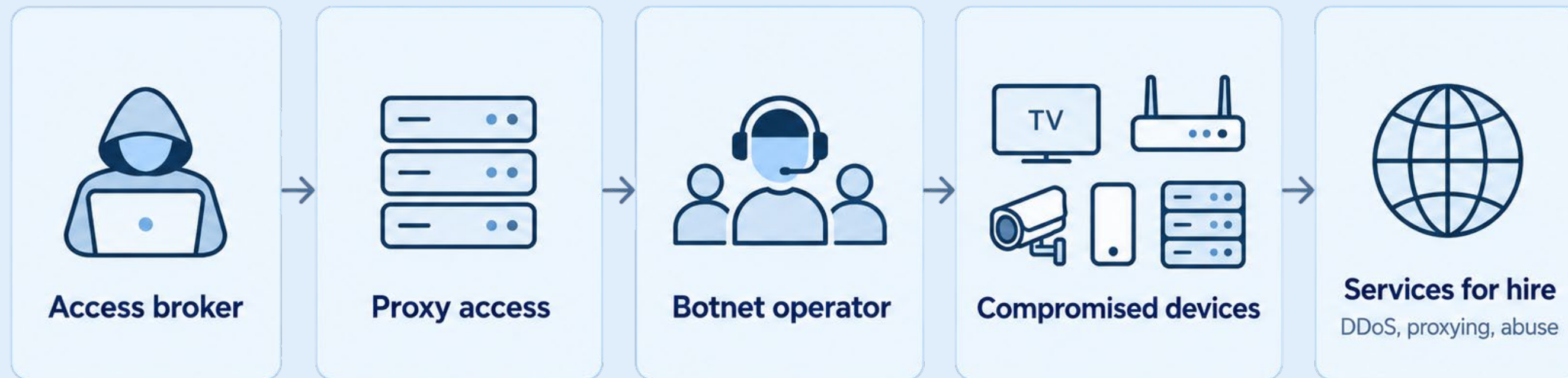


~1M
previous active DDoS bots

100-200M
potentially reachable devices

Residential proxy ecosystems greatly expanded the pool of potential attack sources

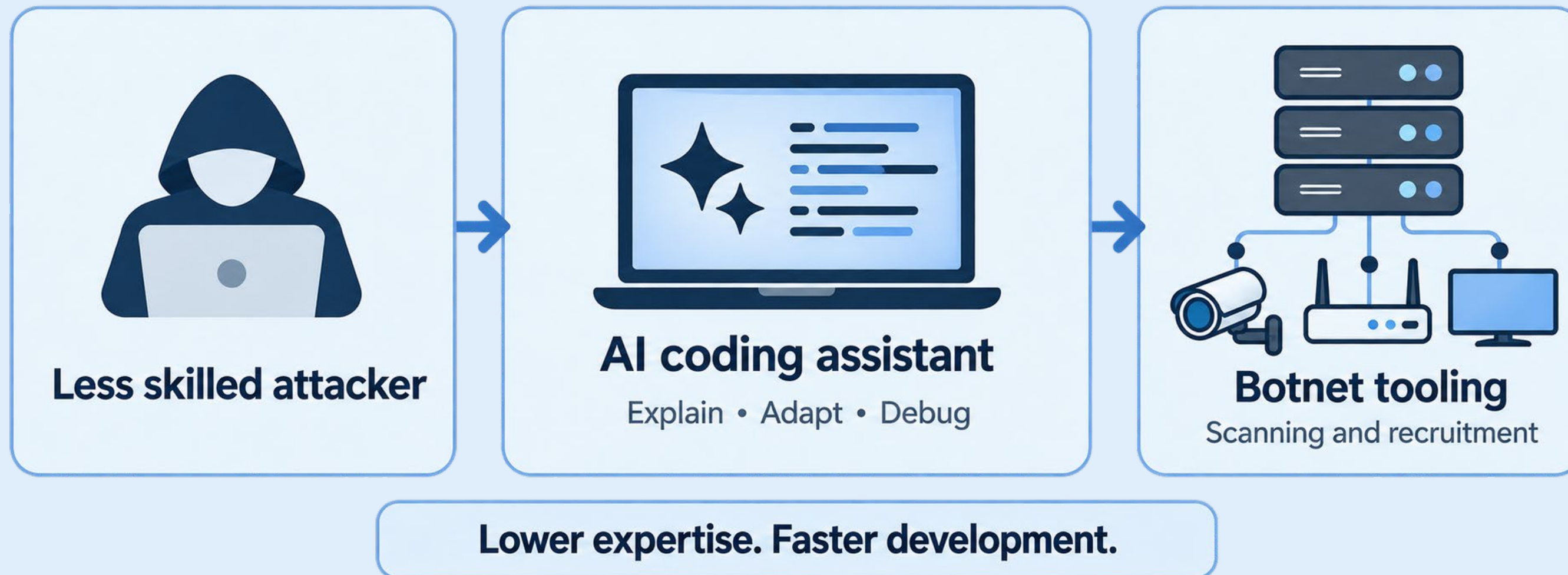
From building botnets to buying access



Buy access → build or rent the botnet → monetize the devices

AI lowers the barrier to building botnets

AI helps less skilled attackers understand vulnerabilities, adapt existing tools and troubleshoot code used for botnet recruitment.



Sources: S2W TALON · Google Threat Intelligence Group

AI-assisted botnet recruitment: a real case

In January 2025, KuroCracks advertised a scanner for botnet recruitment and described developing it with AI assistance.



Source: S2W TALON · 13 May 2025

Botnets now compete for the same infrastructure



Why is DDoS still a problem?



- **Remove one botnet, the supply remains**
 - Vulnerable devices, proxy access, brokers, and infrastructure are still there.
- **Compromised devices have multiple uses**
 - DDoS, proxying, credential abuse, scanning, lateral movement.
- **Successful access paths get copied**
 - AI assistance makes it easier for less skilled attackers to adapt existing tools and troubleshoot recruitment code.

Conclusions and future evolution

1. Takedowns work—but the target is changing

- Disrupting C2 still matters
- Recruitment now runs through proxy/access ecosystems

2. Outbound DDoS is now an operator problem

- Large bot populations can hurt the source network too
- Source-side visibility and containment matter
- DDoS defense becomes a shared responsibility

3. AI lowers the entry barrier

- Less expertise needed to develop and adapt malicious tools
- AI assistance supports botnet recruitment and tool development
- Further automation could shorten the time defenders have to respond

4. Defenses are adapting too

- Faster automated detection with AI
- More source-side cooperation and threat sharing

Thank you!



Virgil Truica

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

virgil@fastnetmon.com / virgil@salesflow.tech

[linkedin.com/in/ virgiltruica](https://linkedin.com/in/virgiltruica)

+40 742 991 619