DDoS Botnets Today

Threat Intel & Lessons Learned to Defend Against DDoS

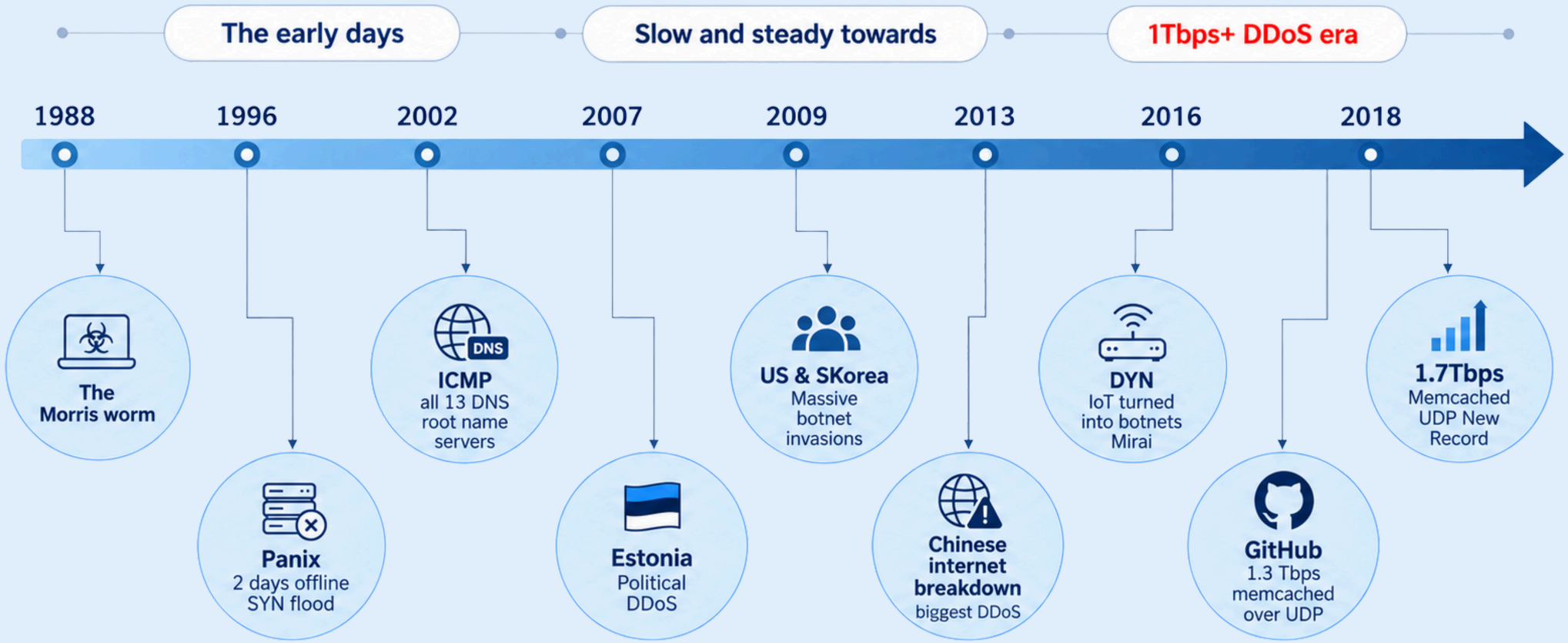
By Outi Maria Pietilanaho
FastNetMon
September 10th 2026

Agenda

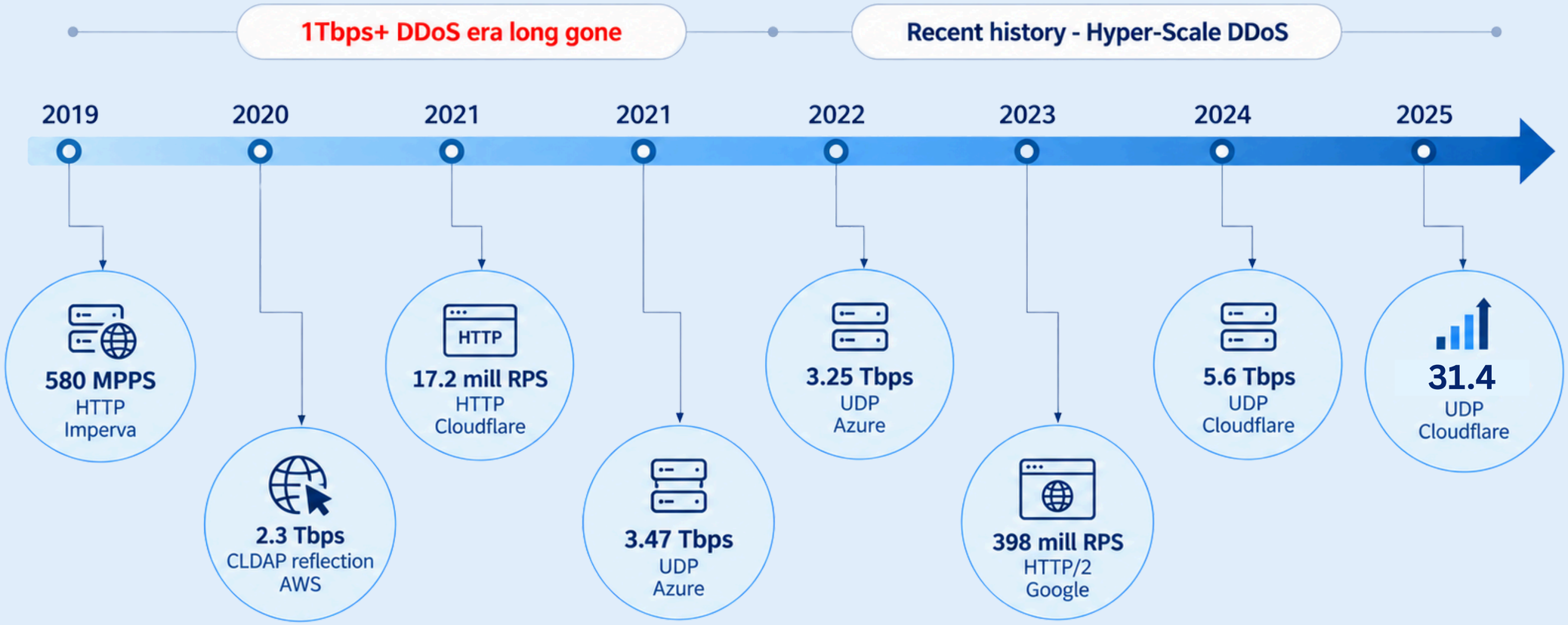
Topics Covered

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

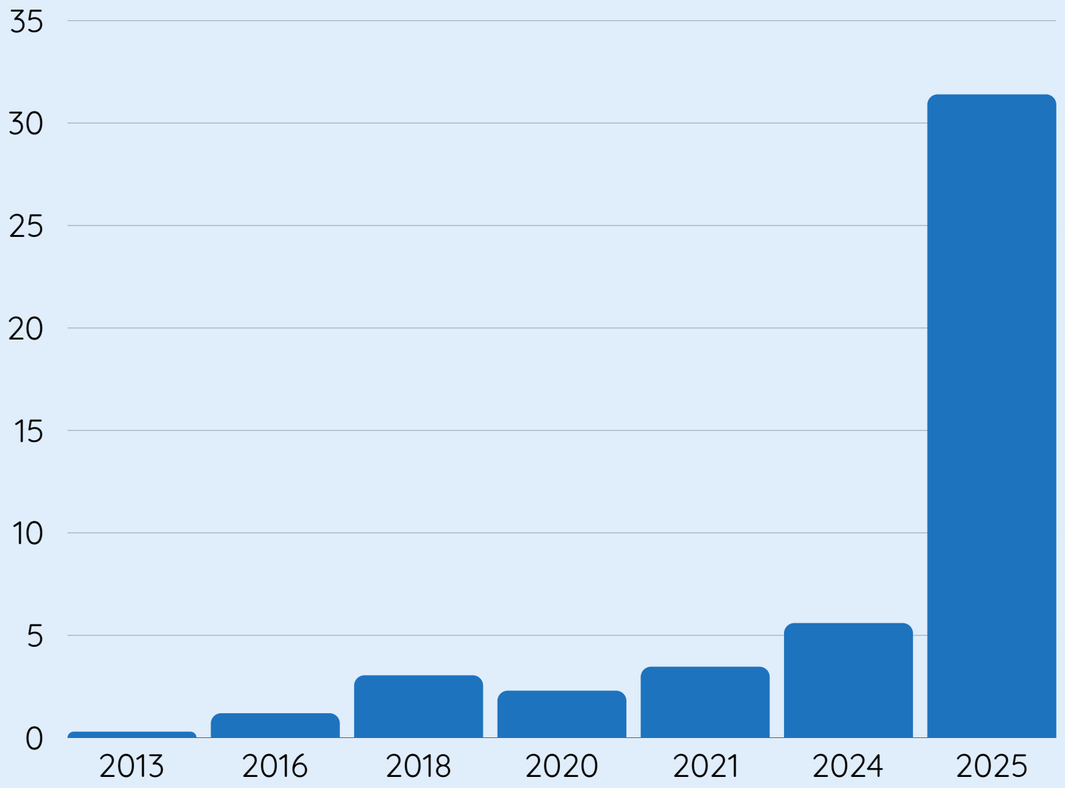
History of DDoS: from Gbps to 30+ Tbps



History of DDoS: from Gbps to 30+ Tbps



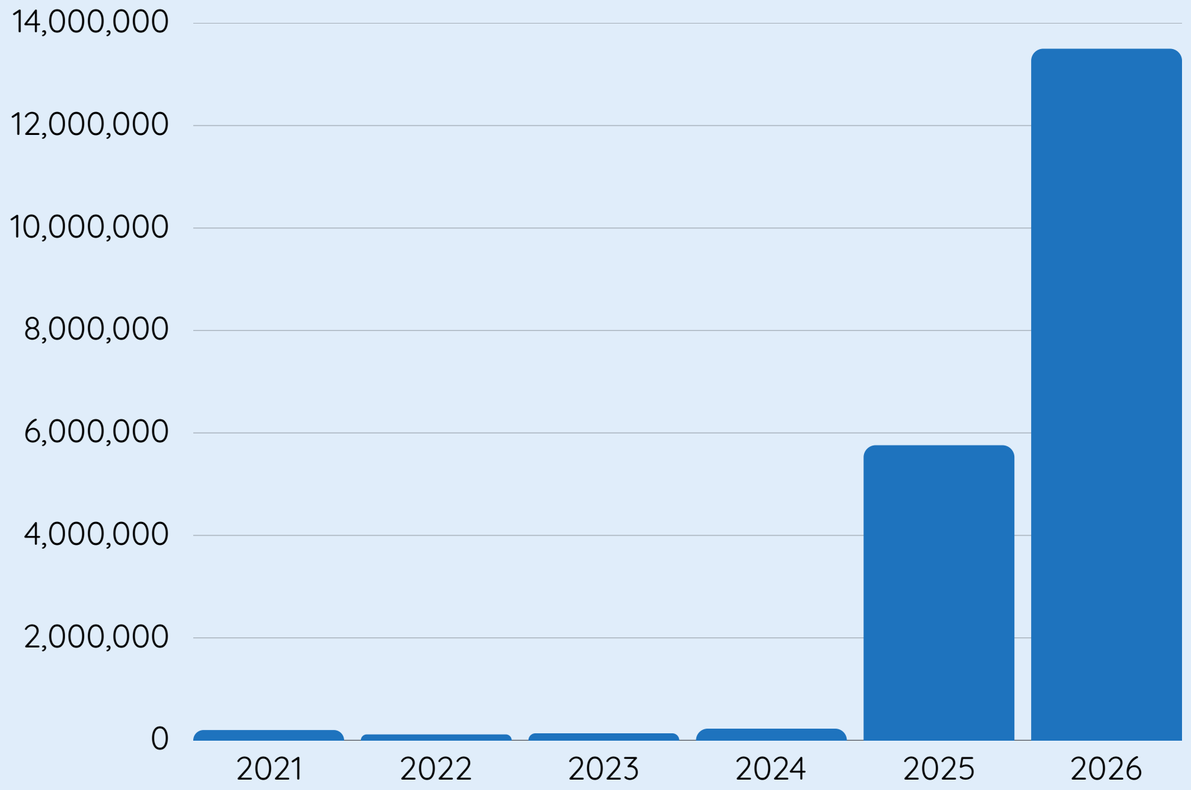
State of DDoS: from Gbps to 30+ Tbps



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

FASTNETMON

Botnets went from thousands to millions of active sources



FASTNETMON

Anatomy of a Botnet

1
RECRUIT

Find and compromise vulnerable devices

2
CONTROL

Manage infected devices via C2

3
ATTACK

Instruct bots to launch an attack

4
IMPACT

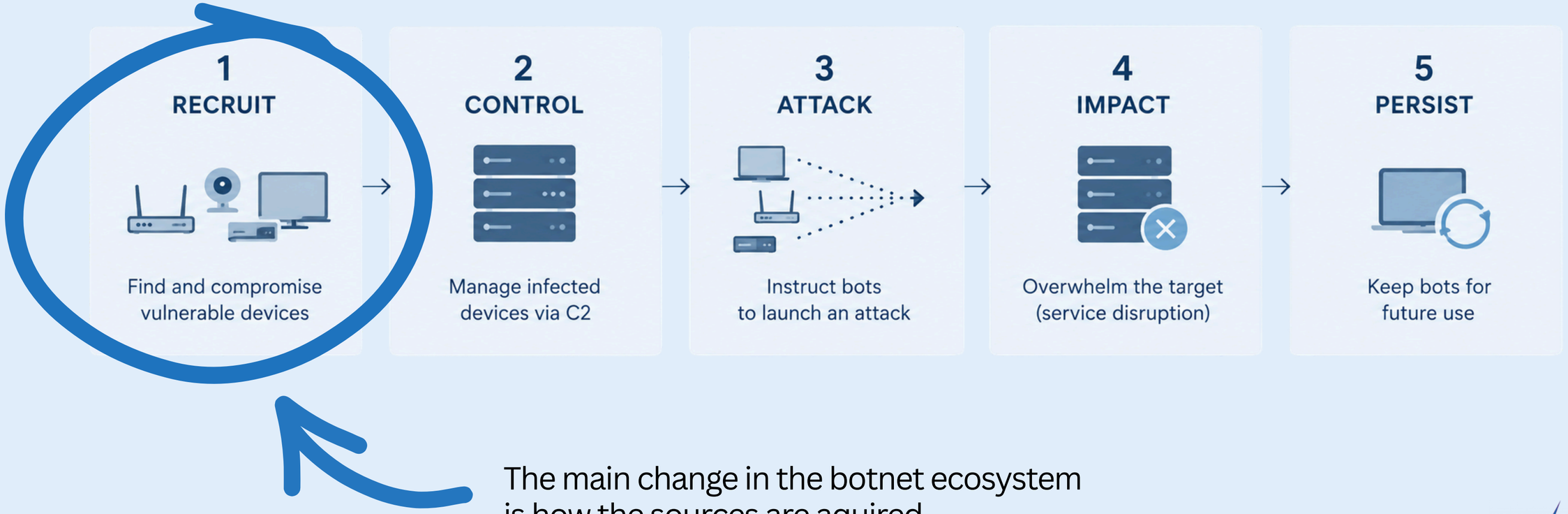
Overwhelm the target (service disruption)

5
PERSIST

Keep bots for future use

FASTNETMON

Anatomy of a Botnet



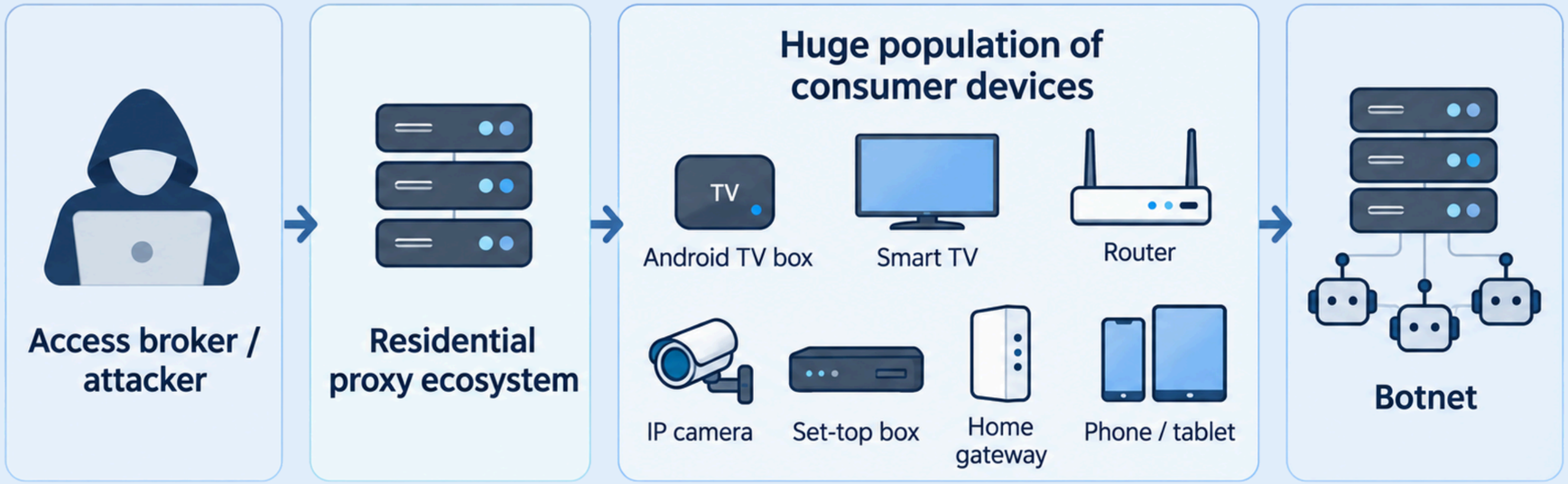
The main change in the botnet ecosystem is how the sources are aquired.

FASTNETMON

The old model: scan → exploit → infect

FASTNETMON

A new supply of bots: residential proxies



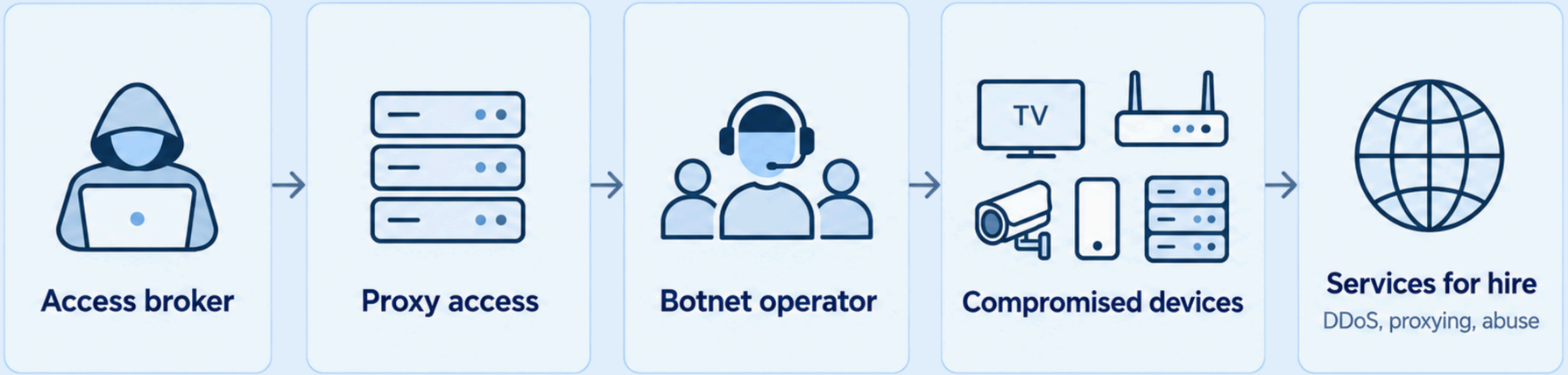
~1M
previous active DDoS bots

100–200M
potentially reachable devices

Residential proxy ecosystems greatly expanded the pool of potential attack sources

FASTNETMON

From building botnets to buying access



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

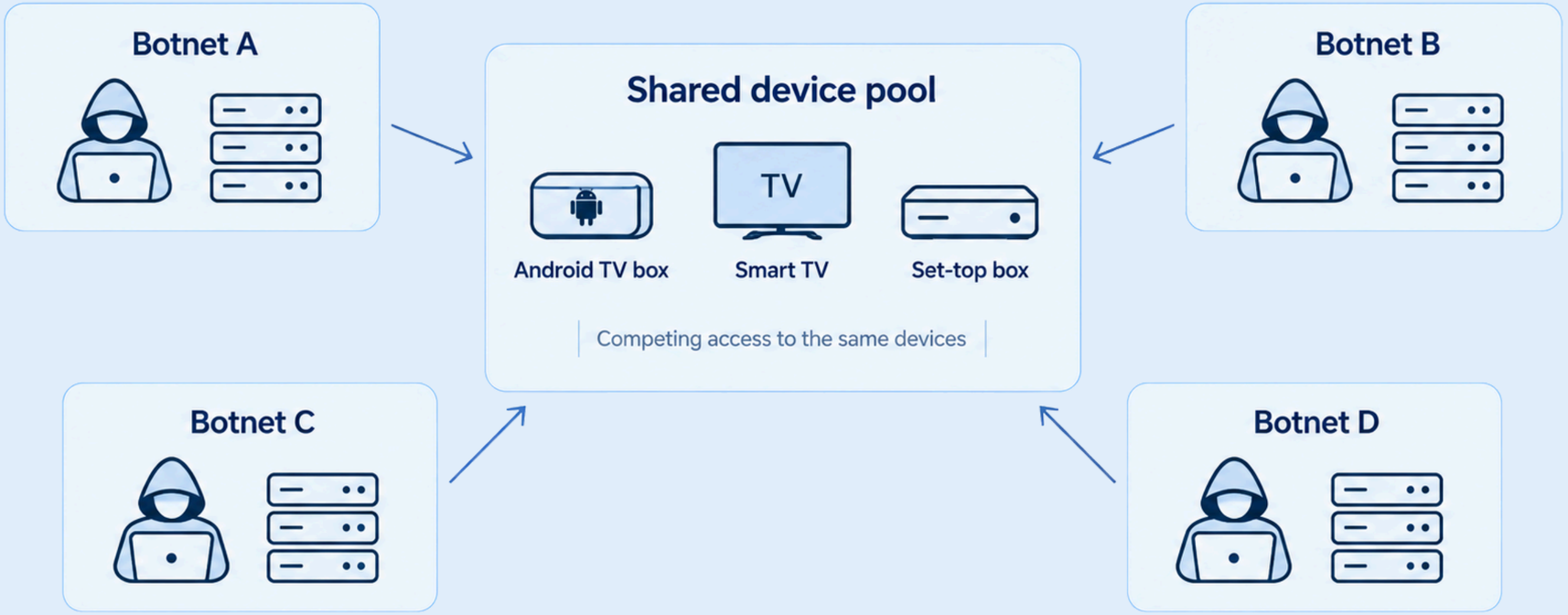
FASTNETMON

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**
  - Once one operator proves a method works, others adopt it quickly.

FASTNETMON

Botnets now compete for the same infrastructure



FASTNETMON

Concusions and future evolution

1. Takedowns work — but the target is changing

- Disrupting C2 still matters
- Recruitment now runs through proxy/access ecosystems
- ENS / blockchain-based coordination makes some C2 harder to remove

2. Outbound DDoS is now an operator problem

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

3. Defences are adapting too

- Faster automated detection
- More source-side cooperation and threat sharing
- Takedowns + network controls + remediation together

FASTNETMON

FAST NETMON

Thank you!

Get the slides, connect with me, find more info -->