# Botnets, Proxies, and the New Era of Hyper-Scale Attacks

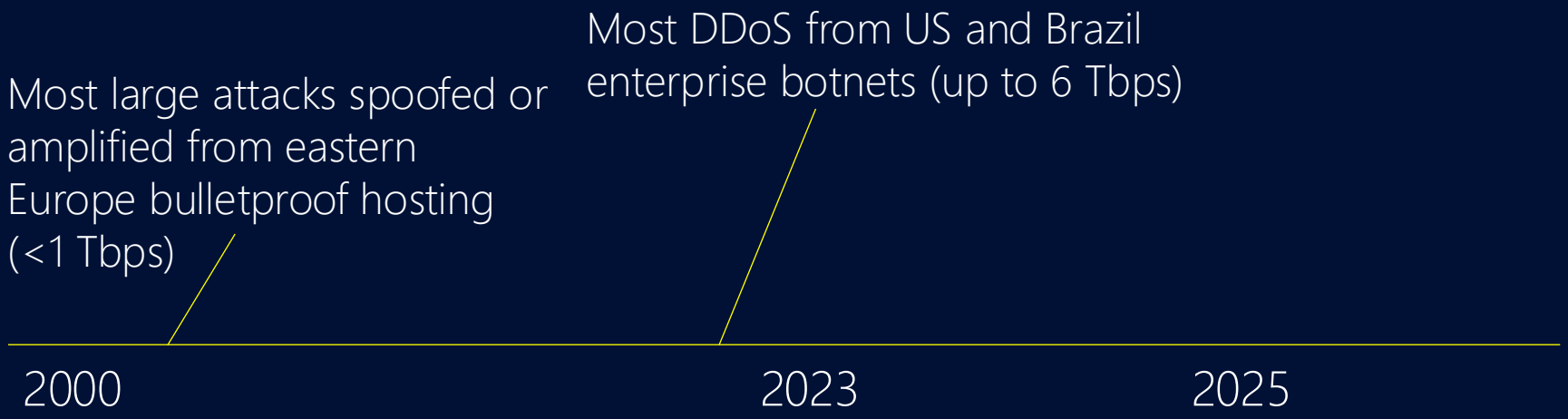
Craig Labovitz

Nokia Deepfield

December 2025

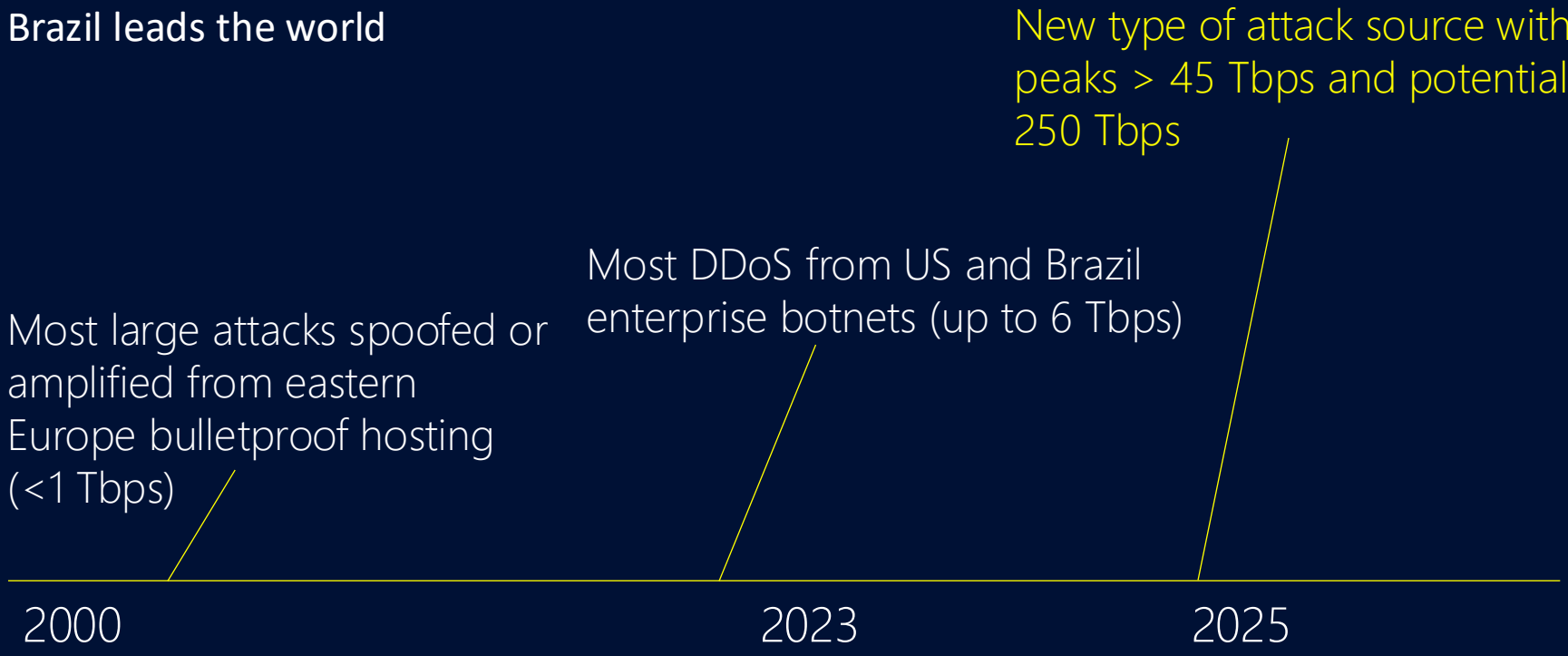
# A Brief History of DDoS

## Brazil leads the world



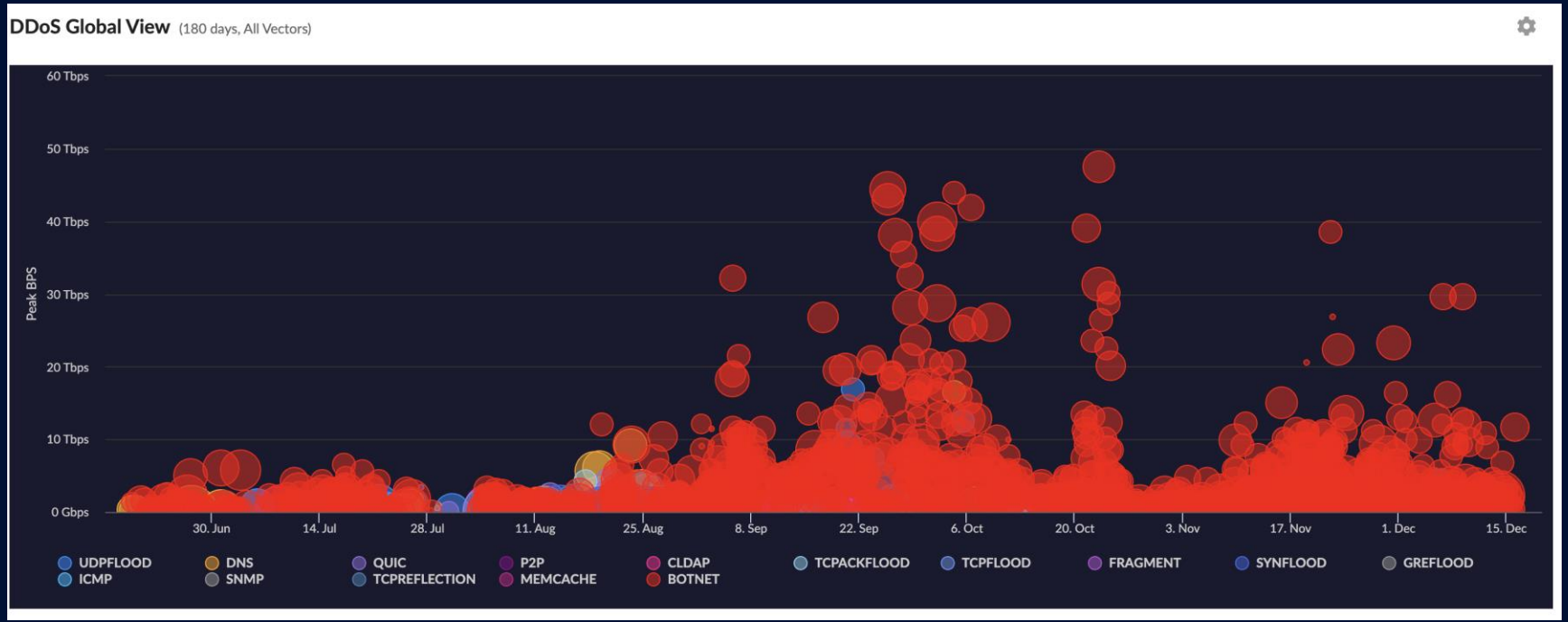
# A Brief History of DDoS

## Brazil leads the world



# DDoS attack increase size / frequency

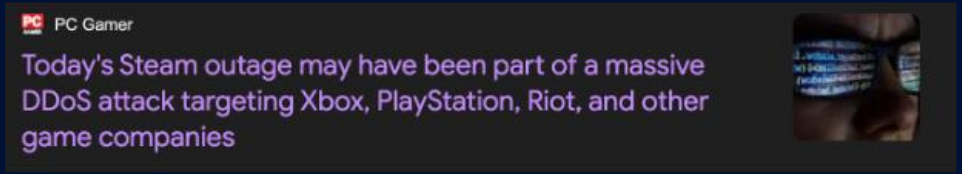
## Dramatic growth in second half of 2025




Graph of attacks by peak bps and attack vector using Nokia GDTA data from collaborating customers. Size of circle corresponds to duration of attack

# DDoS Increase in Outages

- Attacks different in size, number of non-spoofed sources, and geography
- Critically, also surprising number of outages in well-defended social media, game, telecom, finance and government

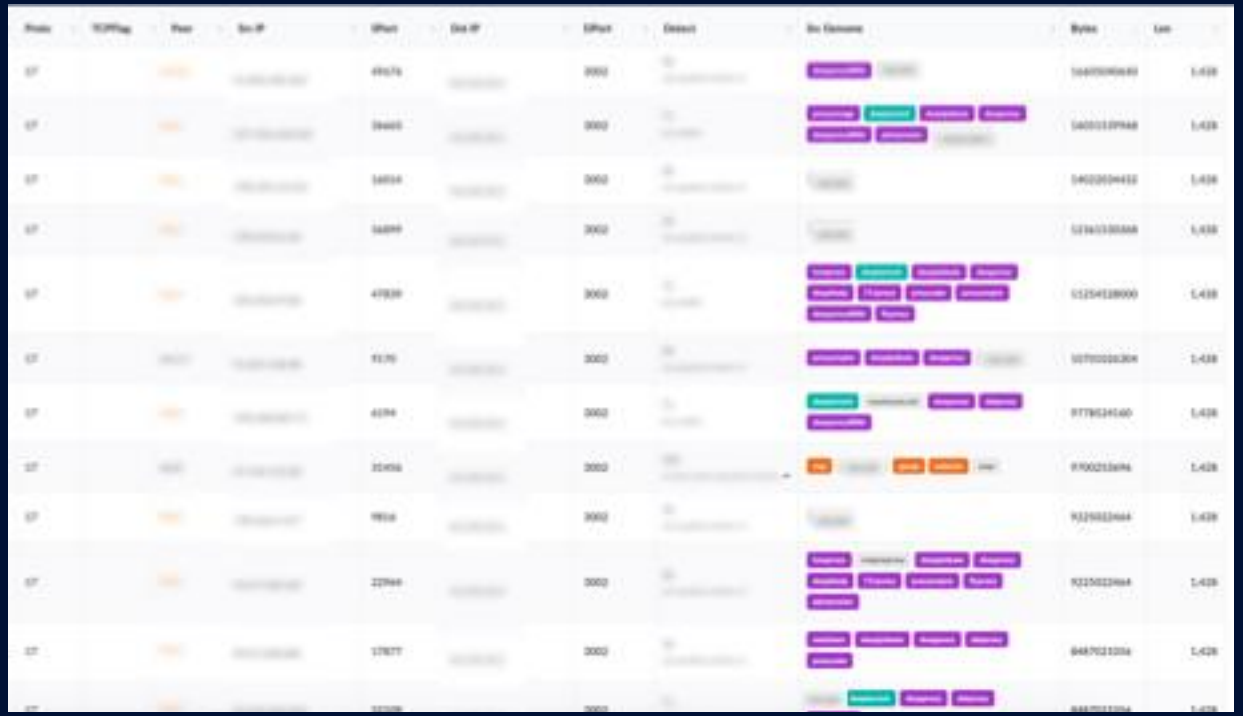

# Motivation

## typical DDoS before 2025 used enterprise cpe / dvr

- Probable **CVE**
- Active in **Botnet** (48h)
- Active in **Proxy** (24h)
- Active in **Monetization** (48h)

# Motivation

## New type of DDoS May 2025

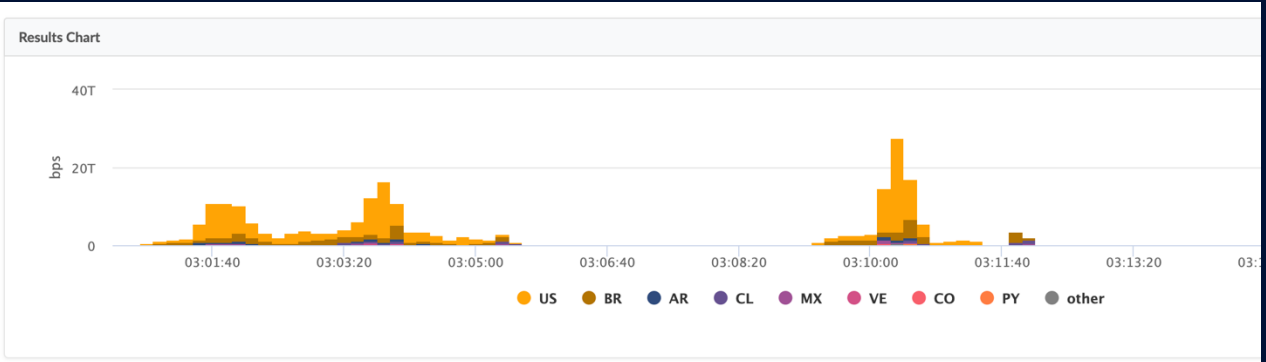


Regular, daily large-scale residential proxy DDoS

- Active in **Proxy** (24h)
- Active in **Monetization** (48h)

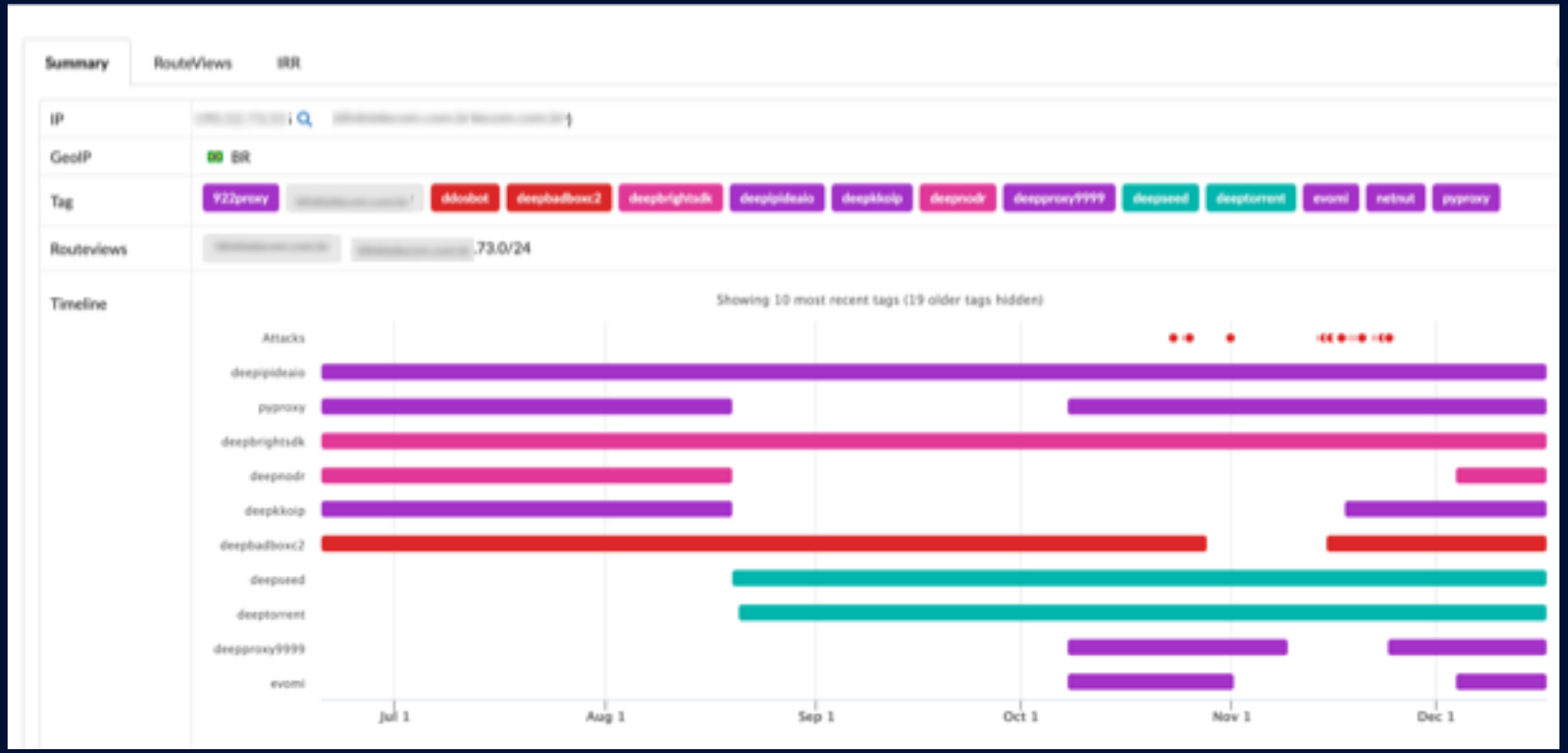
# 20+ Tbps DDoS Example

## December 16, 2025




| Src Country | % Bytes | % Packets | % Nunique Src |
|---|---|---|---|
| US | 67.40 | 67.33 | 74146 |
| BR | 19.82 | 19.81 | 26479 |
| AR | 4.02 | 4.01 | 11111 |
| CL | 3.02 | 3.01 | 3017 |
| MX | 2.47 | 2.47 | 3120 |
| VE | 0.45 | 0.45 | 614 |
| CO | 0.38 | 0.38 | 855 |
| PY | 0.26 | 0.26 | 408 |

# Brazil IP Example




Compromised devices frequently begin as residential proxy / financial crime and move to DDoS

# Let’s talk about residential proxy…

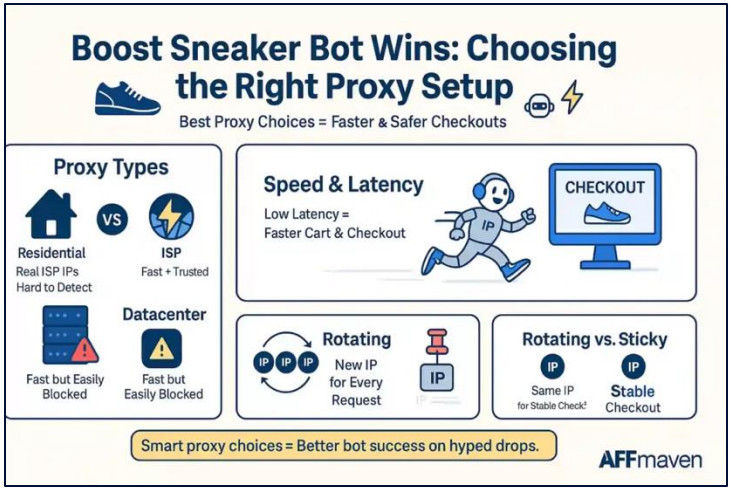
# Understanding Res Proxy
last 24 months

- Active proxy discovery
  - Proxy observed in DDoS + 3rd party data sources
  - Blockchain analysis
- Honeypot and sandbox networks
- Global crawling and passive DNS samples
- GDTA IPFIX samples from collaborating telco providers

# Buy Residential Proxy

Traditional marketing split between black and legal / grey area use cases


Black Hat

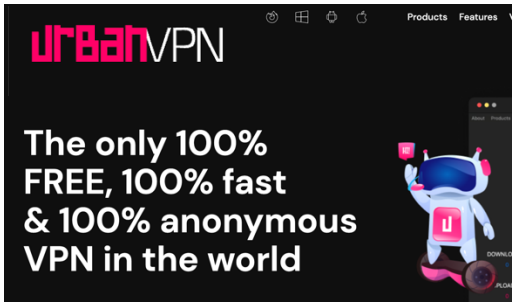



Gray Hat

# Install Residential Proxy

## 30+ SDK companies and malware



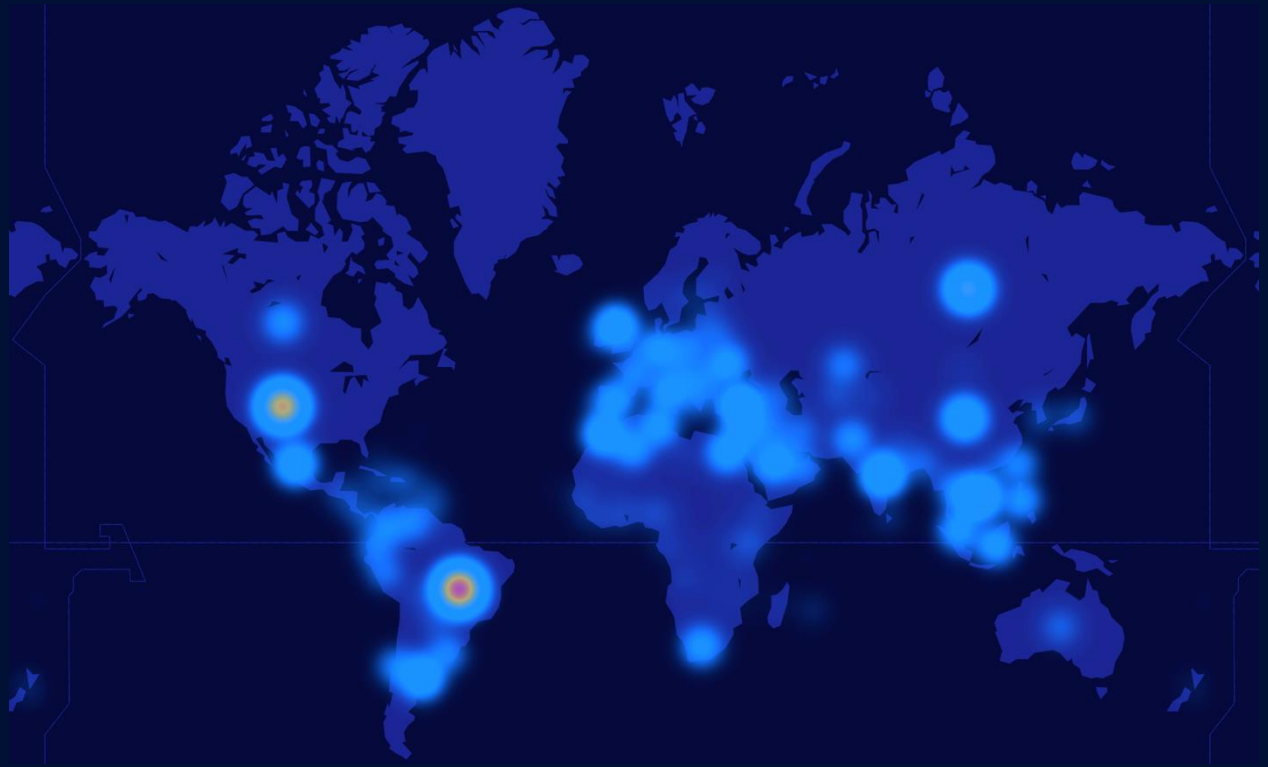




Proxy SDK intentionally installed by end-user or via malware
Malware installs multiple proxy clients for monetization

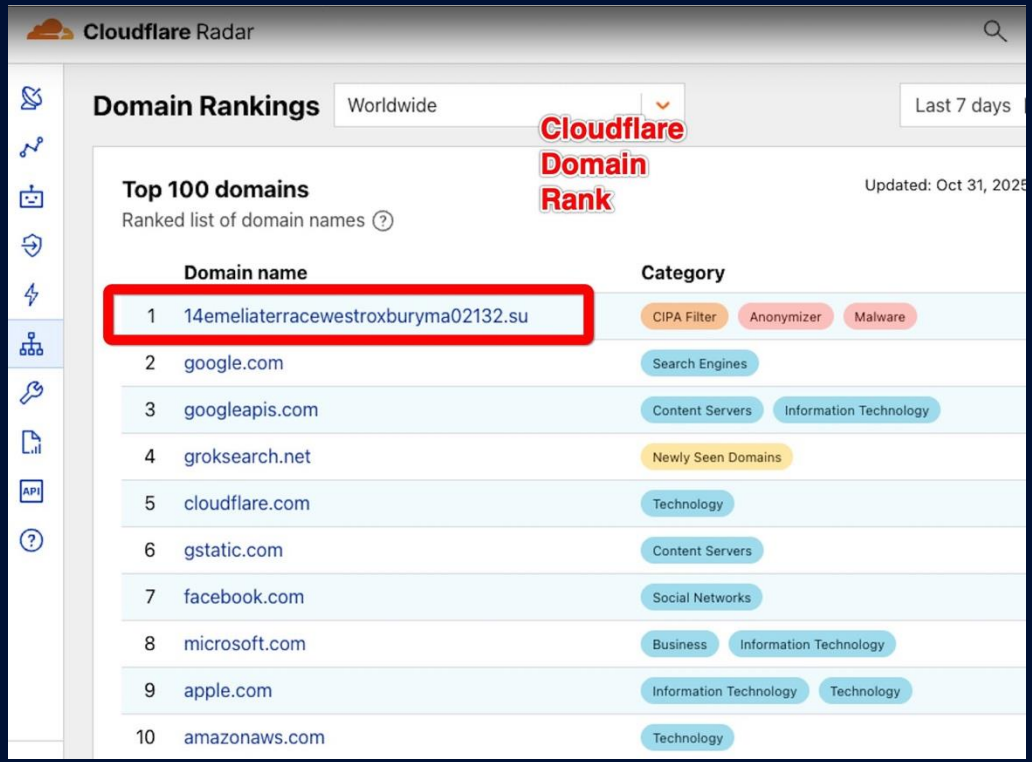
# DDoS attack dramatic increase size / frequency

v4 fixed 100M+ globally with NA (10M+) second to Brazil (25M+)



# 31 October 2025: something strange in (Cloudflare) DNS ranking

## Wait, what's at number one?

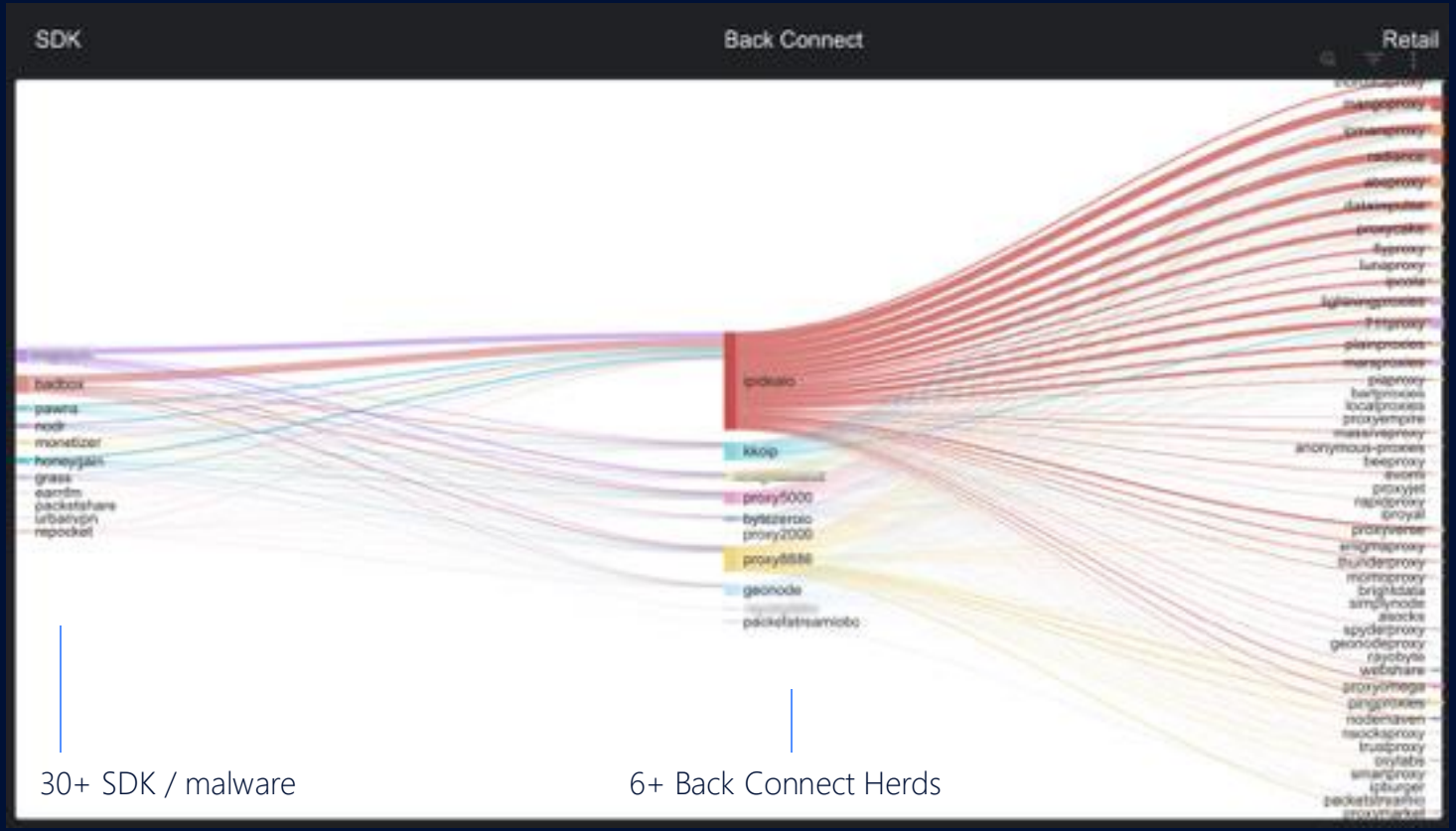



- A botnet C2 domain with more DNS queries than Google
- .su = Soviet Union TLD (yes, it still exists)

https://x.com/Xlab_qax/status/1984194350277157146

# Supply chain mapping

## The facade of competition




30+ SDK / malware

6+ Back Connect Herds

# IPIDEA

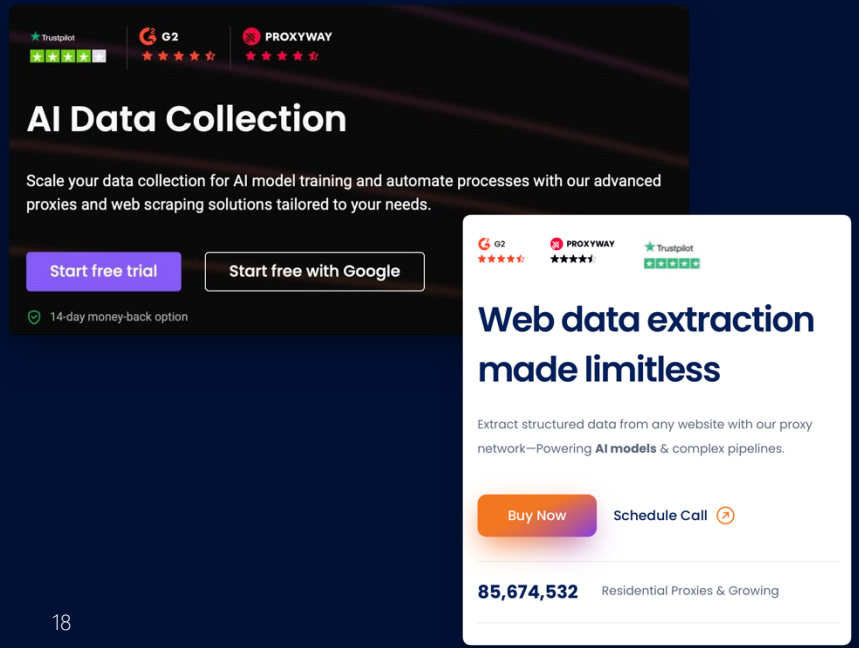
## Single “mega connect” controls majority wholesale global res proxy

- Exit points **in every region**: NA, EU, APAC, LATAM
- Present in your networks: CSPs, enterprise, education, gov
- Opaque ownership and accountability structure
- No meaningful abuse response process
- Single point of control = single point of weaponization
- Infrastructure decisions made without operator visibility
- No recourse when subscribers enrolled without consent
- Shared problem requiring shared solutions

# AI needs data, criminals need revenue

## Supply, meet demand

## Demand side: AI training pipeline

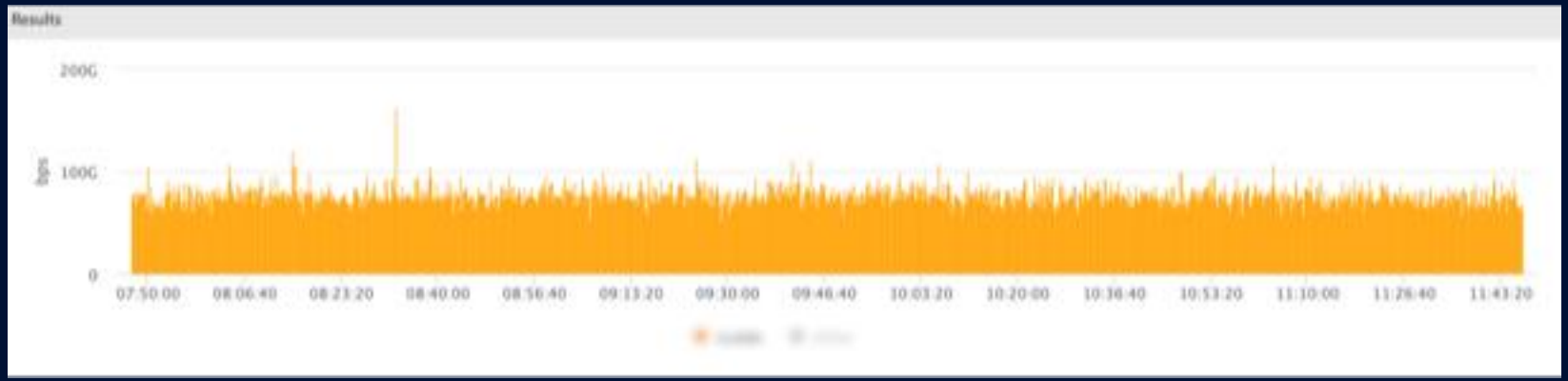



## Supply side: Symmetric Gigabit changed the math

- Average endpoint bandwidth: 275 Mbps → 482 Mbps (+75%)
  - (North American botnet endpoints, Q2 2024 → Q2 2025)
- Supply chain compromises at scale
  - TOTOLINK firmware server: 100K+ routers in one operation

# Who's paying for all this infrastructure?

## Sustained multi-hundred-Gbps flows from AI companies to res. proxy supernodes




What this really means:

- Legitimate enterprise demand is funding this infrastructure
- Same proxy pool routes AI training data and DDoS traffic
- Revenue from scraping sustains the attack capability

# The attack surface shift

## The devices you can't see

### "Conventional" DDoS botnets (2016-2024)

- Exposed IoT devices
- IP cameras, DVRs, routers
- Port forwarding, mostly static IPs
- Directly internet-facing

- You can scan for them
- ~1M active bots at peak

### ResHydra era (2025+)

- Consumer endpoints
- Android TV boxes, mobile apps
- "Free" VPN software
- Behind NAT / CGNAT

- Mostly only outbound
- 100-200M exploitable surface

# The 250 Tbps elephant in the room

## The math

- ~200M proxy endpoints (up ~2× since early 2025)
- 100 Mbps average upstream bandwidth

→ multi-Pbps theoretical, 250 Tbps achievable

## Context

- Most national backbones: tens of Tbps total capacity
- Largest (publicly) recorded attack: 33 Tbps
- This infrastructure can exceed national network capacity

## Capability exists today

- Nodes are infected
- C2 is operational
- Only question is targeting

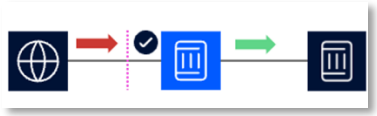


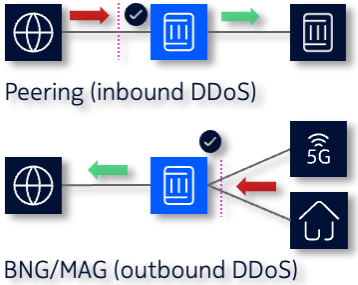
NOKIA

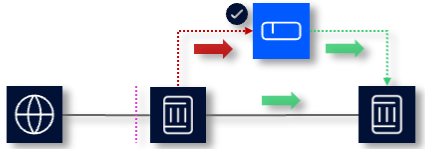
# What do we do about ResHydra / Kimwolf?

# How network protection needs to change

Security defense must be **built into every layer of the network**





## IXP

- Block volumetric at Internet eXchange Points (IXP)
- Commercial services leveraging IXP router / switch infrastructure
- Examples: NL-IX, LINX, KINX

## Network Edge

- Surgical mitigation of inbound volumetric and some application attacks
- Always on visibility, alerting and some critical infrastructure threats
- Block outbound res proxy and botnet

## Scrubbing Center

- Mitigation can be event-driven or always-on
- Volumetric + enhanced L7 countermeasures
- DNS, TLS, HTTP, TCP, SIP server protections

## Inline

- Often deployed as a component of overall DC security protection
- Sees all in/out (bidirectional) traffic; higher mitigation efficacy
- Always-on mitigation

# Proactive versus Reactive Security Stance

## Automated C2 blocking to protected outbound from <u>your</u> subscribers

**Genome Shield**
The first line of defense for your network

Search shield filters... | + Add

| Name | Description | DFMatch Filter | GID | |
|---|---|---|---|---|
| C2 Botnet Aisura | Block command and control (C2) communication with Aisura botnet to limit outbound and east-west botnet driven DDoS traffic | df['addr.src'].isin([ GENOME_AISURA_C2 ]) | 10001 | ✎ |
| C2 Botnet Badbox | Block command and control (C2) traffic to Badbox (millions of low-cost, uncertified Android devices with pre-installed malware) | | 10003 | ✎ |
| C2 Residential Proxy | Block or rate limit communication to residential proxy back connect and command and control infrastructure | df['addr.src'].isin([ GENOME_RESIDENTIAL_PROXY ]) | 10002 | ✎ |

Showing 1 to 3 of 3 entries

Previous | 1 | Next

# Final Thoughts

- Kimwolf / ResHydra now critical and growing threat
- Technology exists detect / block
- Larger issue is awareness, business model and coordination
- Global collaboration of ISP, IXP, Governments and Law Enforcement


NOKIA