

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

Craig Labovitz

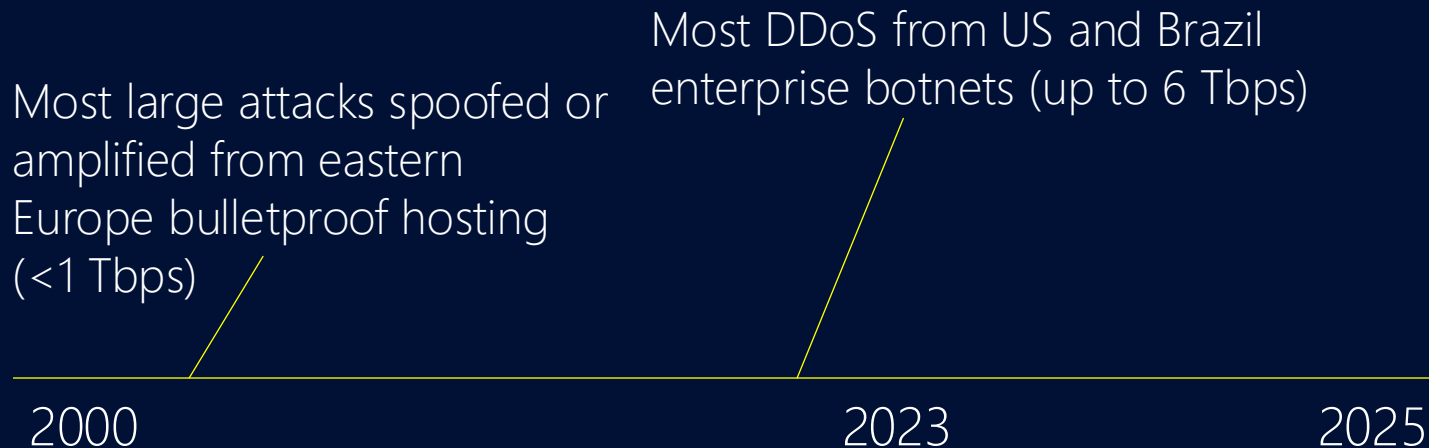
Nokia Deepfield

December 2025



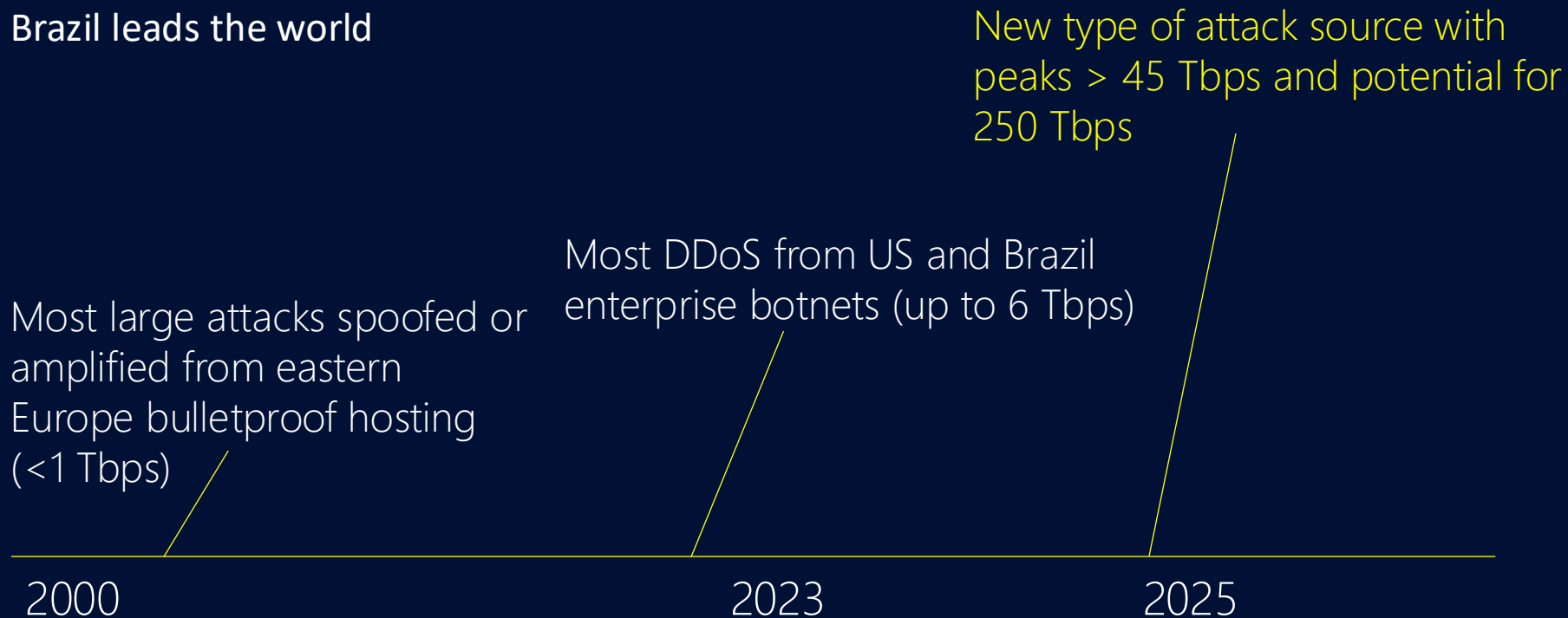
# A Brief History of DDoS

Brazil leads the world



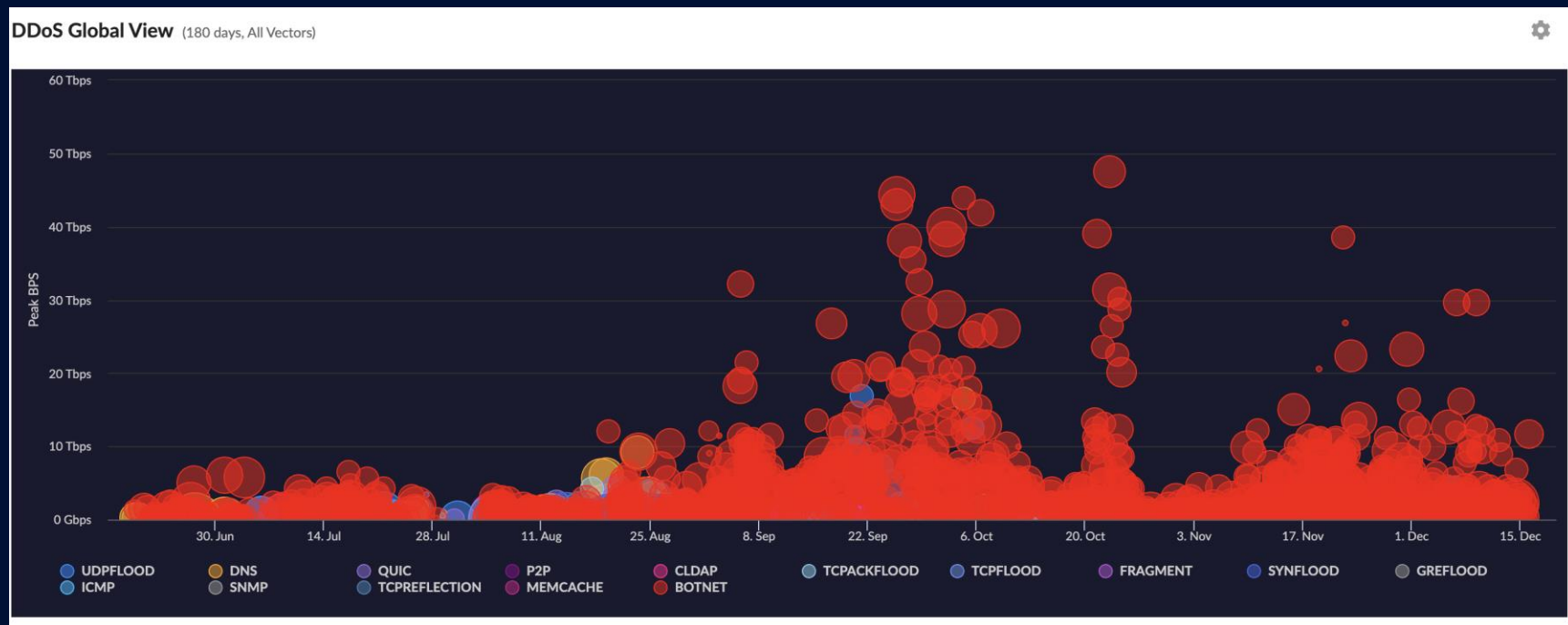
# A Brief History of DDoS

Brazil leads the world



# DDoS attack increase size / frequency

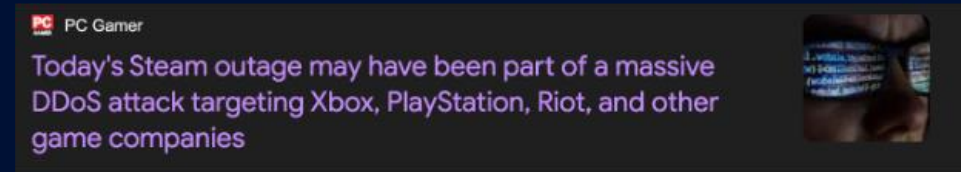
Dramatic growth in second half of 2025



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

New type of DDoS May 2025

Index	ICPFlag	Peer	Src IP	IPPort	Dst IP	DPort	Event	Src Genome	Bytes	Len
07			192.168.1.1	49152	192.168.1.1	8080	Connection	Active in Proxy (24h)	1040000000	1,428
07			192.168.1.1	30000	192.168.1.1	8080	Connection	Active in Proxy (24h) Active in Monetization (48h)	1000110000	1,428
07			192.168.1.1	10000	192.168.1.1	8080	Connection	Active in Proxy (24h)	1000000000	1,428
07			192.168.1.1	10000	192.168.1.1	8080	Connection	Active in Proxy (24h)	1210100000	1,428
07			192.168.1.1	47000	192.168.1.1	8080	Connection	Active in Proxy (24h) Active in Monetization (48h)	1120410000	1,428
07			192.168.1.1	11000	192.168.1.1	8080	Connection	Active in Proxy (24h)	1070000000	1,428
07			192.168.1.1	4000	192.168.1.1	8080	Connection	Active in Proxy (24h) Active in Monetization (48h)	977000000	1,428
07			192.168.1.1	10000	192.168.1.1	8080	Connection	Active in Proxy (24h) Active in Monetization (48h)	990000000	1,428
07			192.168.1.1	10000	192.168.1.1	8080	Connection	Active in Proxy (24h)	932000000	1,428
07			192.168.1.1	22000	192.168.1.1	8080	Connection	Active in Proxy (24h) Active in Monetization (48h)	932000000	1,428
07			192.168.1.1	17000	192.168.1.1	8080	Connection	Active in Proxy (24h) Active in Monetization (48h)	948700000	1,428
07			192.168.1.1	10000	192.168.1.1	8080	Connection	Active in Proxy (24h) Active in Monetization (48h)	948700000	1,428

Regular, daily large-scale residential proxy DDoS

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

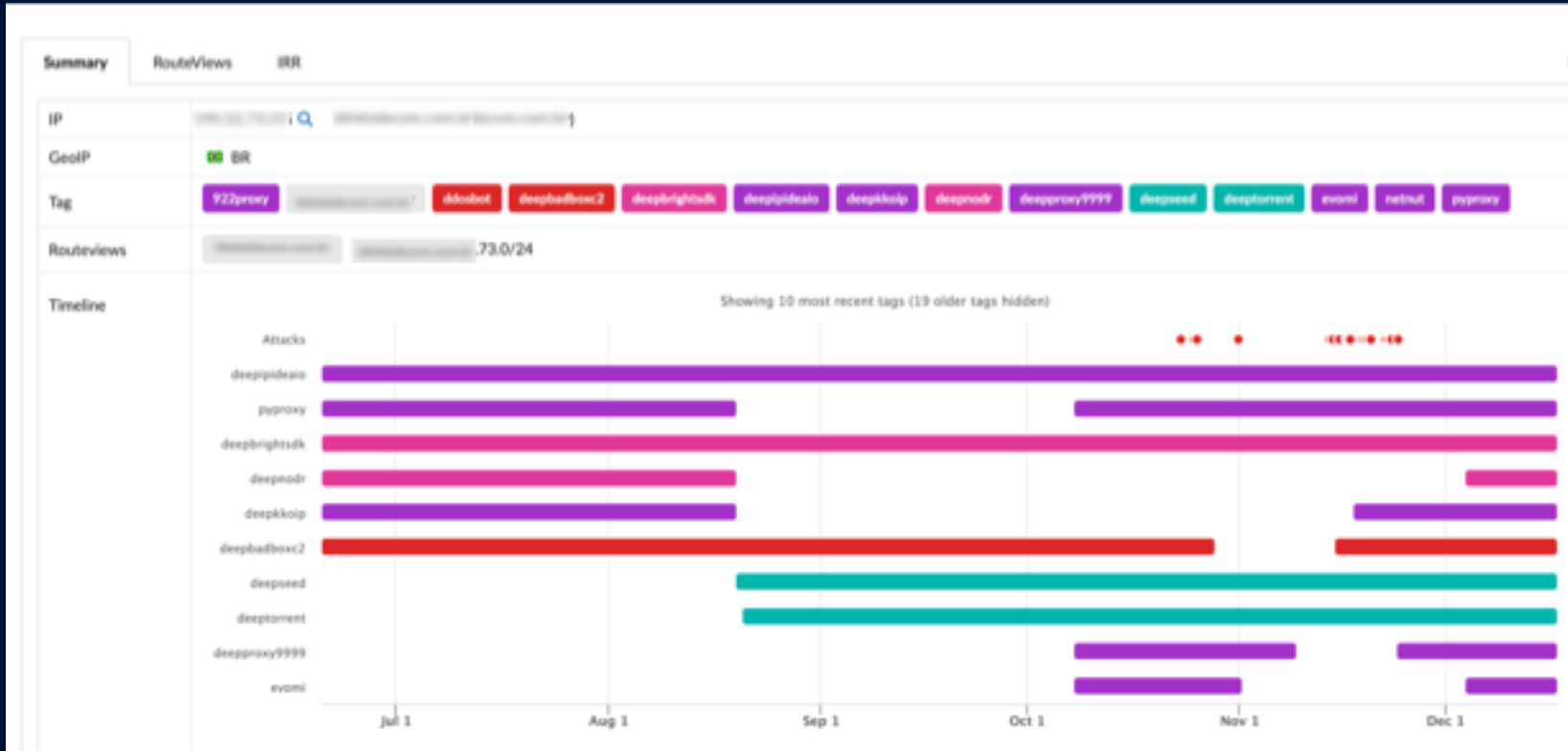
# 20+ Tbps DDoS Example

December 16, 2025





# 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 + 3<sup>rd</sup> 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



## BLACKHATWORLD

INTERNET MARKETING FORUM

**Please Read:** All New: Unlimited US Mobile Proxies at a Fraction of the Cost - 50% Off & Free Trial Available  
BetterKnow · Feb 14, 2025 26 27 28

**Please Read:** ⚠️ \$0.75/IP BartProxies.com | Virgin AT&T & T-MOBILE IPs USA | Unlimited Data | Zero Fraud Score | Many Subnets | Rotating Resi from \$1.2/GB ⚠️⚠️  
BartProxy · Jul 12, 2022 142 143 144

**Please Read:** !! ProxyWing ✅ PREMIUM RESIDENTIAL 2.5\$/GB ✅ 0 FRAUD SCORE ISP from 1,8\$/IP ✅ HIGH SPEED DATACENTER from 0.87\$/IP ✅ BHW Exclusive Code ✅ SUPPORT 24/7  
ProxyWings · Jun 6, 2025 8 9 10

**Please Read:** Selling fully anonymous private proxies - very fast activation - 24/7 support  
unr3al · Mar 6, 2010 583 584 585



Black Hat

### Boost Sneaker Bot Wins: Choosing the Right Proxy Setup

Best Proxy Choices = Faster & Safer Checkouts

#### Proxy Types

**Residential**  
Real ISP IPs  
Hard to Detect

**ISP**  
Fast + Trusted

**Datacenter**  
Fast but Easily Blocked

#### Speed & Latency

Low Latency =  
Faster Cart & Checkout

#### Rotating

New IP  
for Every  
Request

#### Rotating vs. Sticky

**Rotating**  
Same IP  
for Stable Check!

**Sticky**  
Stable  
Checkout

Smart proxy choices = Better bot success on hyped drops.

AFFmaven



Gray Hat

# Install Residential Proxy

## 30+ SDK companies and malware



YOUR GUIDE TO A BETTER FUTURE

### Pirated streaming devices are filled with malware, researchers find

Turns out there was a hidden cost to those jailbroken Fire TV Sticks offering every show for free.

**Alfred Ng**   
April 25, 2019 2:30 a.m. PT




Excellent  19,190 reviews on  Trustpilot

## Use your internet bandwidth to earn extra cash


Start earning with Honeygain just by sharing your connection – no extra effort needed. Join now and get a \$2 starting gift!

[Install & get \\$2](#)





## The only 100% FREE, 100% fast & 100% anonymous VPN in the world



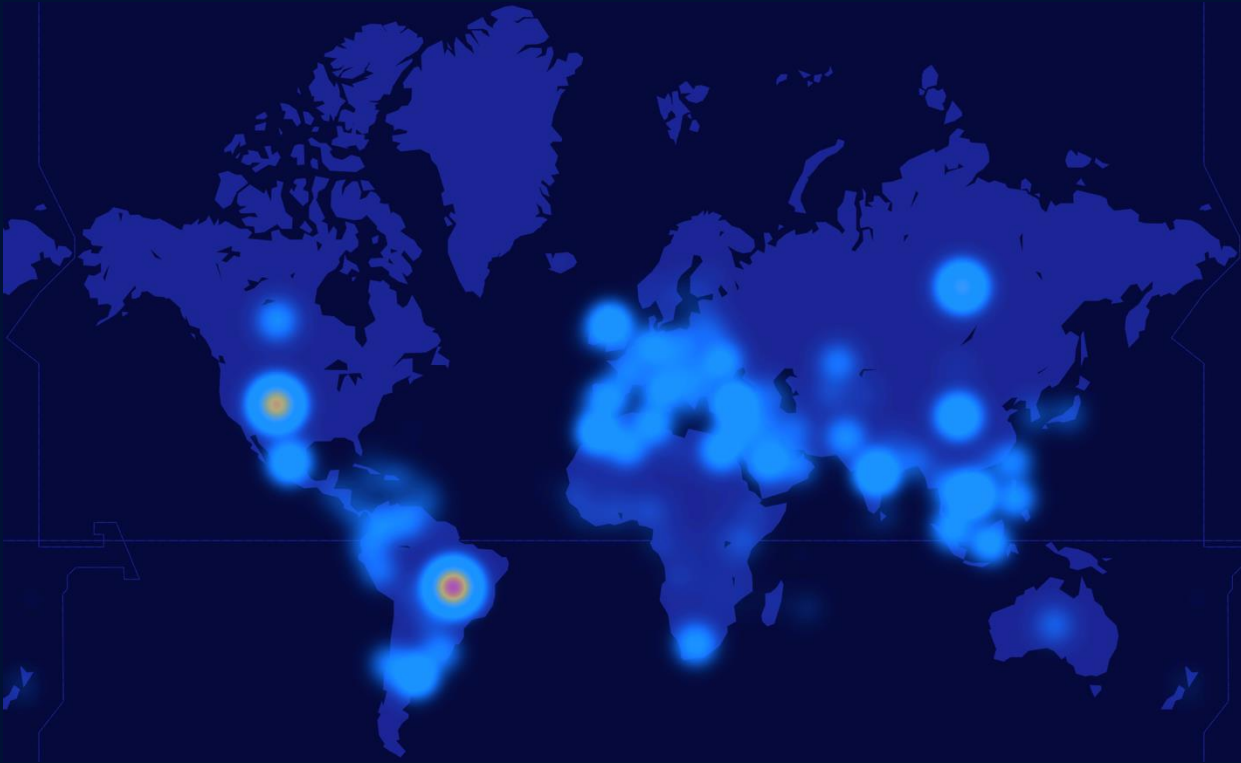
 **grass**™

Trusted by over 3.0M+ Users

## Unlimited internet plan? Rent what you don't use

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?

Cloudflare Radar

Domain Rankings Worldwide Last 7 days

Top 100 domains  
Ranked list of domain names

Updated: Oct 31, 2025

Domain name	Category
1 14emelierracwestroxburyma02132.su	CIPA Filter Anonymizer Malware
2 google.com	Search Engines
3 googleapis.com	Content Servers Information Technology
4 groksearch.net	Newly Seen Domains
5 cloudflare.com	Technology
6 gstatic.com	Content Servers
7 facebook.com	Social Networks
8 microsoft.com	Business Information Technology
9 apple.com	Information Technology Technology
10 amazonaws.com	Technology

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

# The facade of competition





# IPIDEA

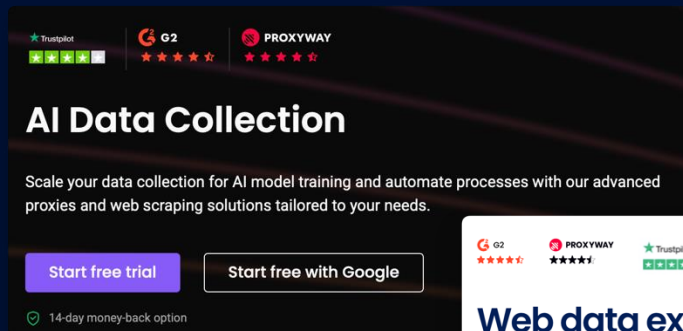
Single “mega connect” controls majority wholesale global res proxy

- 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

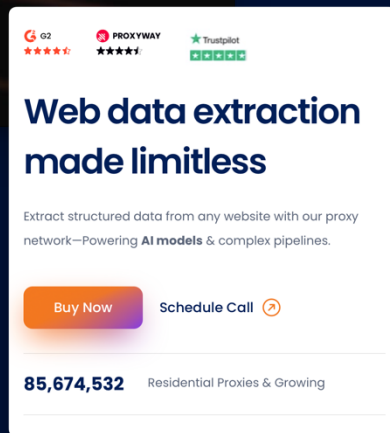
# AI needs data, criminals need revenue

Supply, meet demand

Demand side: AI training pipeline



The screenshot shows the top section of a website. At the top, there are three logos: Trustpilot with a 4.5-star rating, G2 with a 4.5-star rating, and PROXYWAY with a 4.5-star rating. Below these is the heading "AI Data Collection" in large white text. Underneath the heading is a paragraph: "Scale your data collection for AI model training and automate processes with our advanced proxies and web scraping solutions tailored to your needs." At the bottom of this section are two buttons: "Start free trial" in a purple box and "Start free with Google" in a white box with a black border. Below the buttons is a small green icon and the text "14-day money-back option".



The screenshot shows a white card with a dark header. The header contains the same three logos as the previous screenshot: G2, PROXYWAY, and Trustpilot. Below the logos is the heading "Web data extraction made limitless" in large dark blue text. Underneath the heading is a paragraph: "Extract structured data from any website with our proxy network—Powering AI models & complex pipelines." At the bottom of the card are two buttons: "Buy Now" in an orange box and "Schedule Call" in a white box with a black border and a circular arrow icon. Below the buttons is the text "85,674,532 Residential Proxies & Growing".

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



100-200x

# 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

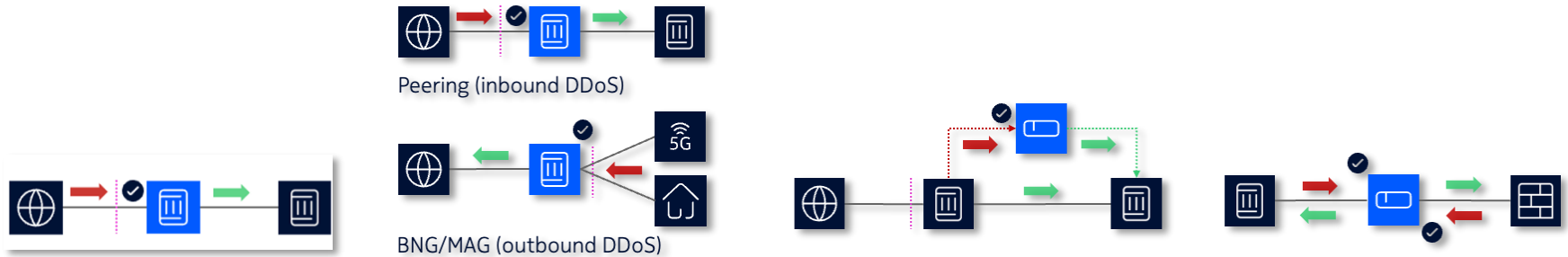
## Capability exists today

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

# 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 your 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