

# The \$30 attack box

inside the Android TV botnet ecosystem

Jérôme Meyer

Nokia Deepfield Emergency Response Team (ERT)

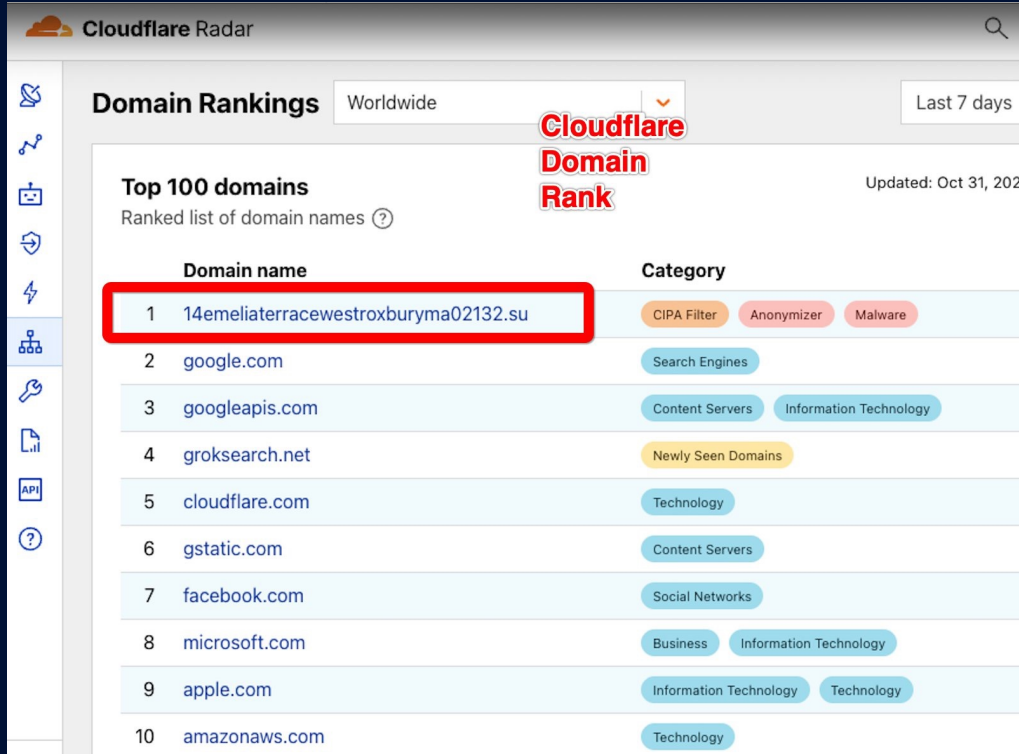
NOKIA

Ring a bell?

14emeliaterracewestroxburyma02132.su

# 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)

# The difference a year makes

## example of DDoS botnet with proxy components (May 2024)

192.168.1.100	rtsp suspicious_hex webcam ddoobot	0.09
192.168.1.101	unknown_https com.br webcam apache ddoobot tomcat	0.09
192.168.1.102	diryatsvigor webcam soomen ddoobot	0.09
192.168.1.103	ddoobot suspicious_hex	0.09
192.168.1.104	ddoobot n.com unknown_web tD6P	0.09
192.168.1.105	charter.com	0.09
192.168.1.106	ddoobot resident suspicious_hex	0.09
192.168.1.107	business m rtsp suspicious_hex webcam ddoobot	0.09
192.168.1.108	rtsp uniview webcam ddoobot residential gasp	0.09
192.168.1.109	ddoobot suspicious_hex	0.09
192.168.1.110	rtsp suspicious_hex webcam br ddoobot	0.09
192.168.1.111	localhost globalc kit talnet suspicious_hex ddoobot talink	0.08
192.168.1.112	proxymarket lpbarger webshare proxymega simplymode suspicious_hex desphonerain smartproxy saylali	0.08
192.168.1.113	ddoobot d.com suspicious_hex gasp	0.08
192.168.1.114	ddoobot suspicious_hex	0.08
192.168.1.115	deepkolo deepproxy 711proxy abcproxy suspicious_hex deepidalo	0.08
192.168.1.116	ddoobot webcam	0.08
192.168.1.117	deepidalo deepproxy5000	0.08
192.168.1.118	unknown_https nginx	0.08
192.168.1.119	genetec microsoft-httpsapi rtsp f webcam ddoobot	0.08
192.168.1.120	ddoobot suspicious_hex m	0.08

2024: **occasional** res proxy in DDoS

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

# The difference a year makes

example of DDoS primarily using res proxy (May 2025)

Proto	TCPFlag	Peer	Src IP	SPort	Dst IP	DPort	Detect	Src Genome	Bytes	Len
17				49676		3002		deepproxy8884	16605040640	1,428
17				36663		3002		proxymega, deeptorrent, deepipidials, deepproxy, deepproxy8884, plainproxies	16051539968	1,428
17				16014		3002			14022034432	1,428
17				56899		3002			12361530368	1,428
17				47839		3002		lunaproxy, deeptorrent, deepipidials, deepproxy, deepkiolp, 771noproxy, proxycake, proxymega, deepproxy8884, flyproxy	11254528000	1,428
17				9170		3002		proxymega, deepipidials, deepproxy	10701026304	1,428
17				6194		3002		deeptorrent, maximuma.net, deepproxy, subproxy, deepproxy8884	9778524160	1,428
17				31456		3002		rip, gsp, webcam, soap	9700253696	1,428
17				9816		3002			9225022464	1,428
17				22964		3002		lunaproxy, enigmaproxy, deepipidials, deepproxy, deepkiolp, 771noproxy, proxymega, flyproxy, plainproxies	9225022464	1,428
17				17877		3002		webinars, deepipidials, deepproxy, subproxy, proxycake	8487021056	1,428
17				52109		3002		deeptorrent, deepproxy, subproxy, proxymega	8487021056	1,428

2025:

**Regular, daily large-scale res proxy DDoS**

# How we got here

Residential proxies were not our problem (until they were)

## 2014-2023: "Someone else's problem"

- Fraud infrastructure (credential stuffing, ad fraud)
- Not a network threat — abuse team territory

## 2024: First network impacts

- NoName057(16) weaponizes free VPN apps for DDoS
- Residential endpoints begin appearing in attacks

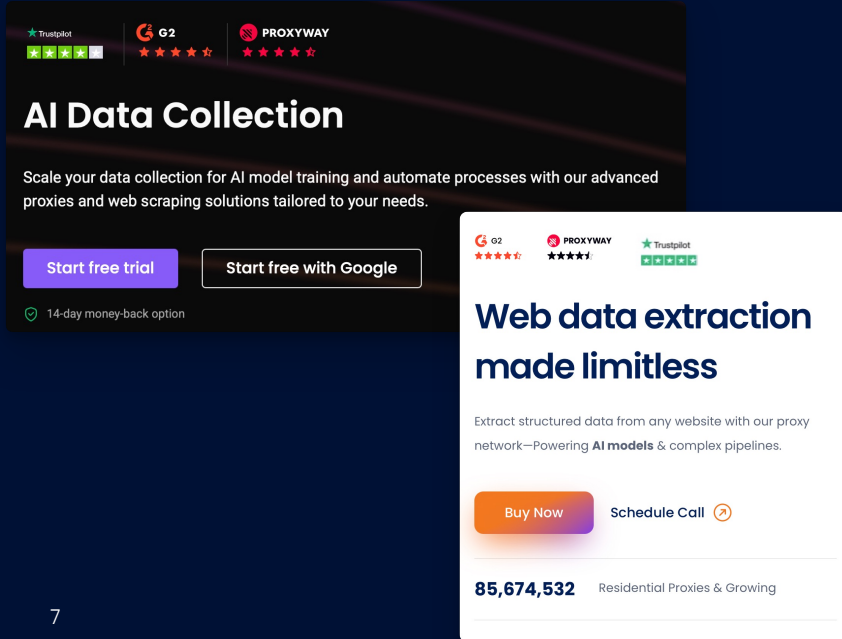
## 2025: ResHydra emerges

- We start talking about "ResHydra" (early 2025): Residential proxies weaponized as DDoS infrastructure
- Rapid botnet succession: RapperBot → Aisuru → Kimwolf
- Latent attack surface: 100-200M consumer endpoints

# AI needs data, criminals need revenue

Supply, meet demand

## Demand side: AI training pipeline



The screenshot shows the Proxyway website's 'AI Data Collection' section. At the top, there are logos for Trustpilot (5 stars), G2 (5 stars), and PROXYWAY (5 stars). The main heading is 'AI Data Collection'. Below it, a sub-heading reads: 'Scale your data collection for AI model training and automate processes with our advanced proxies and web scraping solutions tailored to your needs.' There are two buttons: 'Start free trial' and 'Start free with Google'. At the bottom left, there is a '14-day money-back option' badge. A white callout box is overlaid on the right side of the screenshot, containing the text 'Web data extraction made limitless', a description of the service, and buttons for 'Buy Now' and 'Schedule Call'. At the bottom of the callout, it says '85,674,532 Residential Proxies & Growing'.

### AI Data Collection

Scale your data collection for AI model training and automate processes with our advanced proxies and web scraping solutions tailored to your needs.

[Start free trial](#) [Start free with Google](#)

14-day money-back option

#### Web data extraction made limitless

Extract structured data from any website with our proxy network—Powering **AI models** & complex pipelines.

[Buy Now](#) [Schedule Call](#)

**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)

# 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/Kimwolf era (2025+)

- Consumer endpoints
- Android TV boxes, mobile apps
- "Free" VPN software
- Behind NAT / CGNAT
  
- Mostly only outbound
- **100-200M** exploitable surface



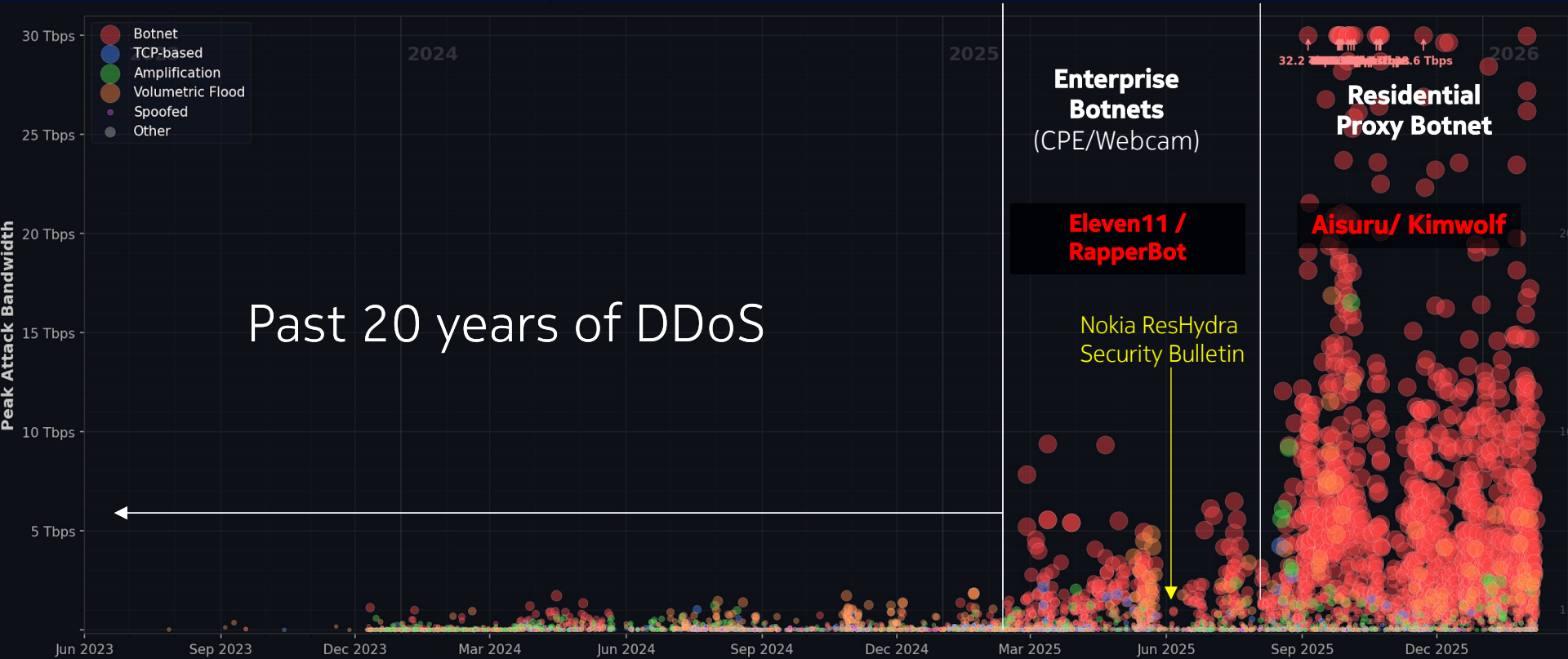
100-200x

# Kimwolf / Aisuru



Sample of attacks over last 12 months. Each circle represents individual attack with color (e.g. red == botnet) mapping to attack type and size of circle correlates to duration. DDoS transition from enterprise botnet to Resproxy August 2025

# Kimwolf / Aisuru



Sample of attacks over last 12 months. Each circle represents individual attack with color (e.g. red == botnet) mapping to attack type and size of circle correlates to duration. DDoS transition from enterprise botnet to Resprox August 2025

# 2025: the year everything scaled

## RapperBot

- Early 2025
- 30-50k bots

Single largest DDoS botnet we tracked (then)

## Aisuru

- Mid-2025
- 300-500k bots

Absorbed RapperBot nodes post LE take-down

## Kimwolf

- Late 2025
- ~3M active at peak
- 100-200M latent capacity (ResHydra: res proxies weaponized for volumetric DDoS)

Overtaking Aisuru in observed attack volume

# Kimwolf

The big one

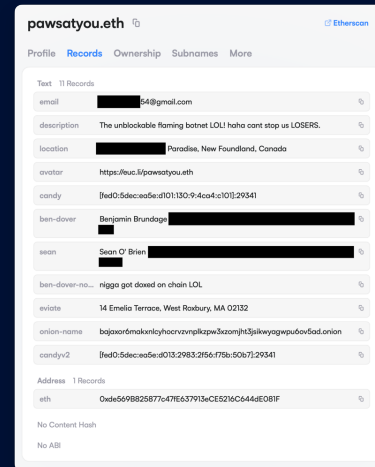
Emerged in late 2025

## What we know

- Apparent operator overlap with Aisuru
- Larger volumetric DDoS capability
- C2 include **re6ce[.]eth** (ENS)
- ~3M bots active for DDoS
- November 2025: Overtaking Aisuru in observed volume
- LE action on 19 March — disruption ongoing

## Latent capacity

- Current DDoS usage: ~3M active bots
- 100-200M endpoints potentially available (ResHydra)



# Kimwolf

The **0.0.0.0** trick: When the proxy SDK routes traffic to itself

## Attacker

purchases  
IPIDEA proxy



## Proxy

routes to  
**xd.resi[.]to**



**0.0.0.0**

Resolves to  
device itself



**ADB:5555**

Unauthenticated  
shell

- Attacker doesn't need to scan the internet
- Proxy SDK routes request to device's own loopback
- Device "scans itself" for open ADB
- Attacker gets shell access
- Device joins botnet and becomes proxy node

<https://synthient.com/blog/a-broken-system-fueling-botnets>

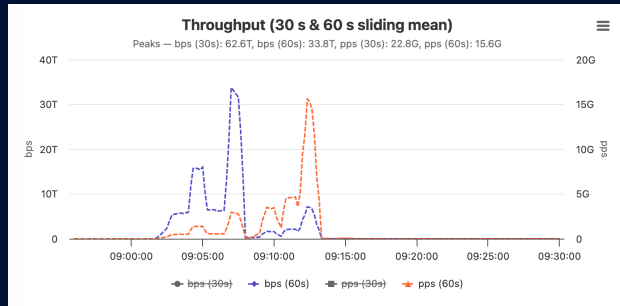
# Attack capabilities

Real devices, real IPs, real problem

- **February:** 6.5 Tbps (Nokia Deepfield)
- **April:** 4.8 Gpps (Cloudflare)
- **September:**
  - 11.5 Tbps (Cloudflare / XLab)
  - 22 Tbps (Cloudflare)
- **October:** 33 Tbps (Nokia Deepfield)

## Attack vectors

- UDP floods (500-700 byte packets, randomized ports)
- TCP floods with randomized flags
- GRE floods
- HTTP(s) via res proxy module



Virtually no IP address spoofing: real devices, real IPs

# Attack capabilities

Real devices, real IPs, real problem

```
botmon L7 attack summary (60m) - kimwolf
• login.live.com (AS8075/microsoft.com/US) | HTTP | 34900 reqs (password, email)
  └─ [REDACTED]
  └─ [REDACTED]
• i.instagram.com (AS32934/facebook.com/NL) | HTTP | 1 reqs (account_enum)
  └─ [REDACTED]
Total: 34901 requests to 2 hosts
```

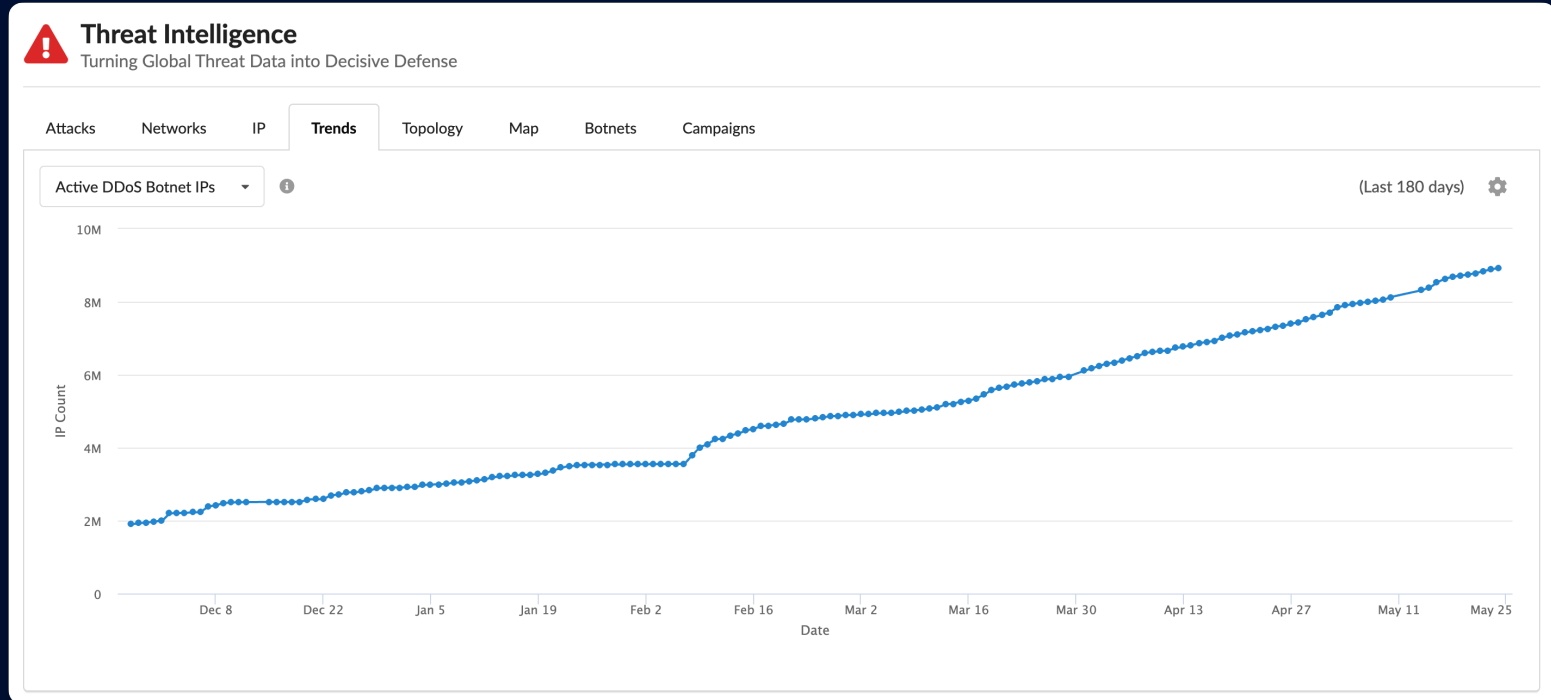
```
botmon L3/L4 attack alert - kimwolf
• 66.165.249.74 (AS29802/hivelocity.net/US) | UDP/:2589 | 540B (fixed) | 1.1M pps
  (5580.6 Mbps)
  └─ 72.6M pkts / 42.2 GB over 65s
```

- L7 credential stuffing + account enumeration attacks (sinkholed) from recent Kimwolf payload (2026-02-05)

- UDP flood from recent Kimwolf payload (2026-02-05)

# Daily Active DDoS Botnet Endpoints

Up from 1M to 8M over last 12 months



Data from Deepfield Secure Genome

Your network is the weapon  
(and sometimes, the target)

## **Outbound impact**

- Attack traffic from your users overwhelms your infra
- CGNAT device failures observed under attack load; congested peering links in several networks
- Non-infected subscribers experience collateral outages

# Six families, one attack surface, three months

Pulling the thread from Kimwolf revealed an ecosystem

## The thread

- We analyzed Kimwolf in late 2025 — 3M active bots, ENS-based C2
- Shared cryptographic fingerprint (RC4+LCG, seed **0xe0a4cbd6**) linked it to Aisuru and Jackskid
- Identical port pools, signing certificates, and co-located infrastructure confirmed: one operation, multiple codebases

## The land rush

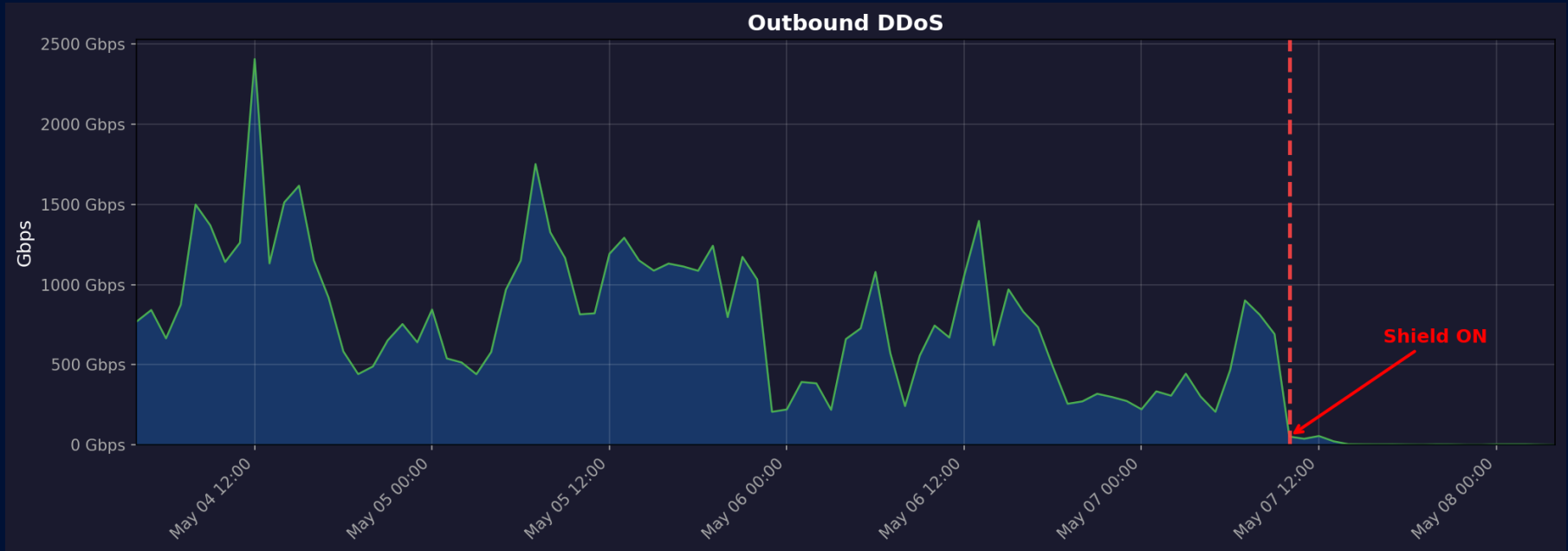
Once ADB-via-proxy proved viable, independent operators piled on:

- **Katana** (Mar): On-device rootkit compiled via TinyCC
- **CECbot** (Mar 20): First malware to weaponize HDMI-CEC — TV appears off, bot keeps running
- **Drifter** (Mar 28): Independent codebase, 2.6 Tbps from 80K sources, masquerades as CCTV management traffic

All published at  
<https://github.com/deepfield/public-research>

# Security is about automation

Shield router ACLs blocking Tbps of DDoS from compromised subscribers



Data from Nokia LATAM customer enabling Nokia Shield for first time May 7, 2026

# Summary & close

## 1. These devices are **already on your network**

Budget Android TV boxes in subscribers' homes, mobile apps with embedded proxy SDKs — they arrive compromised, no user error required

## 2. **Look for C2**, not just attack traffic

ENS queries from residential subnets, DNS to .su/.st/OpenNIC TLDs, outbound traffic on non-standard port pools — these are the signals that precede attacks

## 3. **Disruption at the edge** works

Blocking C2 communication stops both the DDoS commands and the proxy revenue — one policy, two threats neutralized

NOKIA