NEW RESEARCH

Catch Me If You Can

New Research Reveals CanOworms

Inside the Anonymization-for-Hire Network

Wade Lance
VP, Field CISO

Gilad Friedenreich Maizles | SecurityScorecard STRIKE | August 2026

SecurityScorecard

On the Author

Find me at

Gilad Friedenreich Maizles

ROLE & PASSION

Security researcher, analyst and cyber enthusiast.

RESEARCH FOCUS

Main focus on state sponsored APTs and campaigns, as well as threat actor behavioral profiling and analysis.

KEY PUBLICATIONS

Researcher and author behind STRIKE's recent publications on the LapDogs ORB and Operation WrtHug.

CURRENT INITIATIVE

Currently leading SecurityScorecard STRIKE's research team.

It Started with One Detail

Most investigations begin with a detail that doesn't add up.

THE LEAD

A post flagged an APT41-linked Cobalt Strike team server reached by an XWorm sample.

THE ANOMALY

On its own, unremarkable. But the host presented a self-signed, deliberately malformed TLS certificate that wasn't unique to it.

THE THREAT

We asked: how many other hosts presented this exact certificate? The answer was not a few. It was hundreds.

The Lazy String

CN=*

O=kickass

L=Bar

ST=Foo

C=WS

A value typed once into a cert-generation script, then deployed across an entire fleet.

Anonymity for Rent

Threat actors no longer build their entire infrastructure from scratch; they rent it.

We've identified **CanOworms**, a commercial "anonymity for rent" service consisting of **633 rented VPN/proxy servers across at least a dozen countries.**

Criminals lease this infrastructure the same way a business rents a commercial VPN. This design defeats traditional defenses: IP blocklists, geography filters, and hosting reputation all fail against infrastructure built to absorb takedowns.

Geographic Distribution

The Commercial Architecture

CanOworms: anonymization laundered at every layer

TENANTS · who rents concealment

Commodity RATs (Remcos, Quasar, NanoCore, NetWire, AsyncRAT, Loki), plus peer-claimed APTs as tenants (low confidence).

↓

CanOworms RELAY FLEET · ~633 nodes / dense /24s

Squid, SOCKS, OpenVPN, IPsec. One shared self-signed 'kickass' certificate (plus nVpn) binds the fleet.

↓

RESELLER / PROCUREMENT · the branded middle

PrivacyFirst, Zero Logs VPN, Freemesh, El Ghoubrashi Net. AS214366, sponsored by MAXKO d.o.o.

↓

LANDLORD ASNs · the ground it stands on

Fink Telecom, Datasource AG, FBW, w1n, Amanah, Beltelecom, Rostelecom. Space leased across 6+ providers.

CONTROL PLANE

Czech hosts on borrowed / compromised boxes; laundered.

OPERATOR

Unattributed; every pivot lands on an innocent host.

Tracking the Un-Trackable

One Lazy String

The CN=*, O=kickass issuer string led us in, but an issuer string alone is trivial to fake. In fact, 748 IPs carried the string, but 115 look-alikes failed our combo test and were excluded.

The true membership signal is the **shared per-/24 certificate thumbprint** (the reused private key).

Three Signals

Membership requires three independent signals to agree across the host:

- **Shared Certificate Thumbprint** (per-/24 private key reuse)
- **Fleet JARM**: 21d10d000...e61583b...
- **Fleet JA4X:** 2bab15409345...

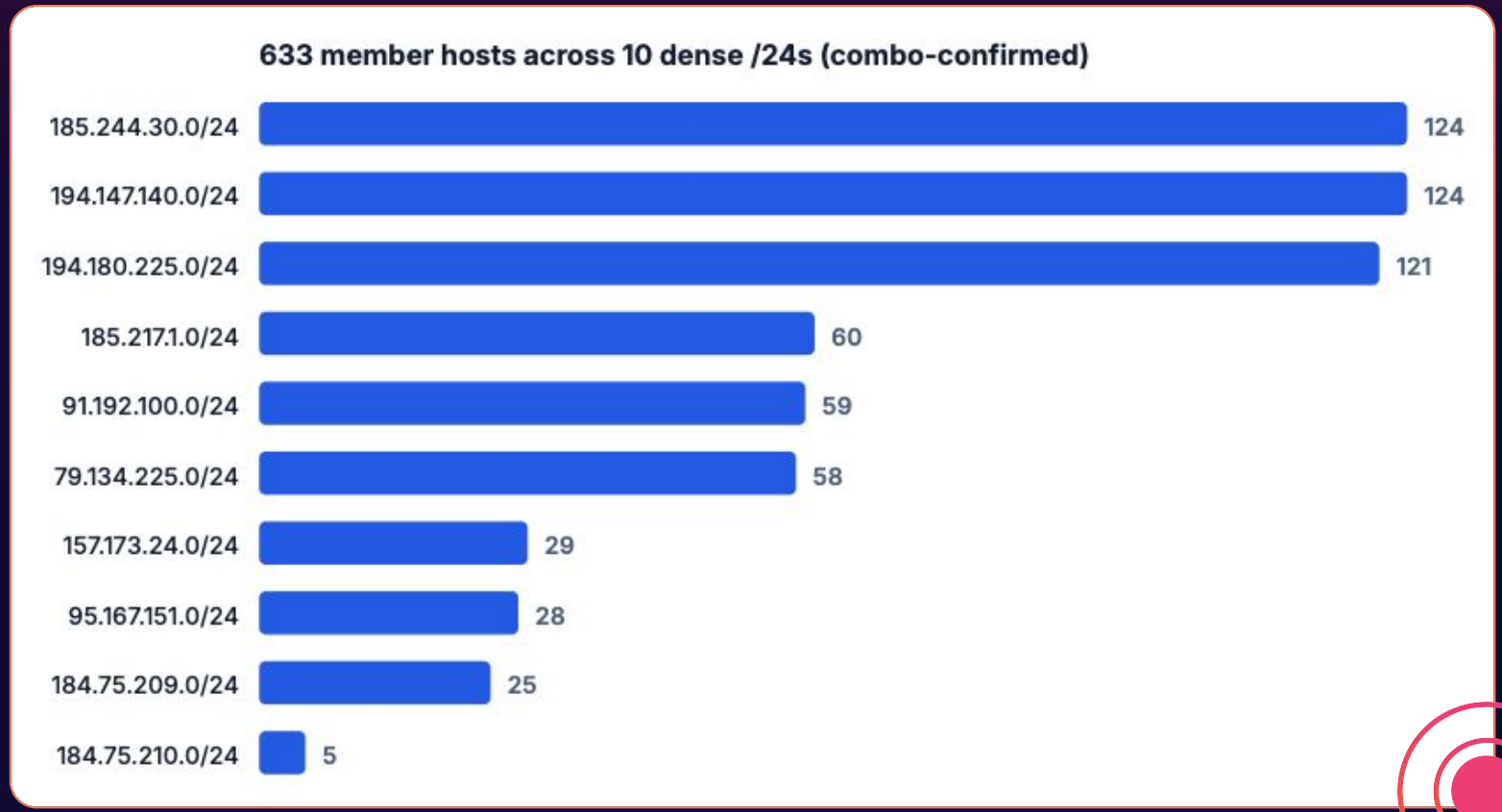
This confirmed 633 member nodes.

The Size of the Fleet

180-Day Snapshot: This is a living membrane of proxies, not a static list of IPs. Nodes rotate in and out of service.

The network is concentrated in densely-populated /24 address blocks.

Durability Caveat: Fingerprints are durable relative to IP churn, not permanent. A re-image shifts JARM/JA4X, making the reused private key (thumbprint) the sturdier anchor.



Front, Not C2: The Proxies

MODERATE CONFIDENCE ASSESSMENT

Hosts tagged by threat feeds as C2s act as "bouncers" for hidden backends.

Uniform Stack

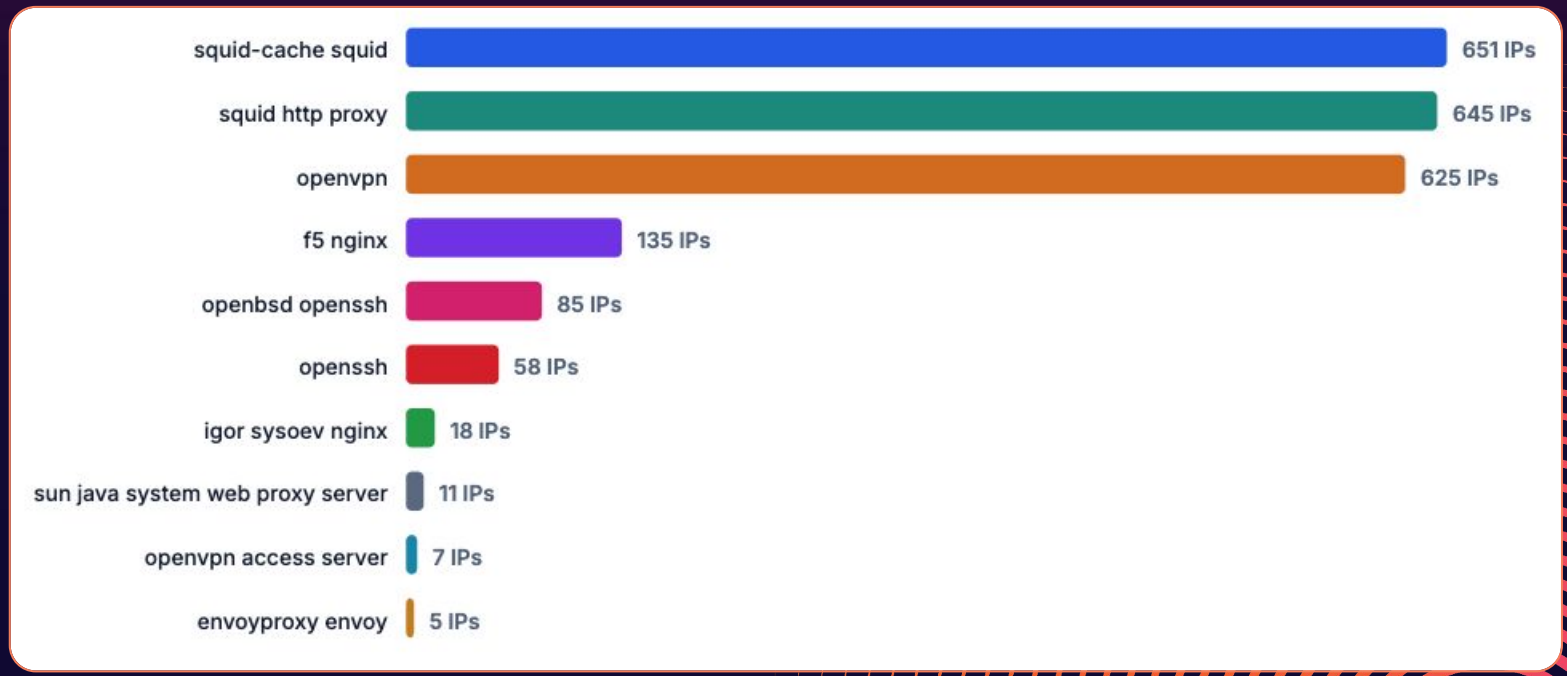
Nodes run Squid, SOCKS, OpenVPN, and IPsec wrapped in one TLS termination layer. They are manufactured relays.

Reputation Paradox

We found hosts deemed reputationally "clean" by AV engines relaying numerous distinct malware samples simultaneously.

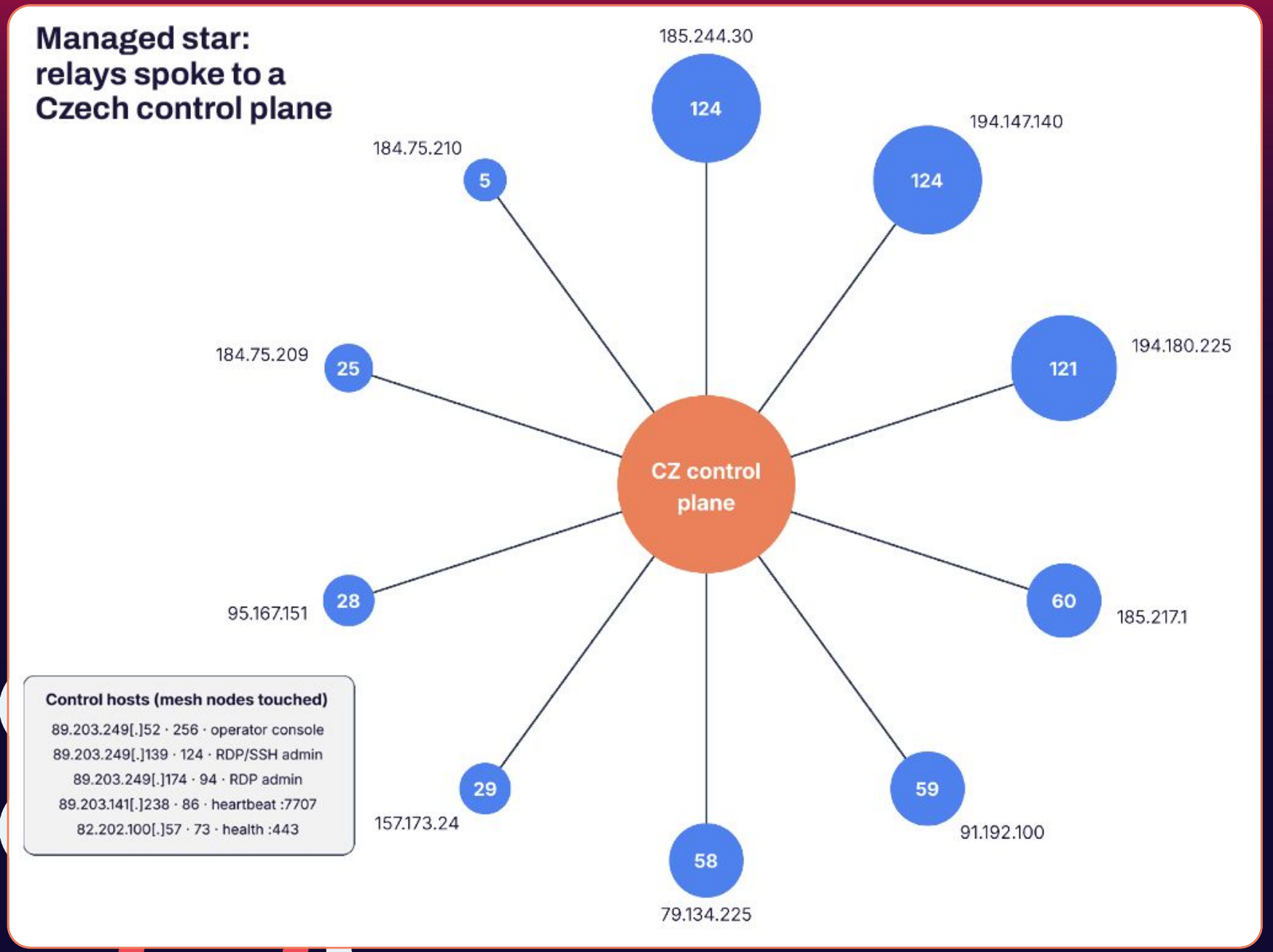
The C2-Shaped Hole

No mesh IP labelled as a C2 returned scan data matching known configs of the malware named against it.



*Caveat: Netflow is pivoted on the mesh. We see traffic go through, but cannot stitch sessions end-to-end. A subset may genuinely terminate C2.

A Centralized, Managed Network



Who is Renting?

LOW CONFIDENCE FOR APTS

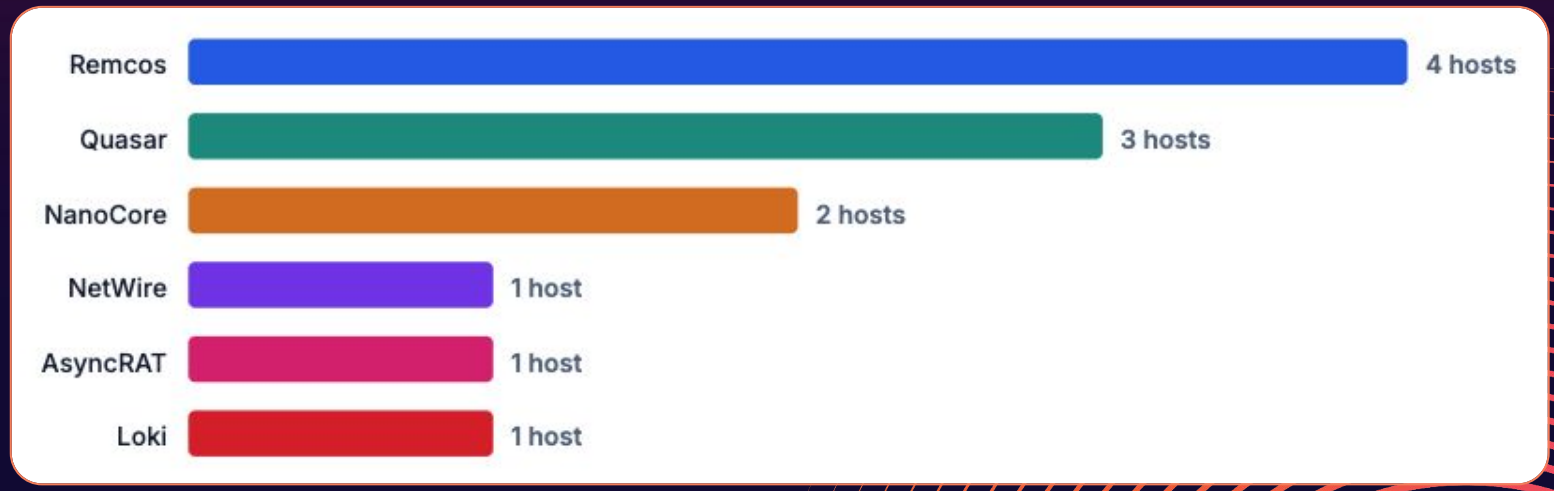
Because multiple unrelated state and criminal actors converge on the same space, single-actor attribution is a trap.

Commodity RATs

Remcos, Quasar, NanoCore, NetWire, AsyncRAT, and Loki dominate the clientele.

State Nexus

Partner reporting places suspected China-nexus (Silver Dragon) and DPRK-nexus actors here, but *only at low confidence, and as tenants among many, not owners.*



Evidence Grading Rubric (High Confidence)

Feed label + Netflow observation + VirusTotal overlap within the certificate membership window.

e.g., 91.192.100[.]36:8084 (Quasar) = Feed + 14 flows + in-window samples.

Commodity-Crime Geography, on Both Ends

The geographical layout of the network undercuts the "elite espionage platform" narrative.

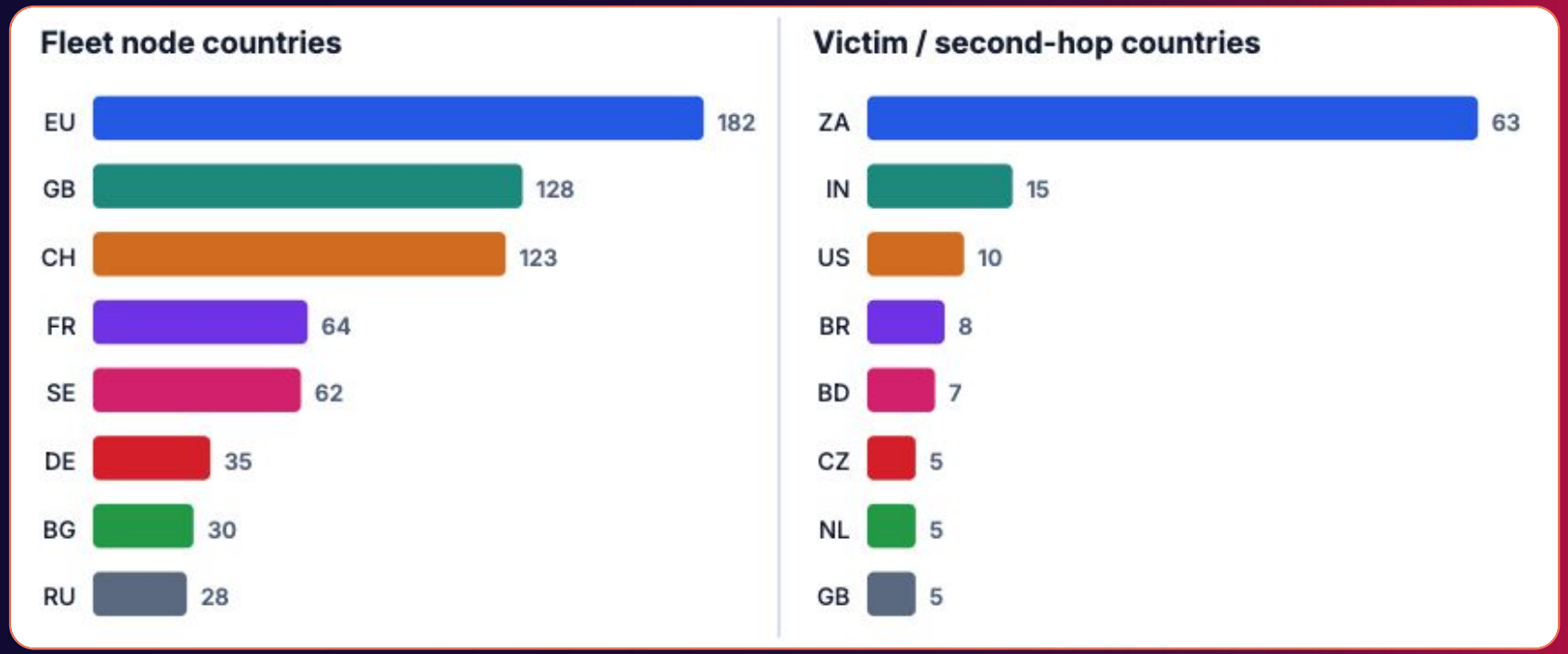
Node Registrations

Cluster heavily in European ranges (EU-registered space, GB, CH, FR, SE).

Victims

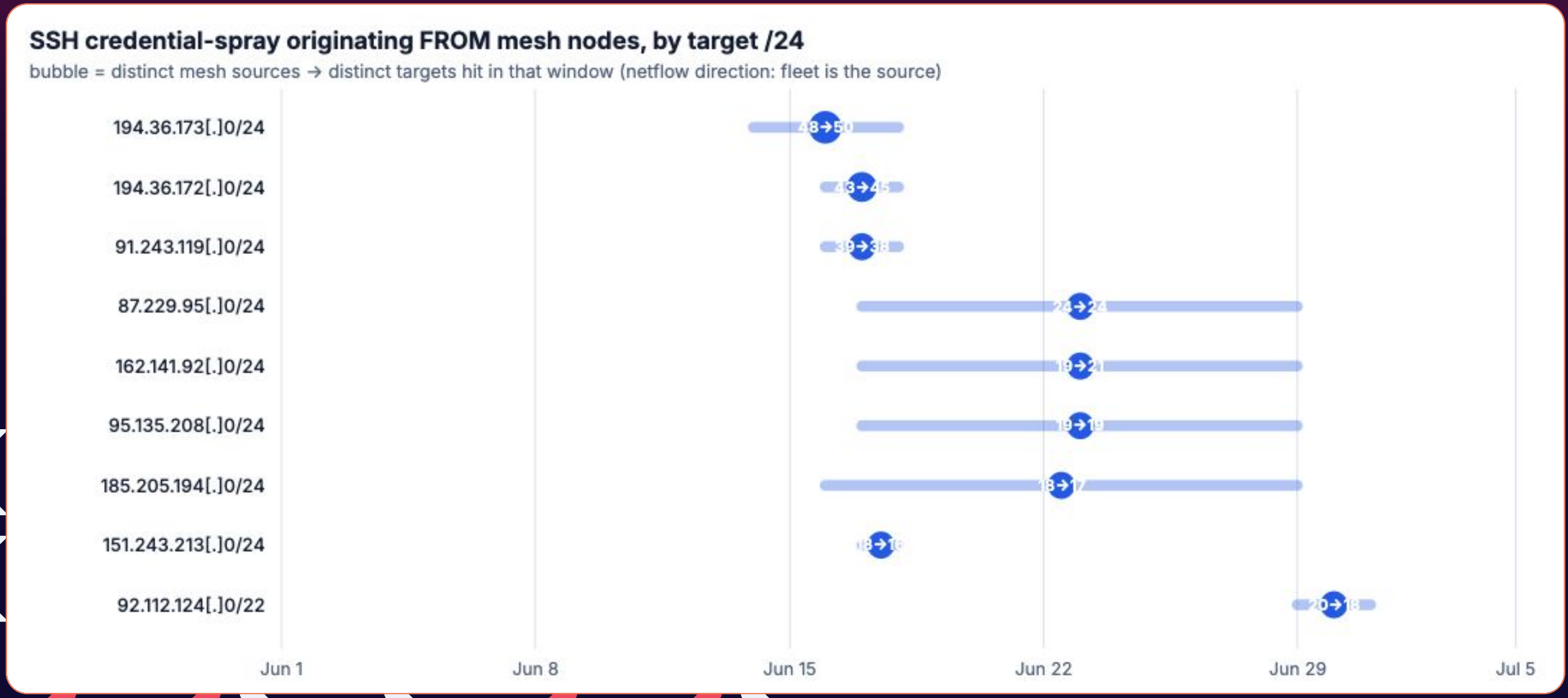
Concentrated in South Africa, Bangladesh, India, Pakistan, and Brazil.

This represents typical commodity botnet victims and proxy customers, not European or East-Asian government espionage targets.



Attack-Shaped Traffic Exits the Fleet

UNRESOLVED ATTRIBUTION

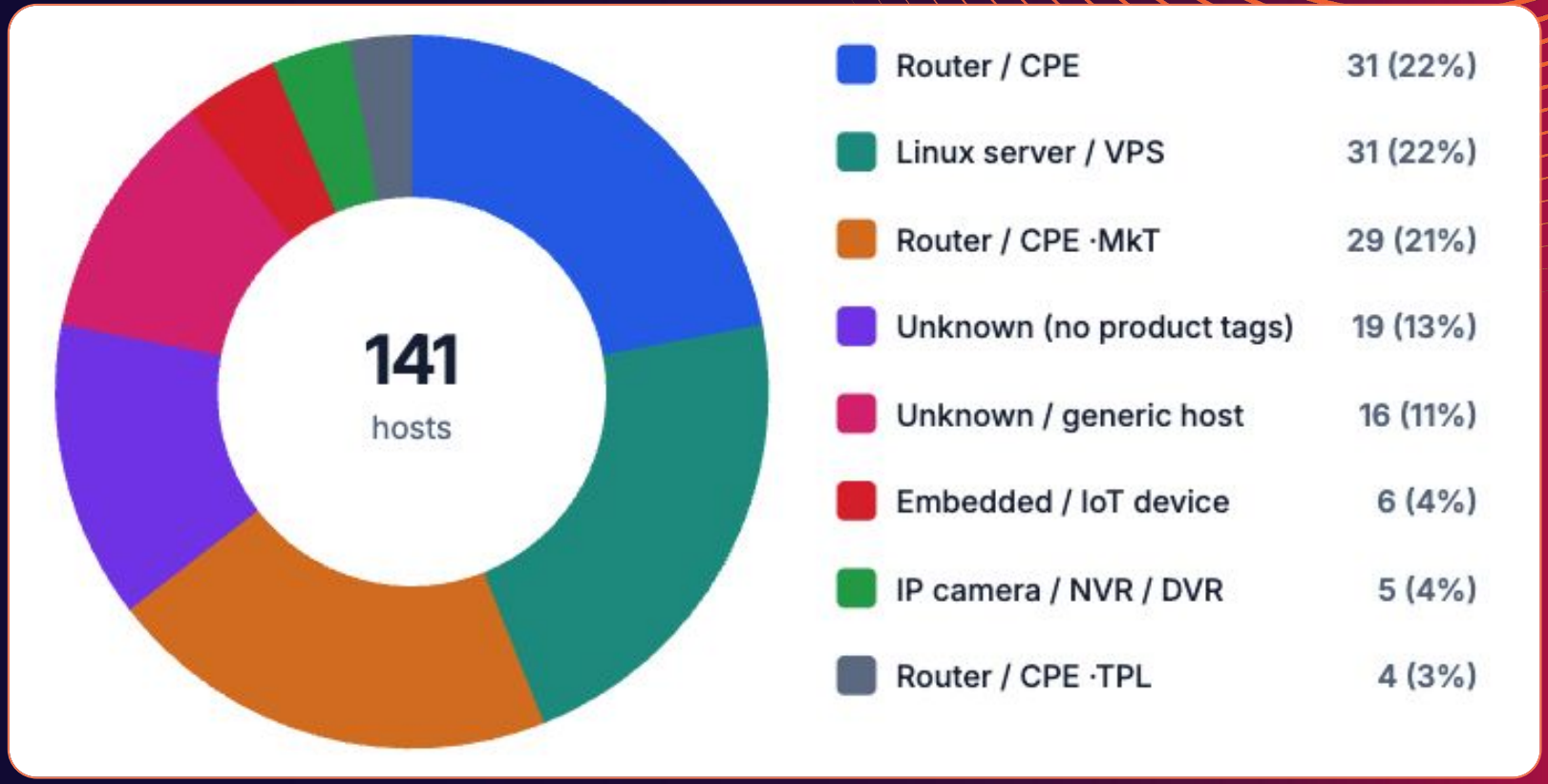


What the Fleet Reaches Out To

When the fleet reaches outward, what is it looking for?
Context: ~41% of targets sit in South Africa across ~154 second-hop hosts.

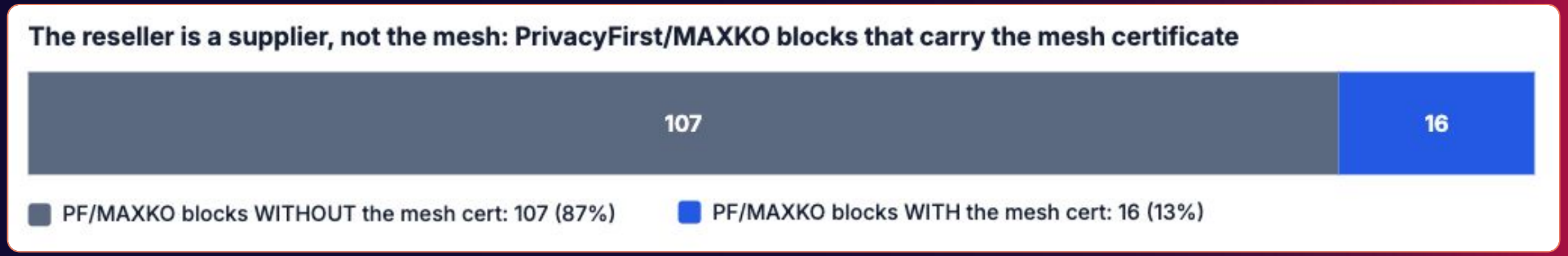
Three hypotheses for this targeting (Unresolved):

1. **Recruitment:** The operator compromising edge devices to grow relay capacity.
2. **Victimization:** Ordinary botnet victimization.
3. **Tenant Scanning:** A tenant's scanner running out through the proxy *(most economical reading).*



Procurement vs. Operation

Registration data reveals resellers and suppliers, not operators. PrivacyFirst/MAXKO is the reseller. Fink Telecom, Datasource, FBW, etc., are the suppliers (landlords).



Gray-Market IPv4

Leased dormant Iranian blocks, protecting the core operation from takedowns.

"No Logs" Fronts

Seychelles abuse shell, pre-declaring abuse requests will fail.

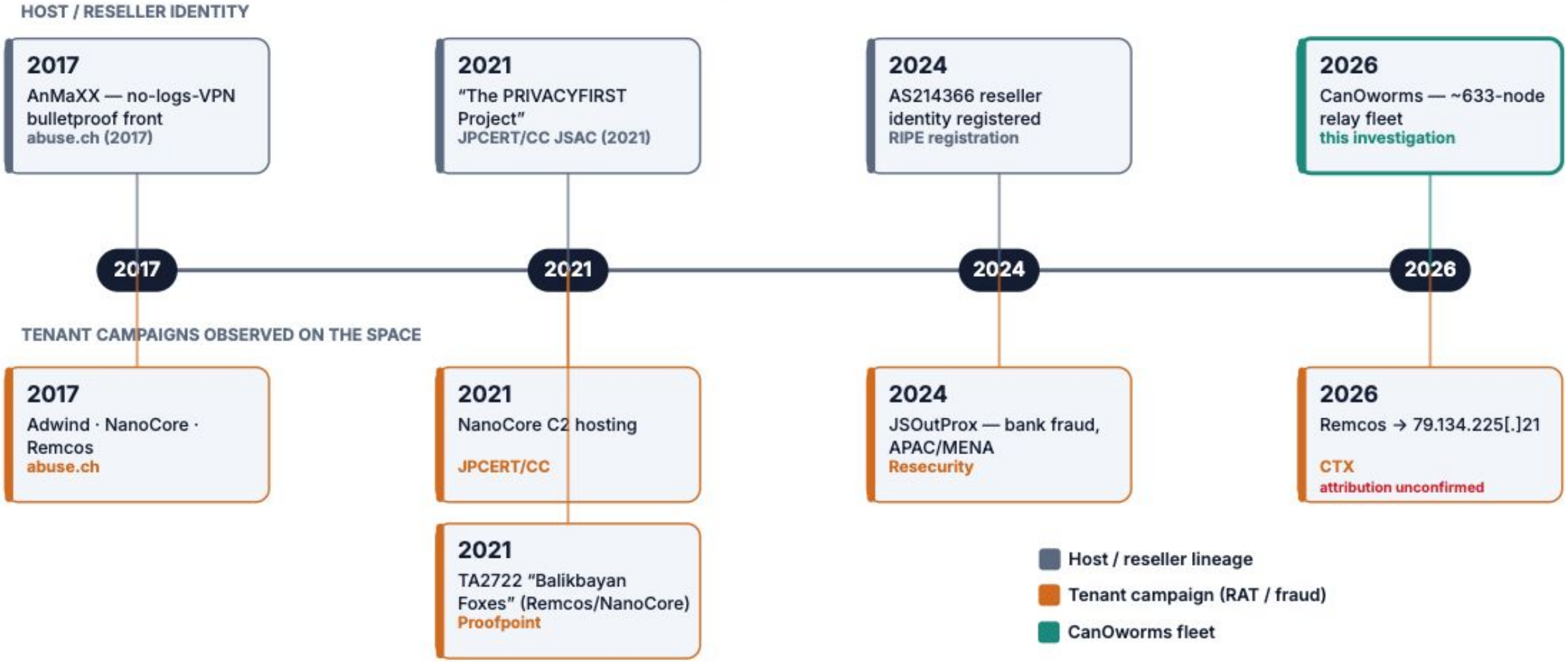
Resilient Transit

Multi-homed transit through European DDoS-mitigation networks.

A Decade of Operations

A durable, multi-tenant operation, 2017–2026

One host / reseller identity persists while a rotating cast of tenants rents the space — co-tenancy is not itself proof of CanOworms brokerage (see §10).



Implications for Defenders

Stop trusting reputations. IP reputation, geolocation blocks, and ASN denylists are exactly what CanOworms is engineered to defeat.

1. Fingerprints Survive Churn

Focus detection on build fingerprints: the shared per-/24 certificate thumbprints, the JARM, and the JA4X hashes.

**Caveat: JARM/JA4X follow software builds and will shift on re-image. Re-derive trackers periodically. Treat IP lists as aging snapshots. (See Appendix A)*

2. The Pressure Point

The control plane is a pressure point, but not a permanent chokepoint.

The collectors are cheap, rented, and movable in minutes. Blocking them disrupts tasking and raises cost, but expect the heartbeat to simply re-home.

Conclusion

Keep the operator, the reseller, and the client in three separate boxes — and refuse to collapse them.

Attribution frameworks built around a single owner per network will misread infrastructure of this kind.

STRIKE

Questions?

Contact the SecurityScorecard
STRIKE Threat Intelligence Team

wade.lance@securityscorecard.io

READ THE FULL REPORT HERE

SecurityScorecard