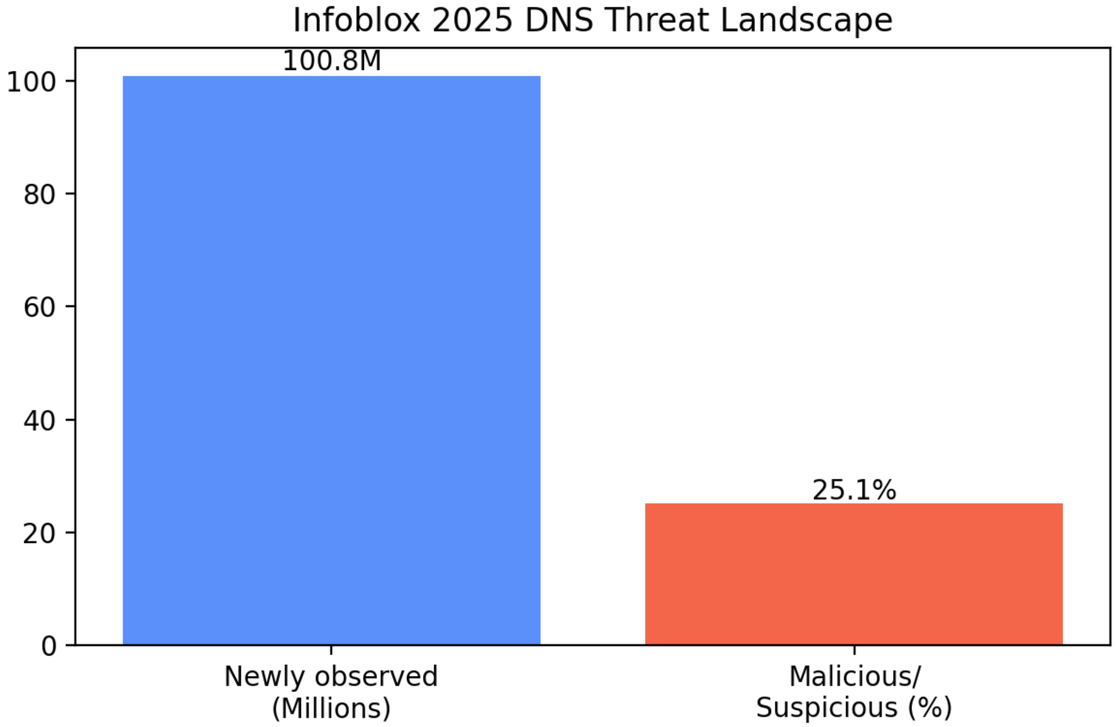
ICANN OCTO ISPCP/SSAC: Emerging DNS Abuse Trends and Mitigation Strategies

- Key Trends & Regulatory Signals

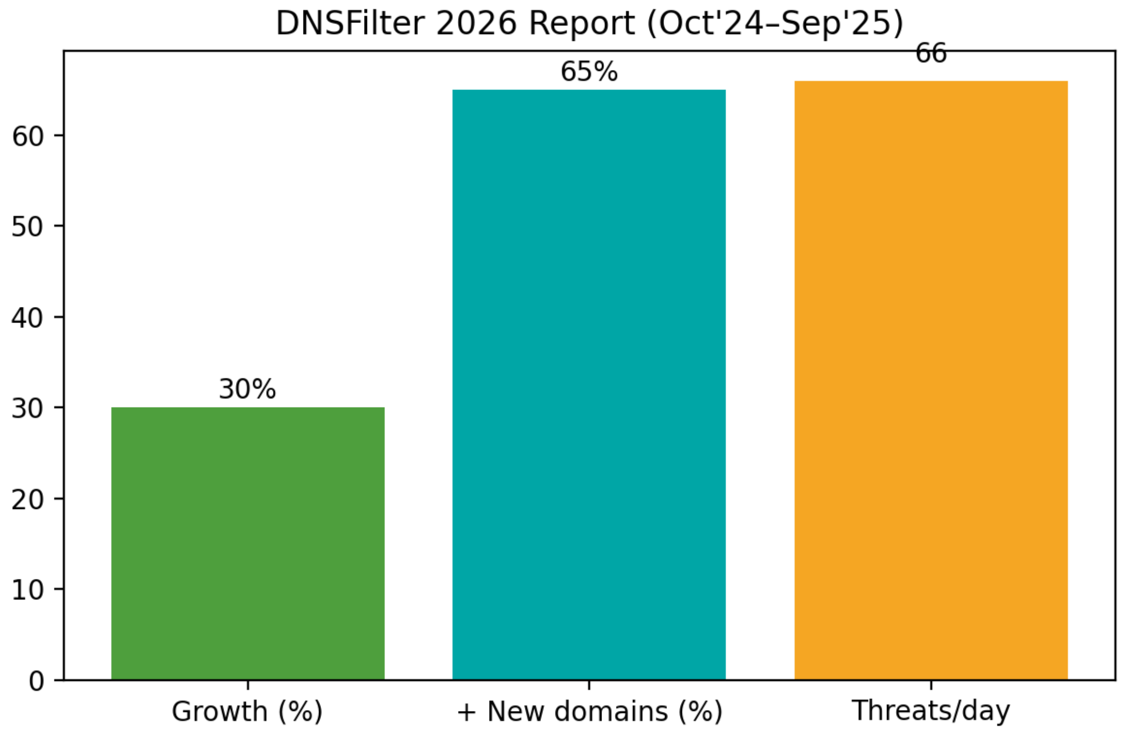
Explosion of New Domains Driving Abuse

- 100.8M newly observed domains (2025)
- ~25% malicious or suspicious
- High churn defeats legacy blocklists



Threat Velocity Is Accelerating

- ~30% YoY growth in DNS threats
- >65% of threat domains are brand-new
- ~66 threats per user per day blocked



Phishing Is Sustained, Not Seasonal

- Q2 peak >1.13M incidents
- High baseline persists in Q1 and Q3
- Phishing is now continuous infrastructure abuse

Phishing trends in 2025

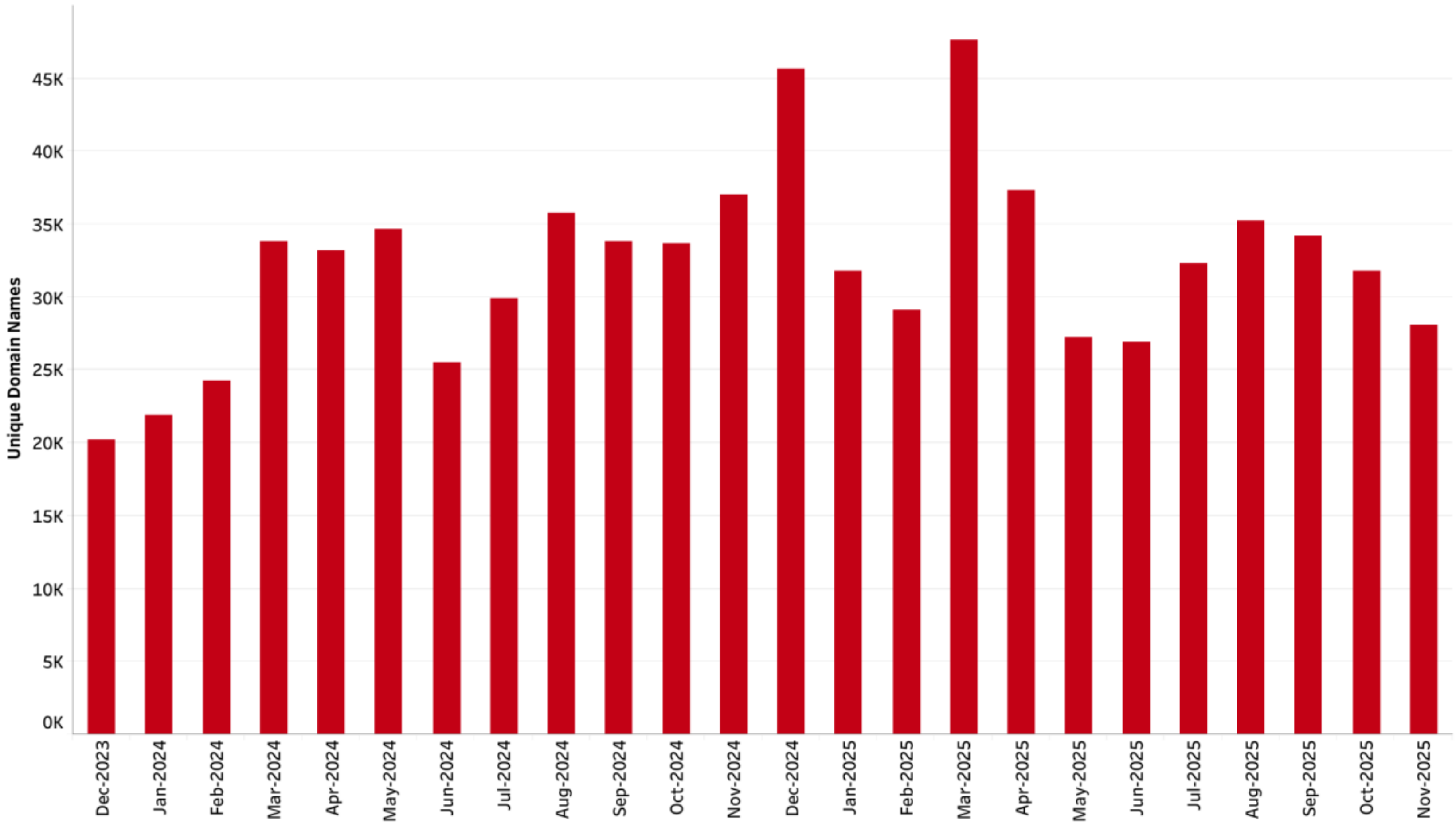


*Figure 2: Aggregate Trends - **Phishing***

Rising Botnet Command & Control Activity

- +26% growth H1 2025
- +24% growth H2 2025
- RATs ~42% of top malware families

How Attacks Begin

Phishing ~60%

Vulnerability exploitation ~21%

Other vectors are significantly smaller

UK Online Safety Act — 2025 Milestones

Illegal-content duties live (Mar 2025)

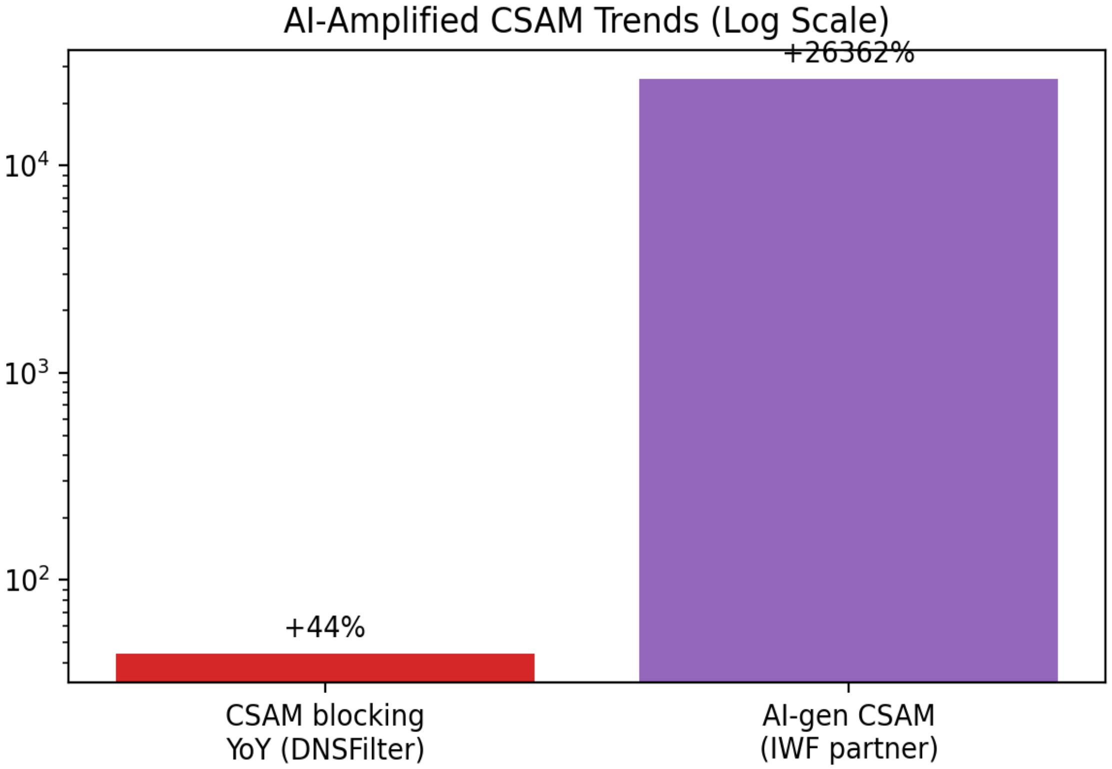
Child-safety & age verification live (Jul 2025)

Ofcom* enforcement underway

*Since **2025**, Ofcom has become the **online safety regulator** under the **UK Online Safety Act**. This significantly expanded its authority.

CSAM & AI-Generated Abuse Escalation

- +44% YoY DNS-level CSAM blocks
- +26,362% AI-generated CSAM video growth
- AI has slashed cost of harm creation



Mitigation Methodology Trends

Evidence-First Abuse Handling

- Threats reports as allegations until validated
- Automated evidence collection and validation
- Defensible, auditable mitigation
- Aligned with ICANN guidance
  - – Why it matters: Enables defensible decisions at scale

Rapid DNS Abuse Detection

- Registrars combine internal analytics with external threat feeds
- ML-enhanced detection
- From purely reactive to proactively preventive
  - Why it matters: Some threats are neutralized before impact

Tiered Evidence Classification

- Formal Tier 1–5 model
- Tier 1 enables frictionless action
- Lower tiers routed for review
- Full audit trail
  - – Why it matters: Balances speed and accuracy

Evidence-Governed Automation

- Automation-first architecture
- Tier-1 cases fully automated
- Lower tiers documented automatically
- Compliance-ready logs
  - – Why it matters: Seconds, not days

Campaign-Level Intelligence (Pivot)

- Correlates domains into campaigns
- Uses zone, RDAP, infra signals
- Detects trends beyond reputation
- Proactive defense
  - – Why it matters: Stops whack-a-mole mitigation

Hydrated Abuse Reports

- Automatic enrichment
- Technical fingerprints
- Infrastructure footprints
- Persistent evidence
  - – Why it matters: Better decisions and escalation

Sinkhole-Backed Intelligence

- Large-scale sinkholing
- Removes harm
- Captures live traffic
- Feeds intelligence
  - Why it matters: Mitigation becomes insight

What's Next?

- Partnership in cross stack abuse mitigation
  - Internet Infrastructure Forum (IIF) spearheaded by gTLD Registries and Registrars
- Working together to form policies to address online harms via operative initiatives
- More community and end user education

Sources

- Infoblox (2025); DNSFilter (2026); Spamhaus (2025); APWG (2025);
- ENISA Threat Landscape (2025); ICANN DNS Abuse Dashboards;
- EU DSA Transparency Database; Ofcom OSA (2025); UN, UNICEF, UN Women
- Netbeacon 2025 MAP Report
- CleanDNS 2025 Roadmap