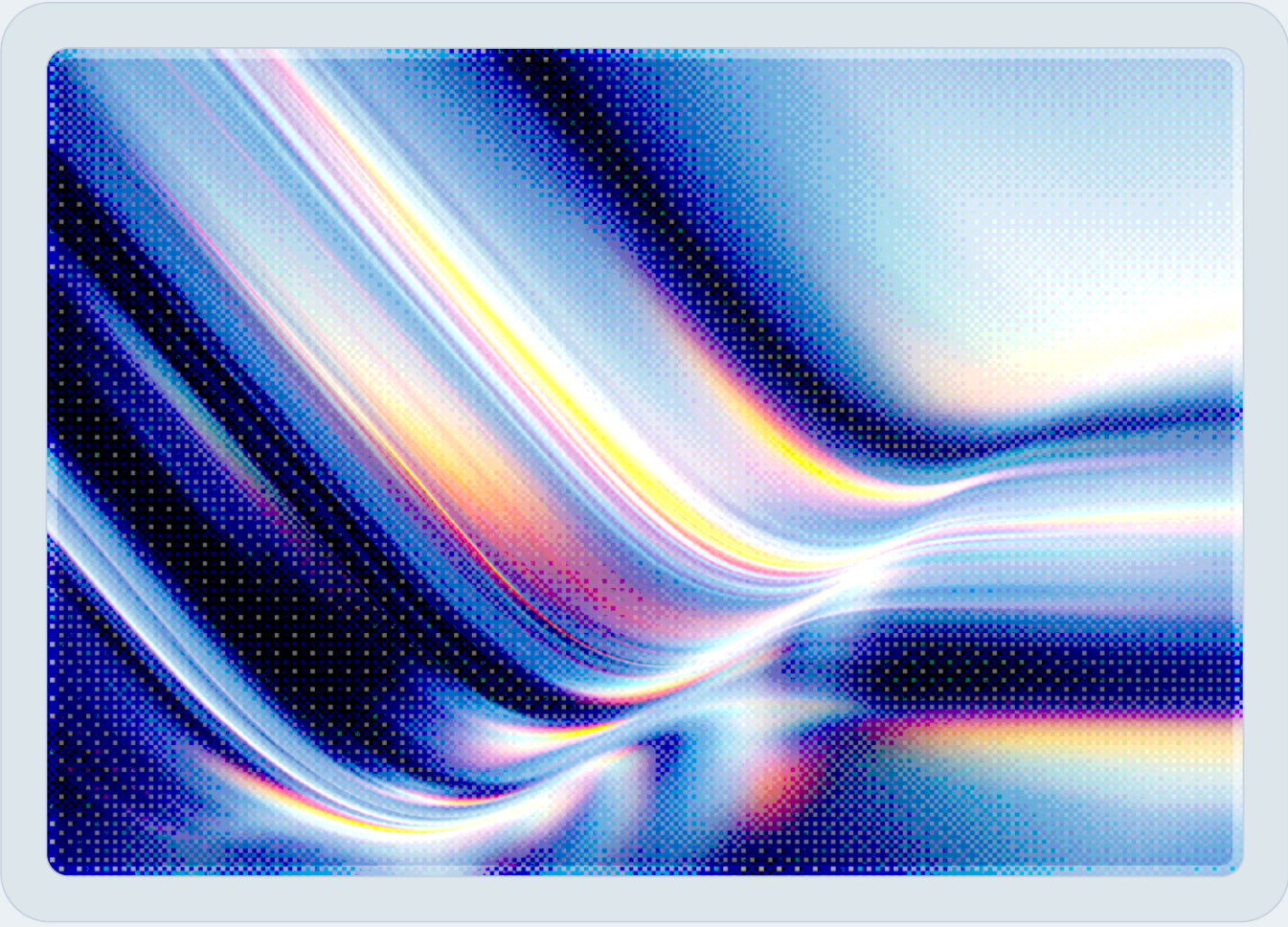
CSAI Foundation | Cloud Security Alliance

Residential Proxy Botnets: A Structural Attribution Blind Spot

How Consumer Devices Became Untraceable Relay Infrastructure for Cybercrime and Espionage

2026-08-13

AI-assisted Rapid Research



CSAI

CSA cloud security alliance®

Key Takeaways

- A single class of infrastructure — consumer devices repurposed as residential proxy exit nodes — now underlies commercial data-scraping SDKs, DDoS botnets, ad-fraud rings, and nation-state reconnaissance, making it unreliable to categorize traffic from any given home IP address as benign or malicious without out-of-band context [1][2][3].
- The July 2026 FBI/IRS seizure of the NetNut platform removed a single operator but not the underlying problem: at least two million devices worldwide were enrolled, in many cases with no disclosure a device owner would reasonably notice, and the SDK-based recruitment model NetNut used appears across numerous other residential proxy brands [3][8].
- Palo Alto Networks' Unit 42 documented Kimwolf v7, an Android/IoT DDoS botnet that both exploits unauthenticated Android Debug Bridge (ADB) services reachable through residential proxy infrastructure and disguises its own attack traffic as ordinary browser sessions using HTTP/2 and Chrome fingerprint mimicry [1][4].
- Cheap Android TV boxes sold on mainstream retail sites have shipped with firmware that alternates between acting as a residential proxy node and impersonating a mobile phone to commit ad fraud, illustrating that the commercial and criminal layers of this economy are frequently the same code running on the same device [5][6].
- Because reputation-based defenses (geofencing, IP blocklists, ASN filtering) assume that malicious traffic originates from identifiably malicious infrastructure, the residential proxy economy undermines that core assumption [2][8]. This note argues that enterprises should therefore prioritize behavioral and identity-centric controls over IP-reputation tooling alone.

Background

Residential proxy networks route internet traffic through IP addresses assigned to real home internet connections rather than through datacenter infrastructure, which makes the traffic appear to originate from an ordinary consumer rather than a hosting provider or VPN exit. That property has legitimate commercial value: companies that scrape public web data for AI model training, price monitoring, or ad verification pay a premium to route requests through residential IPs because anti-bot systems trust them more than datacenter IPs. It has equally strong criminal value for the same reason, and over the past two years the two use cases have become difficult to separate, both technically and financially.

The market has grown large enough to attract law enforcement attention at scale. On July 2, 2026, the FBI and IRS Criminal Investigation seized hundreds of domains belonging to NetNut, a residential proxy service operated by the publicly traded Israeli company Alarum Technologies (NASDAQ: ALAR) [3][8]. Google's Threat Intelligence Group, which supported the takedown alongside Lumen and Shadowserver, had already linked NetNut to a botnet it calls Popa, comprising at least two million home devices worldwide, many enrolled through software development kits (SDKs) bundled with pirated streaming apps or preinstalled on inexpensive, off-brand Android TV boxes and streaming sticks [8]. In a single week in June 2026, GTIG observed 316 distinct threat clusters — spanning cybercriminal and espionage-motivated actors — routing traffic through suspected NetNut exit nodes, using the network to mask the source of password-spraying campaigns and command-and-control communications [8]. Google also identified overlap between NetNut's plugin components and the previously disrupted BadBox2.0 campaign — a documented instance suggesting that device-recruitment supply chains may be shared and reused across nominally distinct botnet brands rather than built independently by each operator [8].

The consumer hardware layer of this economy has its own well-documented case study. Bitsight researcher Pedro Falé traced an ad-fraud network back to Zhejiang Fengwo IoT Technology Ltd, a mainland Chinese firm operating as the Fengwo Group, after discovering that a lapsed domain once used to coordinate the operation was available for registration [5][6]. Fengwo's software ships on H96-brand Android TV boxes sold through mainstream retailers including Amazon, Best Buy, and Newegg, and it alternates functions depending on whether the television is actively in use: while the screen displays HDMI input, the device behaves as a residential proxy exit node; when idle, it spoofs the identity of a Samsung, Huawei, Vivo, or Xiaomi smartphone and clicks ads on machine-generated websites [5][6]. Bitsight's verified sample of roughly 38,000 unique devices modeled gross returns of about $1.25 per device per day, implying tens of thousands of dollars in daily fraud revenue from that sample alone, with shell registrations in Hong Kong and Singapore obscuring the operation's ultimate ownership [5][6].

Malware operators have begun treating this residential proxy layer as attacker infrastructure in its own right rather than merely as a target for recruitment. Unit 42 documented in August 2026 that Kimwolf v7 — the latest version of a DDoS botnet lineage tracked since 2024 under the name AISURU — uses existing residential proxy services to reach Android TV boxes that expose an unauthenticated Android Debug Bridge (ADB) service on port 5555 within their local network, a misconfiguration common on inexpensive set-top boxes [1][4]. Once installed, Kimwolf v7 relies on a tiered, takedown-resistant command-and-control design: it first attempts to resolve control infrastructure through the Ethereum Name Service using several hard-coded public Ethereum RPC endpoints, and falls back to a hard-coded Tor v3 hidden service, routing all resulting traffic through a local proxy at 127.0.0.1:23075 so the malware can move fluidly between clearnet and Tor paths [1][4]. The v7 release also introduces an HTTP/2-based flood built on the nghttp2 library that constructs a complete Chrome browser fingerprint at both the protocol and header level, a change Unit 42 assesses was made specifically to defeat mitigation efforts that flagged the botnet's earlier, more distinguishable traffic patterns [1].

Security Analysis

Consent mechanisms do not distinguish commercial from criminal use. NetNut and Fengwo's H96 devices both relied on the same consent model: enrollment folded into an end-user license agreement bundled with a free VPN app, a "free" streaming device, or a pirated-content SDK, with any disclosure buried in dense legal text no consumer reads [3][5][6][8]. In the H96 case, the ad-fraud function was never disclosed at all [5][6]. Once a company's business model depends on aggregating a large enough pool of such nodes, the line between commercial proxy vendor and botnet operator becomes difficult for outside observers to draw — a concern this note treats as an open question specific to the documented NetNut and Fengwo cases, not a settled equivalence across the residential proxy industry generally. CSA's own analysis of AI-scraping proxy SDKs found that the same technical mechanisms — VPN-bypass network binding, background operation invisible to the device owner, and unauthenticated remote configuration channels — appear whether the SDK's stated purpose is AI training data collection or something more clearly abusive [2]. The Popa botnet's overlap with the previously disrupted BadBox2.0 campaign, and Kimwolf's direct exploitation of residential proxy access to reach vulnerable devices, show that criminal operators do not need to build recruitment infrastructure from scratch; they can rent, infiltrate, or piggyback on infrastructure a proxy vendor already built [1][4][8].

Why attribution failure is structural. Traditional network defenses assume that an IP address carries a stable reputational signal: datacenter ranges, known VPN exits, and previously flagged addresses can be blocked or deprioritized with reasonable confidence. Residential proxy infrastructure breaks that assumption by design — the same home IP address may carry a household's ordinary browsing traffic in one connection and an account-takeover attempt routed by a criminal renting proxy access in the next, with no durable technical signal to distinguish them at the network layer. Geofencing and IP-reputation controls that assume "malicious infrastructure" and "consumer infrastructure" are separate populations struggle badly against a population that is genuinely both at once, as GTIG's observation of 316 distinct threat clusters sharing one platform's exit nodes in a single week illustrates [8]. This is a primary reason enterprises should treat embedded proxyware as a first-class threat category in its own right rather than as an edge case to be handled by existing IP-reputation tooling [2].

State-linked actors are also renting the same consumer-device substrate. GTIG's observation that both cybercriminal and espionage-motivated clusters used NetNut's exit nodes in the same week is a documented instance of state-linked operators treating commercial residential proxy access as disposable relay infrastructure for obscuring origin [8]. This note argues that the pattern likely generalizes beyond a single platform, though that broader claim is not yet independently confirmed across other residential proxy brands. A related pattern appears in the China-linked JDY botnet, which Lumen's Black Lotus Labs documented growing from roughly 650 compromised SOHO and IoT devices in January 2024 to more than 1,500 by June 2026, and which survived the FBI's 2024 takedown of the

related KV-botnet to become a shared reconnaissance resource for multiple China-nexus threat actors, capable of scanning for a newly disclosed, critical Fortinet vulnerability (CVE-2026-35616, CVSS 9.1) within hours of public disclosure [7][9]. Whether the underlying device population is enrolled through a criminal exploit chain (JDY, Kimwolf) or a commercial SDK with a consent mechanism disclosed only nominally (NetNut, Fengwo), the operational effect for a defender is similar: attack and reconnaissance traffic increasingly originates from address space that looks exactly like an ordinary residential ISP subscriber, and conventional network-perimeter attribution tooling has no reliable way to tell the difference.

Recommendations

Immediate Actions

Security teams should inventory outbound network traffic for indicators associated with the specific campaigns documented above — Kimwolf's Tor v3 hidden service address and ENS-resolution RPC endpoints, NetNut/Popa SDK domains, and known Fengwo/H96 command infrastructure — and treat any internal device found beaconing to this infrastructure as compromised rather than merely policy-violating [1][4][8]. Organizations that issue or permit smart TVs, streaming boxes, or other consumer IoT devices on corporate or guest networks should audit those devices for unauthenticated ADB or similar remote-debugging services exposed on the local network, since this is Kimwolf's primary infection vector on Android TV hardware [1][4].

Short-Term Mitigations

Enterprises should extend software composition analysis and mobile application vetting to explicitly screen for residential proxy SDKs bundled in employee-facing or BYOD applications, since these SDKs are designed to bypass VPN-based monitoring at the network layer and will not be visible through traffic inspection alone [2]. Network segmentation should isolate smart TVs and other consumer IoT devices from corporate network segments entirely, rather than relying on application allowlisting, because the proxy and ad-fraud functions documented in the Fengwo case operate independently of the device's advertised purpose and are not reliably identifiable by application name [5][6]. Defenders should also shift threat-detection logic away from static IP reputation and geofencing — which IDC analyst Sakshi Grover has separately noted fail against distributed residential infrastructure, as quoted in CSA's JDY botnet research note — toward behavioral anomaly detection that flags unusual request patterns, timing, or volume regardless of source IP classification [7].

Strategic Considerations

Because commercial and criminal residential proxy infrastructure share recruitment mechanisms, vendors, and in some documented cases the same physical devices, organizations should factor SDK governance and residential-proxy exposure into vendor risk assessments and procurement criteria for any AI data vendor, ad-tech partner, or IoT hardware supplier, treating undisclosed proxy or telemetry functionality as a material finding rather than a boilerplate EULA disclosure [2]. Given that law enforcement action against a single operator (NetNut) removes one brand without addressing the underlying device-recruitment supply chain that produced it — a supply chain BadBox2.0's reappearance inside NetNut's infrastructure demonstrates is reused across operators — organizations should expect the residential proxy economy to persist in some form regardless of individual takedowns, and should plan detection and governance strategies accordingly rather than treating any single enforcement action as resolving the risk [8].

CSA Resource Alignment

CSA's own research provides the most directly applicable frameworks for this threat class. *Hidden Nodes: AI Scraping SDKs as Enterprise Attack Vectors* examined the same underlying infrastructure from the commercial side, documenting how AI-data-collection SDKs from vendors such as Bright Data enroll consumer devices as residential proxy exit nodes, bypass VPN-based enterprise monitoring, and converge with criminal botnet infrastructure including Kimwolf, Vo1d, and Badbox [2]. That paper's recommendation to treat embedded proxyware as a first-class enterprise threat category — with detection built on DNS/firewall blocking, software composition analysis, and network segmentation rather than IP reputation alone — applies directly to the NetNut, Popa, and Fengwo cases documented here, and its CSA Cloud Controls Matrix Supply Chain Management (STA-09 through STA-12) mappings give security teams a concrete control baseline for vendor and SDK governance [2].

JDY Botnet: China-Linked SOHO Scanning Targets U.S. Military documents the nation-state reconnaissance side of this same consumer-device attack surface, and its recommendations — accelerated edge-device patching, disabling internet-facing administrative interfaces, and applying Zero Trust least-privilege network policies to SOHO/IoT devices — are equally applicable to the ADB-exposed Android TV boxes that Kimwolf v7 targets [7]. Both documents converge on the same underlying control gap: consumer and SOHO devices receive materially less security investment, patching discipline, and monitoring than enterprise endpoints, even as they increasingly serve as the substrate for both criminal and state-sponsored operations.

Where this research note extends into AI data-supply-chain governance and vendor accountability more broadly, CSA's AI Controls Matrix (AICM) v1.1 — the current, expanded successor to the Cloud Controls Matrix, spanning 247 control objectives across 18 domains — provides the applicable control baseline for organizations assessing AI data vendors, SDK providers, and IoT hardware suppliers whose products may embed undisclosed residential proxy functionality [10].

References

[1] Palo Alto Networks Unit 42. "Kimwolf v7: An Evolution of the Kimwolf Botnet." Palo Alto Networks, August 2026.

[2] Cloud Security Alliance. "Hidden Nodes: AI Scraping SDKs as Enterprise Attack Vectors." CSA AI Safety Initiative, June 8, 2026.

[3] Krebs, Brian. "FBI Seizes NetNut Proxy Platform, Popa Botnet." Krebs on Security, July 2026.

[4] The Hacker News. "Kimwolf v7 Android Botnet Makes HTTP/2 DDoS Traffic Look Like Legitimate Browsing." The Hacker News, August 2026.

[5] Krebs, Brian. "Read This Before You Buy That TV Streaming Stick." Krebs on Security, July 2026.

[6] The Hacker News. "Cheap Android TV Boxes Pose as Phones and Turn Owners' Broadband Into Proxies." The Hacker News, July 2026.

[7] Cloud Security Alliance. "JDY Botnet: China-Linked SOHO Scanning Targets U.S. Military." CSA AI Safety Initiative, June 11, 2026.

[8] Google Cloud. "Google's Continued Disruption of Malicious Residential Proxy Networks." Google Cloud Blog, July 2026.

[9] The Hacker News. "China-Linked JDY Botnet Expands to 1,500+ Devices for Cyber Reconnaissance." The Hacker News, June 2026.

[10] Cloud Security Alliance. "AI Controls Matrix (AICM) v1.1." Cloud Security Alliance, June 22, 2026.