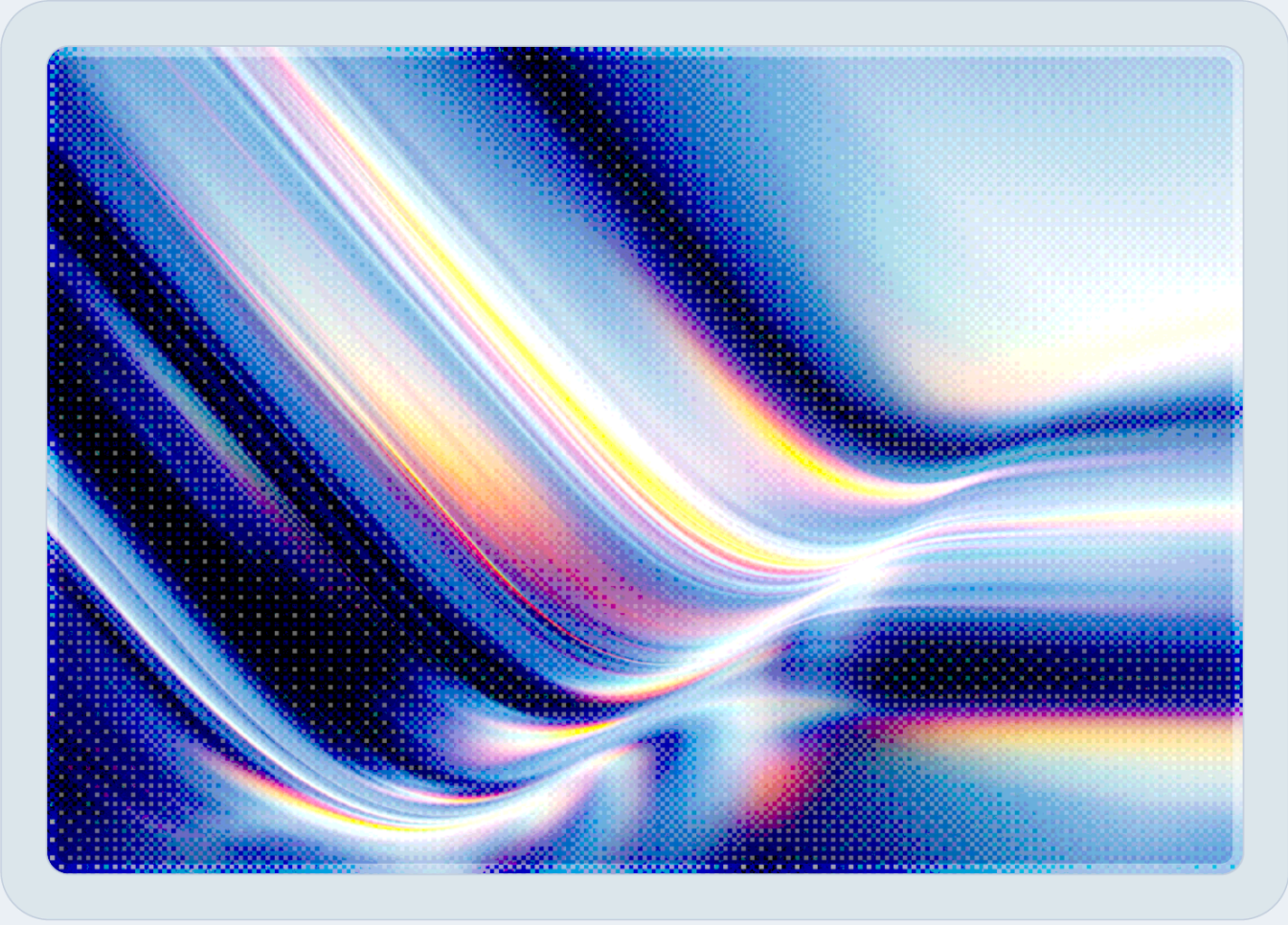
CSAI Foundation | Cloud Security Alliance

The Proxy-for-Profit Economy: Consumer Devices as Attack Infrastructure

2026-08-15

AI-assisted Rapid Research



CSAI

CSA cloud security alliance®

Key Takeaways

Four separate disclosures between July and August 2026 document that the residential proxy economy has become a self-sustaining ecosystem where legitimate advertising-supported businesses, hardware vendors, and criminal botnet operators now share the same underlying infrastructure, and in at least one documented case — NetNut's residential IP pool and the Popa botnet — the same compromised devices. The FBI's July 2 seizure of hundreds of domains tied to NetNut, a residential proxy service operated by the publicly traded Israeli firm Alarum Technologies, exposed direct operational overlap with the Popa botnet, a network of more than two million largely unconsenting smart TVs and streaming boxes [1]. Independent research from Spur found that proxy software development kits ship inside 42 percent of apps on LG's webOS smart TV store and more than 25 percent of apps on Samsung's Tizen platform; days later, LG announced it will suspend any app that will not remove the capability [2][3]. A parallel investigation into inexpensive Android streaming sticks sold under the H96 brand found roughly 38,000 devices silently leasing their owners' internet connections while simultaneously running an ad-fraud scheme worth an estimated $50,000 a day [4]. Most recently, Socket researchers identified 737 Chrome browser extensions, many impersonating trusted VPN brands, that routed users' entire browsing sessions through an undisclosed SOCKS5 proxy network, collecting more than 75,000 installs before hundreds were removed from the Chrome Web Store [5]. Read together, these four cases show that the residential proxy economy has outgrown any single vendor, platform, or takedown, and that consumer-facing hardware and software has become durable, hard-to-attribute infrastructure for scraping, fraud, and cyberattack traffic.

Background

Residential proxy networks route internet traffic through the IP addresses of ordinary consumer devices rather than through data-center servers, making that traffic appear to originate from a real household rather than a hosting provider. Commercial proxy vendors have marketed this capability for years as a tool for market research, ad verification, and, increasingly, for collecting the volumes of web data that large language model training and retrieval pipelines require. CSA's own research has previously assessed AI data-collection demand as a significant driver of this market's growth, with one major provider alone advertising a pool of more than 400 million residential IP addresses [9]. What has

changed through the middle of 2026 is the degree to which the supply side of that market, the mechanism by which a household's IP address ends up for sale, has converged with methods indistinguishable from botnet recruitment.

The NetNut case illustrates that convergence directly. Google's Threat Intelligence Group found that criminal actors used NetNut's exit nodes to mask the origin of attacks against victim environments, and proxy-tracking firm Synthient documented that NetNut's daily traffic and pricing grew to rival its predecessor, IPIDEA, after that service was disrupted by law enforcement earlier in 2026 [1]. Investigative reporting published June 19 tied NetNut's residential IP pool to the Popa botnet, a collection of at least two million compromised devices, overwhelmingly smart TVs and streaming boxes, infected with proxy software often without meaningful user consent [1]. In a single week in June 2026, researchers observed 316 distinct threat-actor clusters routing traffic through NetNut exit nodes for purposes including mass content scraping, advertising fraud, account-takeover attempts, and distributed denial-of-service activity [1]. The FBI's subsequent domain seizure, conducted jointly with the IRS Criminal Investigation division and assisted by Google, Lumen, and Shadowserver, sent Alarum Technologies' publicly traded stock down 67 percent, a decline that illustrates the direct financial and legal consequences enforcement can now carry for companies operating in this space [1].

The H96 streaming-stick investigation and the Spur research into smart TV app stores show that the same dynamic operates at the hardware and platform level, not only through a single vendor's software. Devices sold under the H96 brand, tied to the mainland Chinese firm Zhejiang Fengwo IoT Technology, shipped with software that behaved differently depending on whether the television was in active use: while a viewer watched, the device quietly relayed third-party proxy traffic; once the screen went dark, the same device pivoted to executing ad fraud by impersonating mobile phones and clicking ads on fabricated websites [4]. Bitsight researcher Pedro Falé described discovering the scheme when devices reporting into Fengwo's infrastructure and identifying themselves as smart TV boxes were, in fact, behaving like phones [4]. Separately, Spur's July 2 research found that legitimate app developers, from screensaver makers to a Pac-Man clone, had embedded proxy SDKs, predominantly from vendor Bright Data, inside otherwise ordinary smart TV apps distributed through LG's and Samsung's official app stores, with users typically consenting through a single buried prompt rather than an ongoing, meaningful disclosure [2][3].

Security Analysis

The most consequential pattern across these four disclosures, in this report's assessment, is that residential proxy infrastructure has become effectively fungible between commercial data-collection use cases and criminal attack infrastructure — and that, in the cases documented here, neither a device's

owner nor the platform hosting the app reliably distinguished which use was occurring at a given moment. NetNut is marketed as a legitimate commercial proxy provider, yet Google's own threat intelligence team documented its use by attackers seeking to mask their origin during intrusions, and independent researchers linked its residential IP supply directly to a two-million-device botnet [1]. Bright Data, whose SDK accounts for the majority of proxy code found in LG and Samsung app stores, describes its own network in its published trust materials as consent-based, stating that "every individual part of our residential network has voluntarily opted in" and that only vetted, approved apps may carry the SDK [7]. Yet Bright Data did not respond to reporters' questions about the specific LG and Samsung findings, and the consent Bright Data describes typically took the form of the kind of single buried prompt that Spur researcher Trevor Sutter argued is "not a substitute for meaningful transparency, ongoing control, and platform oversight," a gap Sutter noted is compounded when a household member who is not the device's primary user, including a minor, is the one who taps through it [2][3]. The distinction between a "legitimate" proxy network and a botnet, in practice, has become a matter of consent quality and downstream customer vetting rather than of the underlying technical architecture, and the evidence from mid-2026 suggests that both are frequently deficient.

This ambiguity creates a durable enterprise and consumer risk that the single enforcement action documented here did not resolve. When the FBI disrupted IPIDEA earlier in 2026, criminal customers did not disappear; they migrated to NetNut, whose traffic volume and pricing grew to match its predecessor within months [1]. Enforcement against a single named provider, based on that migration, appears to address a symptom of an economic structure rather than the underlying incentive for consumer hardware manufacturers, app developers, and advertising-supported businesses to keep monetizing their users' bandwidth — the persistent demand for residential-IP anonymization from actors who scrape, commit fraud, or launch attacks. The H96 case demonstrates the hardware-level version of the same incentive: Fengwo's own internal documentation, according to researchers, described a business model built around "only a small number of highly-skilled developers," with lower-skilled staff producing execution units at scale specifically to keep operating costs down, a structure optimized for maximizing device deployment rather than for user disclosure [4].

The Chrome extension findings extend this pattern from dedicated hardware into everyday enterprise and consumer software. Socket's research found that 737 extensions, at least 40 separate Chrome Web Store developer accounts, and 274 direct impersonations of established VPN brands including Proton VPN, NordVPN, Surfshark, and ExpressVPN routed every request a victim's browser made, including internal network addresses, through SOCKS5 infrastructure that Socket researchers assessed as linked to a single Russian-based operator [5][6]. Because the extensions displayed convincing fake premium-tier interfaces and included internal operator instructions to avoid hard-coding proxy domains directly into Chrome's proxy-settings API, standard endpoint inspection would likely miss the behavior entirely, a technique that mirrors the VPN-bypass mechanisms CSA has previously documented in commercial proxy SDKs embedded on mobile and smart TV platforms [5][9]. An organization that treats "the user

installed a VPN extension" as a benign or even protective event, without verifying the extension's actual routing behavior, is exposed to a closely comparable class of silent, unmonitored egress that smart TV and Android-based proxyware creates, extending the structural attribution problem CSA identified across consumer IoT devices to any employee's personal or work browser [8].

Recommendations

Immediate Actions

Security teams should inventory outbound network traffic for indicators tied to the four schemes documented here, including known NetNut, Bright Data, and Fengwo/H96 domains, and should treat any smart TV, streaming box, or Android TV device on a corporate or home network as a potential proxy exit node rather than a passive display. Enterprises should also audit installed Chrome extensions across managed endpoints against Socket's published indicator list and remove any extension exhibiting SOCKS5 proxy behavior inconsistent with its advertised function, regardless of its Chrome Web Store rating or install count, since the campaign's fake reviews and premium-tier interfaces appear crafted to defeat cursory vetting [5].

Short-Term Mitigations

Organizations should extend software composition analysis and application-vetting processes to cover consumer and BYOD devices connecting to corporate networks, not only managed endpoints, since the Spur research demonstrates that even trivial applications such as screensavers and simple games can carry proxy SDKs capable of bypassing VPN-based monitoring [2][3]. IT and procurement teams evaluating smart TVs, streaming hardware, or browser extensions for organizational use should favor platforms that have demonstrated active SDK governance, such as LG's July 2026 policy change, over platforms that have not yet restricted background proxy functionality, and should build proxy-SDK disclosure into vendor security questionnaires going forward [3].

Strategic Considerations

Because enforcement against a single proxy provider or device manufacturer has, in the case observed here, shifted criminal demand to the next available supplier rather than eliminating it, security leadership should treat residential proxy exposure as a risk category warranting recurring review even as this pattern awaits confirmation across additional enforcement actions, rather than as a one-time remediation triggered by a specific news event. This means building egress-monitoring architecture that

authenticates traffic by device and application behavior rather than by IP reputation alone, since residential proxy traffic is by design indistinguishable from a legitimate home user at the network layer, and periodically reassessing that architecture as new device categories, from smart TVs to browser extensions to, plausibly next, other IoT and wearable form factors, are recruited into the same economy.

CSA Resource Alignment

CSA's own research, published two days before this note, already documents the pattern described here in detail. Residential Proxy Botnets: A Structural Attribution Blind Spot, published August 13, 2026, examines the same NetNut seizure and H96/Fengwo case studies covered here and reaches the same core conclusion: reputation-based defenses that assume malicious traffic originates from identifiably malicious infrastructure no longer hold, because commercial data-scraping SDKs, DDoS botnets, ad-fraud rings, and state-sponsored reconnaissance now run on the same enrolled consumer devices [8]. That note did not yet capture the Chrome VPN-extension campaign Socket disclosed on August 11 and 12, and this research note's principal contribution is extending CSA's structural-attribution finding to browser-based proxy infrastructure, showing that the same fungibility between commercial and criminal use applies to software users install directly rather than only to hardware they buy. Hidden Nodes: AI Scraping SDKs as Enterprise Attack Vectors, published June 8, 2026, supplies the underlying technical detail on how commercial proxy SDKs bypass VPN monitoring at the control- and data-plane level, detail directly transferable to auditing the Chrome extensions' SOCKS5 traffic redirection described above [9]. Organizations acting on either publication's recommendations should also consult CSA's AI Controls Matrix (AICM) v1.1, whose supply-chain management and application and interface security domains provide control-level structure for the SDK governance, vendor due-diligence, and network segmentation measures recommended in this note [10].

References

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

[2] Krebs, Brian. "LG to Ban Residential Proxies from Smart TV Apps." Krebs on Security, July 2026.

[3] Help Net Security. "Residential Proxy SDKs Are Hiding in LG and Samsung Smart TV Apps." Help Net Security, June 2026.

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

[5] Pandya, Kush. "737 Chrome VPN Extensions Linked to Brand Impersonation and Browser Traffic Redirection." Socket, August 2026.

[6] The Hacker News. "737 Chrome VPN Extensions Caught Routing Traffic Through Proxies." The Hacker News, August 2026.

[7] Bright Data. "Bright SDK: Ethical Data Practices." Bright Data Trust Center, 2026.

[8] Cloud Security Alliance. "Residential Proxy Botnets: A Structural Attribution Blind Spot." Cloud Security Alliance, August 2026.

[9] Cloud Security Alliance. "Hidden Nodes: AI Scraping SDKs as Enterprise Attack Vectors." Cloud Security Alliance, June 2026.

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

