INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-06 14:05 UTC

Smart TVs as Silent Proxies: How SDK Supply Chains Route AI Scraping Through Home Networks

SECURITY ANALYSIS | MEDIUM | CVSS 5.0

SCC Item ID	SCC-STY-2026-0169
Type	Security Analysis
Severity	MEDIUM
CVSS Base Score	5.0
Affected Products	iOS devices, Roku devices (Petflix app), Samsung Tizen smart TVs, LG webOS smart TVs; apps by PlayWorks Digital, CloudTV, Longvision; Bright Data SDK (proxyjs.brdtnet.com, proxyjs.luminatinet.com, proxyjs.bright-sdk.com)
Published	2026-06-06T04:29:05
Discovery Source	Rss

Executive Summary

Research by Include Security reveals that free consumer apps embedded with Bright Data's SDK are silently enrolling Samsung Tizen smart TVs, LG webOS smart TVs, Roku devices, and iOS phones as residential proxy nodes that relay third-party web scraping traffic without meaningful user consent. The SDK bypasses VPN controls on iOS and operates on unauthenticated peer channels, meaning enterprise BYOD fleets and smart TV deployments may be quietly routing external traffic through corporate network egress points. This finding signals a maturing supply chain risk model where commercial SDKs, not malware, serve as the infrastructure layer for large-scale data collection operations.

Technical Analysis

The research by Include Security presents a technically detailed supply chain abuse scenario that diverges from conventional malware distribution. Rather than deploying a standalone agent, Bright Data's SDK is packaged inside legitimate free applications distributed through standard app marketplaces, including apps by PlayWorks Digital, CloudTV, and Longvision. Once installed, the SDK silently enrolls the host device as a residential proxy exit node, routing web scraping traffic, described in reporting as AI-driven data collection, through the device's residential IP address.

Three technical findings carry the most defensive significance.

First, the SDK's peer channel operates without authentication. This means the relay mechanism is exposed to unauthorized abuse: any actor who understands the protocol could theoretically issue relay instructions without the device owner's or SDK operator's authorization. This maps directly to CWE-287 (Improper Authentication) and elevates the risk beyond the SDK's stated commercial purpose.

Second, on iOS, SDK traffic bypasses VPN tunnels. This is a significant control evasion: organizations relying on VPN-enforced network monitoring, split-tunnel visibility, or CASB policies tied to VPN egress will not see this traffic in their telemetry. The behavior maps to MITRE T1071.001 (Application Layer Protocol: Web Protocols) and T1090.002 (Proxy: External Proxy), and exploits a documented gap in iOS network stack handling rather than a traditional exploit.

Third, the bandwidth caps described in SDK configuration files do not match the disclosures shown to users on opt-in screens. This consent discrepancy is the basis for classifying this under CWE-200 (Exposure of Sensitive Information) and CWE-693 (Protection Mechanism Failure), and it surfaces a regulatory exposure for apps operating in jurisdictions with informed consent requirements.

For enterprise security teams, the threat model shifts. The affected devices, smart TVs and BYOD iOS devices, are frequently outside EDR coverage and below the threshold of standard asset inventory processes. Traffic originating from legitimate residential IPs does not trigger IP reputation blocks. The SDK's presence inside signed, marketplace-distributed applications means application allow-listing provides no protection. The Aisuru botnet is referenced in surrounding reporting as contextual precedent, suggesting the residential proxy market that commercial SDKs like Bright Data's serve has overlap with infrastructure used by more overtly malicious actors.

Source note: Technical claims are attributed to Include Security's published research. These findings have not been independently verified here.

Action Checklist

1. Step 1: Assess exposure, audit your BYOD mobile fleet and smart TV deployments (Samsung Tizen, LG webOS, Roku) for the presence of apps by PlayWorks Digital, CloudTV, or Longvision; check for network connections to proxyjs.brdtnet.com, proxyjs.luminatinet.com, and proxyjs.bright-sdk.com
2. Step 2: Review controls, verify whether your network monitoring covers traffic from iOS devices that bypass VPN tunnels; standard split-tunnel VPN visibility will not capture SDK relay traffic per the Include Security findings; evaluate DNS logging (NIST AU-2) and firewall egress rules (CIS 4.4, CIS 4.5) for coverage of the Bright Data SDK domains
3. Step 3: Update threat model, add commercial SDK-as-proxy-infrastructure to your supply chain threat register; this pattern is distinct from traditional malware and requires policy review of third-party SDK vetting for any app permitted on BYOD or corporate smart TV deployments; reference MITRE T1195.002 (Supply Chain Compromise: Compromise Software Supply Chain) and T1090.002 (Proxy: External Proxy)
4. Step 4: Communicate findings, brief leadership on the BYOD and smart TV asset gap using business-impact framing: unmonitored residential proxy enrollment creates unknown bandwidth consumption, potential regulatory exposure under data protection frameworks in applicable jurisdictions, and reputational risk if corporate IP addresses are associated with third-party scraping operations
5. Step 5: Monitor developments, track Include Security's published research for updated indicators; watch for regulatory responses from Apple, Roku, Samsung, or LG regarding SDK disclosure requirements; monitor for any law enforcement or FTC action related to Bright Data's SDK consent practices

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate to immediate priority and engage legal/privacy counsel if DNS or firewall logs confirm active proxy relay traffic from devices handling corporate data, if any affected device is within scope of GDPR, CCPA, or HIPAA due to the data types it accesses, or if corporate public IP addresses are confirmed to appear in Bright Data's residential proxy pool — any of these conditions creates regulatory notification exposure.
Recovery Notes	After blocking the three Bright Data SDK domains at DNS and firewall egress, verify that no residual outbound connections to those domains or their CDN IP ranges persist by monitoring firewall deny logs for 72 hours post-block. Remove or quarantine apps by PlayWorks Digital, CloudTV, and Longvision from BYOD devices via MDM push and from smart TV deployments via manual uninstall or device policy enforcement; confirm removal by re-running the app inventory audit from Step 1. Maintain heightened DNS and NetFlow monitoring on BYOD and smart TV segments for 30 days post-remediation to detect any SDK variant domains or updated Bright Data endpoints that may emerge if the SDK rotates its infrastructure in response to disclosure.
Forensic Artifacts	DNS query logs from your internal resolver filtered for proxyjs.brdtnet.com, proxyjs.luminatinet.com, and proxyjs.bright-sdk.com — these are the primary C2/relay registration domains identified in the Include Security research and will show which devices initiated SDK enrollment | Outbound NetFlow or firewall session records from Samsung Tizen, LG webOS, and Roku device MAC/IP addresses showing persistent long-duration TCP sessions to Bright Data CDN IP ranges — the SDK maintains peer relay channels that appear as unusual long-lived outbound flows distinct from normal smart TV streaming traffic | iOS device network extension or per-app VPN configuration state from MDM console — the SDK's ability to bypass VPN on iOS means evidence of relay activity will appear in on-device network logs (accessible via Apple Configurator 2 syslog capture or MDM diagnostic logs) rather than corporate VPN gateway logs | App binary strings or manifest analysis artifacts for PlayWorks Digital, CloudTV, or Longvision apps — specifically the presence of 'proxyjs', 'brdtnet', 'luminatinet', or 'bright-sdk' strings extracted via 'strings | grep -E brdtnet|luminatinet|bright-sdk' confirming SDK inclusion in the specific app version installed on the device | Router or managed switch interface bandwidth counters for the BYOD and smart TV network segments showing anomalous outbound traffic volume during off-hours — Bright Data SDK relay traffic on behalf of third-party scraping operations frequently occurs outside normal user activity windows and will appear as unexplained bandwidth spikes in interface statistics

Per-Action IR Details

Step 1: Assess exposure — audit your BYOD mobile fleet and smart TV deployments (Samsung Tizen, LG webOS, Roku) for the presence of apps by PlayWorks Digital, CloudTV, or Longvision; check for network connections to proxyjs.brdtnet.com, proxyjs.luminatinet.com, and proxyjs.bright-sdk.com

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection & Analysis: Identify affected assets and confirm scope of adversarial activity before proceeding to containment

Controls: NIST AU-2 (Event Logging), NIST AU-6 (Audit Record Review, Analysis, And Reporting), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 2.1 (Establish and Maintain a Software Inventory)

Compensating: On network edge: run 'sudo tcpdump -n host proxyjs.brdtnet.com or host proxyjs.luminatinet.com or host proxyjs.bright-sdk.com' on the gateway interface to capture live relay traffic. For DNS discovery without SIEM, query Pi-hole or pfSense/OPNsense DNS logs: grep -E 'brdtnet\.com|luminatinet\.com|bright-sdk\.com' /var/log/pihole.log. For Roku and Tizen inventory, cross-reference router DHCP leases (show ip dhcp binding on Cisco IOS, or cat /tmp/dhcp.leases on DD-WRT) against known MAC OUI prefixes for Samsung (Samsung Electronics OUI blocks) and Roku Inc. For iOS BYOD, use Apple Configurator 2 or MDM console app inventory to list installed app bundle IDs matching PlayWorks Digital, CloudTV, or Longvision titles.

Evidence: Capture BEFORE auditing: (1) Full DNS query logs from your resolver covering the prior 30 days — filter for proxyjs.brdtnet.com, proxyjs.luminatinet.com, proxyjs.bright-sdk.com; (2) NetFlow or firewall session logs showing outbound connections from smart TV VLAN or BYOD segments to Bright Data CDN IP ranges; (3) Router/DHCP lease table snapshot with MAC addresses and hostnames to establish which devices are Samsung Tizen, LG webOS, or Roku; (4) MDM app inventory export listing installed apps with developer/publisher metadata on enrolled iOS devices.

Step 2: Review controls — verify whether your network monitoring covers traffic from iOS devices that bypass VPN tunnels; standard split-tunnel VPN visibility will not capture SDK relay traffic per the Include Security findings; evaluate DNS logging (NIST AU-2) and firewall egress rules (CIS 4.4, CIS 4.5) for coverage of the Bright Data SDK domains

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection & Analysis: Validate that monitoring instrumentation has adequate visibility into the specific evasion mechanism (VPN bypass on iOS) before declaring detection coverage adequate

Controls: NIST AU-2 (Event Logging), NIST AU-12 (Audit Record Generation), NIST AC-17 (Remote Access), NIST AC-4 (Information Flow Enforcement), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices), CIS 8.2 (Collect Audit Logs)

Compensating: To test VPN bypass blind spot: connect an iOS test device to the corporate network without VPN, install a known Bright Data SDK-embedded app, and run Wireshark on the network tap or mirror port — if SDK traffic to proxyjs.* domains appears unencrypted or via direct TCP without tunneling through your VPN gateway IP, the bypass is confirmed. For persistent monitoring without SIEM, deploy a DNS sinkhole rule in Pi-hole or Bind9 for the three Bright Data SDK domains and set logging to verbose; any resolution attempt will generate a syslog event capturable by syslog-ng or rsyslog forwarding. Add explicit DENY egress rules in pfSense/OPNsense firewall for proxyjs.brdtnet.com, proxyjs.luminatinet.com, proxyjs.bright-sdk.com and enable rule hit logging to /var/log/filter.log.

Evidence: Capture BEFORE control review: (1) Current VPN gateway session logs showing which iOS devices are enrolled in split-tunnel vs. full-tunnel configurations — export from your VPN admin console; (2) Firewall egress rule set export to document the current state of outbound filtering for smart TV VLANs and BYOD segments; (3) A packet capture (pcap) from the LAN-side of the internet gateway during a 15-minute window on a network segment containing Samsung Tizen or LG webOS devices — save as baseline evidence of current relay traffic volume to proxyjs.* endpoints; (4) DNS resolver query log snapshot (prior 7 days minimum) as baseline before any sinkholing is applied.

Step 3: Update threat model — add commercial SDK-as-proxy-infrastructure to your supply chain threat register; this pattern is distinct from traditional malware and requires policy review of third-party SDK vetting for any app permitted on BYOD or corporate smart TV deployments; reference MITRE T1195.002 (Supply Chain Compromise: Compromise Software Supply Chain) and T1090.002 (Proxy: External Proxy)

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: Update threat models, policies, and detection capabilities based on lessons learned from the incident to prevent recurrence

Controls: NIST AC-20 (Use Of External Systems), NIST CM-1 (Policy And Procedures), CIS 2.2 (Ensure Authorized Software is Currently Supported), CIS 2.3 (Address Unauthorized Software), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: For a 2-person team without a GRC platform: create a simple threat register entry in a shared spreadsheet or Markdown file documenting the Bright Data SDK pattern with these fields: Threat Name ('Commercial SDK Residential Proxy Enrollment'), Affected Asset Classes ('iOS BYOD, Samsung Tizen, LG webOS, Roku'), MITRE Techniques ('T1195.002, T1090.002'), Detection Gap ('iOS VPN bypass, unauthenticated peer channels'), and Vetting

Control Gap ('No SDK publisher vetting in BYOD policy'). Add a mandatory SDK vetting checklist to your app approval workflow: check app publisher against known Bright Data SDK partners, search app binary or manifest for proxyjs.* domain strings using 'strings | grep -E brdtnet|luminatinet|bright-sdk', and require privacy policy review for any free app relying on ad or data monetization.

Evidence: Capture BEFORE threat model update: (1) Export current BYOD acceptable-use policy and any existing third-party app vetting criteria as a baseline document to demonstrate the policy gap; (2) Network traffic summary report showing confirmed or suspected Bright Data SDK relay sessions — this quantifies blast radius and supports the threat register entry; (3) List of all currently approved apps on BYOD fleet and smart TV deployments with their SDK dependency information (where obtainable from app store privacy labels or developer documentation) to identify other potential SDK-as-proxy exposures beyond PlayWorks Digital, CloudTV, and Longvision.

Step 4: Communicate findings — brief leadership on the BYOD and smart TV asset gap using business-impact framing: unmonitored residential proxy enrollment creates unknown bandwidth consumption, potential regulatory exposure under data protection frameworks in applicable jurisdictions, and reputational risk if corporate IP addresses are associated with third-party scraping operations

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment: Execute IR plan in coordination with relevant stakeholders; communicate scope, impact, and required decisions to leadership to authorize containment actions

Controls: NIST AC-1 (Policy And Procedures), NIST AU-6 (Audit Record Review, Analysis, And Reporting), CIS 3.2 (Establish and Maintain a Data Inventory)

Compensating: Prepare a one-page executive brief with three concrete data points: (1) Number of devices confirmed or potentially enrolled as Bright Data proxy nodes based on DNS/firewall log hits against proxyjs.* domains; (2) Estimated outbound bandwidth consumed by relay traffic — pull this from router/firewall interface statistics for the smart TV VLAN and BYOD segment over the prior 30 days using SNMP polling data or 'show interfaces' on managed switches; (3) Corporate IP exposure risk — use a free WHOIS or BGP lookup against your public IP ranges to confirm whether any of those IPs appear in Bright Data's advertised residential proxy pool (Bright Data publicly markets its residential proxy network, so checking their proxy pool documentation or contacting them directly is a legitimate verification step). Frame the ask: authorization to block the three Bright Data SDK domains at the DNS and firewall layer immediately.

Evidence: Capture BEFORE leadership brief: (1) Firewall and DNS log excerpts (sanitized for readability) showing specific timestamps and device IPs making connections to proxyjs.brdtnet.com, proxyjs.luminatinet.com, or proxyjs.bright-sdk.com — these are your primary evidence exhibits; (2) Bandwidth utilization data for BYOD and smart TV network segments over the prior 30 days to quantify the operational impact of proxy relay activity; (3) Screenshot or export of the Include Security research findings and any app store privacy label data for PlayWorks Digital, CloudTV, or Longvision apps as third-party corroboration supporting the business case.

Step 5: Monitor developments — track Include Security's published research for updated indicators; watch for regulatory responses from Apple, Roku, Samsung, or LG regarding SDK disclosure requirements; monitor for any law enforcement or FTC action related to Bright Data's SDK consent practices

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: Incorporate external intelligence updates and regulatory developments into improved detection capabilities and policy; share lessons learned

Controls: NIST AU-13 (Monitoring For Information Disclosure), NIST AU-11 (Audit Record Retention), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: Set up free RSS or GitHub watch alerts on the Include Security blog (https://includesecurity.com) and their public research repositories to receive notification of updated Bright Data SDK indicators of compromise. Create a Google Alert for 'Bright Data SDK' and 'proxyjs residential proxy' to track regulatory and press developments. Retain all DNS logs, firewall session logs, and packet captures collected during Steps 1-4 for a minimum of 12 months per NIST AU-11 (Audit Record Retention) in case FTC or data protection authority inquiries require evidence of organizational awareness and response. Schedule a 90-day review of the smart TV and BYOD app approval policy to incorporate any new SDK vetting requirements issued by Apple, Roku, Samsung, or LG in response to this research.

Evidence: Capture BEFORE closing monitoring posture: (1) Archive all DNS sinkhole hit logs for proxyjs.* domains after blocking is applied — these logs document continued resolution attempts post-remediation, which would indicate persistent SDK activity despite app removal; (2) Retain a snapshot of your network egress firewall ruleset showing the Bright Data SDK domain blocks as timestamped evidence of your remediation action date; (3) Document any app removals from BYOD devices or smart TV deployments with device identifiers and removal timestamps to establish a remediation evidence trail for potential regulatory inquiries.

Detection Guidance

Primary detection surface is DNS and egress traffic. Block and alert on connections to the three documented Bright Data SDK domains: proxyjs.brdtnet.com, proxyjs.luminatinet.com, and proxyjs.bright-sdk.com. These domains should be added to DNS sinkholes and firewall egress deny lists immediately.

For network anomaly hunting, look for smart TV or mobile device traffic profiles inconsistent with user activity: sustained outbound connections at non-peak hours, elevated bandwidth from devices that should be idle, or outbound web-protocol traffic to rotating external endpoints. Smart TVs in conference rooms or common areas are particularly likely to be missed by endpoint-focused monitoring.

For iOS BYOD fleets, standard VPN-tunnel-based traffic inspection will not surface SDK relay traffic per the research findings. Supplement with DNS query logging at the resolver level (covering all network egress, not only VPN-tunneled flows) and review per NIST AU-2 (Event Logging) to confirm smart TV and BYOD device categories are in scope for audit log collection.

Audit your mobile application management (MAM) policy against the affected apps: PlayWorks Digital, CloudTV, and Longvision apps are the confirmed SDK carriers. CIS 2.1 (Establish and Maintain a Software Inventory) and CIS 2.3 (Address Unauthorized Software) apply directly: if these apps appear on managed or BYOD devices, treat them as unauthorized pending policy review.

For broader SDK supply chain posture, review your third-party app vetting process against NIST AC-20 (Use of External Systems) to determine whether apps permitted on BYOD or corporate endpoints are evaluated for embedded SDK data handling. The consent discrepancy documented in this research suggests that app store privacy labels alone are insufficient for vetting.

Behavioral hunting hypothesis: query DNS logs for any device in the smart TV or mobile asset category resolving domains matching the pattern proxyjs.*.com. Flag any device generating sustained TCP connections to external IPs over standard web ports (80/443) at volumes inconsistent with user-initiated browsing.

Indicators of Compromise

Type	Value	Context	Confidence
DOMAIN	`proxyjs.brdtnet.com`	Bright Data SDK command-and-control domain used to enroll devices as residential proxy nodes and route scraping traffic	HIGH
DOMAIN	`proxyjs.luminatinet.com`	Bright Data SDK infrastructure domain; alternate endpoint for proxy enrollment and relay traffic	HIGH

Type	Value	Context	Confidence
DOMAIN	`proxyjs.bright-sdk.com`	Bright Data SDK infrastructure domain; alternate endpoint for proxy enrollment and relay traffic	HIGH

Framework Mappings

MITRE-ATTACK

- **T1059** — Command and Scripting Interpreter
- **T1571** — Non-Standard Port
- **T1016** — System Network Configuration Discovery
- **T1090.002** — External Proxy
- **T1036** — Masquerading
- **T1071.001** — Web Protocols
- **T1195.002** — Compromise Software Supply Chain
- **T1102** — Web Service
- **T1496** — Resource Hijacking

NIST-800-53R5

- **CM-7** — Least Functionality
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-7** — Software, Firmware, and Information Integrity
- **SA-9** — External System Services
- **SR-3** — Supply Chain Controls and Processes
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-8** — Identification and Authentication (Non-Organizational Users)
- **AC-3** — Access Enforcement
- **SC-28** — Protection of Information at Rest
- **SR-2** — Supply Chain Risk Management Plan

OWASP-TOP10-2021

- **A07:2021** — Identification and Authentication Failures
- **A01:2021** — Broken Access Control

CIS-V8

- **6.3** — Require MFA for Externally-Exposed Applications
- **6.4** — Require MFA for Remote Network Access
- **6.5** — Require MFA for Administrative Access
- **15.1** — Establish and Maintain an Inventory of Service Providers

- **8.2** — Collect Audit Logs

SOC2-TSC

- **CC6.1** — The entity implements logical access security software, infrastructure, and architectures over protected information assets
- **CC9.2** — Manages risks associated with vendors and business partners

HIPAA-SECURITY

- **164.312(d)** — Person or Entity Authentication
- **164.312(a)(1)** — Access Control

NIST-CSF-2

- **GV.SC-01** — Cybersecurity supply chain risk management program
- **DE.CM-01** — Networks and network services are monitored

ISO-27001-2022

- **A.5.21** — Managing information security in the ICT supply chain

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1059	Command and Scripting Interpreter	Execution
T1571	Non-Standard Port	Command-And-Control
T1016	System Network Configuration Discovery	Discovery
T1090.002	External Proxy	Command-And-Control
T1036	Masquerading	Defense-Evasion
T1071.001	Web Protocols	Command-And-Control
T1195.002	Compromise Software Supply Chain	Initial-Access
T1102	Web Service	Command-And-Control
T1496	Resource Hijacking	Impact

Sources

Source	URL	Tier
Security News	https://thehackernews.com/2026/06/free-apps-are-quietly-turning-sma...	T3
Smart TV | Samsung TV Apps | Samsung US	https://www.samsung.com/us/tvs/smart-tv/samsung-tv-apps/	T3

Source	URL	Tier
Your smart TV may be crawling the web for AI - The Verge	https://www.theverge.com/column/885244/smart-tv-web-crawler-ai	T2
Consumer Apps Embedding Bright Data SDK Turn Smart TVs and ...	https://qpulse.quasarcybertech.com/news/3871/consumer-apps-embeddin.. .	T3
Introducing Smart TV SDKs for Roku, Samsung and LG Devices	https://community.brightcove.com/product-updates/introducing-smart-...	T3

Generated 2026-06-06 14:05 UTC by TJS Security Command Center