INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-07-03 06:49 UTC

Popa Botnet Links NASDAQ-Listed NetNut/Alarum Technologies to 2.5M Daily Hijacked Android TV Devices

THREAT CAMPAIGN | **HIGH** | CVSS 7.5

SCC Item ID	SCC-CAM-2026-0615
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Android-based TV boxes (multiple brands); pirated streaming apps including CRICFy, DooFlix, Sprozfy, RTS Tv, Flixoid, CyberFlix, Rapid Streamz, TvMob, HD/OceanStreams; RoboVPN app; NetNut residential proxy platform; Alarum Technologies Ltd (NASDAQ: ALAR); Vo1d botnet ecosystem
Published	2026-07-02T15:27:33
Discovery Source	Rss

Executive Summary

Coordinated research from Lumen Black Lotus Labs, Nokia Deepfield, Synthient, Qurium, and Spur has linked the Popa botnet, a component of the Vo1d Android TV malware ecosystem, to NetNut, a residential proxy service operated by NASDAQ-listed Alarum Technologies (ALAR). According to these researchers, the botnet silently enrolls between 1.5 and 2.5 million consumer Android TV device IP addresses daily as proxy exit nodes without meaningful user consent, routing traffic through approximately 250-300 relay nodes. The hijacked IPs are assessed by researchers to support ad fraud, account takeover, and mass data scraping operations, and this incident is notable because it implicates a publicly traded commercial proxy provider in active botnet infrastructure.

Technical Analysis

Popa is reported to function as a modular plugin component of the broader Vo1d/BADBOX 2.0 Android TV malware ecosystem. No CVE has been assigned; infection relies on trojanized applications and platform misconfiguration rather than a discrete exploitable vulnerability. Identified infection vectors include pirated streaming applications (CRICFy, DooFlix, Sprozfy, RTS Tv, Flixoid, CyberFlix, Rapid Streamz, TvMob, HD/OceanStreams) and the RoboVPN app, distributed via third-party app stores and sideloading on Android TV hardware. Relevant CWEs: CWE-940 (Improper Verification of Source of a Communication Channel), CWE-668

(Exposure of Resource to Wrong Sphere), CWE-284 (Improper Access Control), CWE-506 (Embedded Malicious Code). Mapped MITRE ATT&CK techniques include T1584.005 (Compromise Infrastructure: Botnet), T1090.002 (Proxy: External Proxy), T1071.001 (Application Layer Protocol: Web Protocols), T1105 (Ingress Tool Transfer), T1036.005 (Masquerading: Match Legitimate Name or Location), T1496 (Resource Hijacking), and T1102 (Web Service). Live traffic analysis by multiple independent research organizations provides the primary corroborating evidence linking Popa botnet egress traffic to NetNut infrastructure. No vendor-issued patch exists; remediation centers on application removal and platform hardening. Alarum Technologies has not publicly confirmed the researchers' characterization of the findings; no regulatory action has been publicly announced as of the configuration date of this session.

Action Checklist

1. Step 1: Containment, Block known NetNut residential proxy IP ranges at your perimeter and web application controls if your environment performs IP-reputation-based access decisions; flag or block traffic originating from residential proxy infrastructure associated with Popa egress nodes. Audit any services exposed to the internet that rely on IP reputation for account access or rate limiting, as hijacked residential IPs bypass conventional blocklists (NIST SC-7, Boundary Protection).
2. Step 2: Detection, Review authentication and access logs for anomalous login patterns originating from residential IP ranges, particularly those associated with Android TV device ASNs. Look for behavioral indicators consistent with T1110 (Brute Force) and T1199 (Trusted Relationship abuse): high-velocity login attempts from geographically dispersed residential IPs, account takeover patterns, and scraping signatures in web server logs. Query SIEM for connections to known Popa/Vo1d C2 infrastructure if threat intelligence feeds include those indicators. Cross-reference against Spur, Lumen, or Nokia Deepfield published IOC lists (NIST AU-6, Audit Record Review, Analysis, and Reporting; CIS 8.2, Collect Audit Logs).
3. Step 3: Eradication, For organizations managing Android TV device fleets (digital signage, hospitality, retail): audit sideloaded or third-party-sourced applications; remove any of the named trojanized apps (CRICFy, DooFlix, Sprozfy, RTS Tv, Flixoid, CyberFlix, Rapid Streamz, TvMob, HD/OceanStreams, RoboVPN); enforce application allowlisting restricted to official app store sources. For consumer-facing services: rotate any credentials or API keys potentially exposed via ATO-sourced access. Apply CIS 2.3 (Address Unauthorized Software) and CIS 4.7 (Manage Default Accounts on Enterprise Assets and Software) to Android TV and streaming device inventories.
4. Step 4: Recovery, After removing identified malicious applications, verify device integrity by confirming no persistent plugin components remain (review running processes and scheduled tasks consistent with Vo1d's modular architecture). Monitor post-remediation for resumed proxy enrollment indicators: unexpected outbound connections to known relay node IP ranges, anomalous bandwidth consumption (T1496, Resource Hijacking), or re-emergence of suspicious application processes. Validate that account lockout and MFA controls are functioning for externally exposed services (CIS 6.3, Require MFA for Externally-Exposed Applications; NIST AC-7, Unsuccessful Logon Attempts).
5. Step 5: Post-Incident, Conduct a review of third-party application vetting processes for any Android-based devices in your environment, including digital signage, conferencing hardware, and hospitality endpoints. Evaluate whether residential proxy IP traffic is adequately distinguished from legitimate user traffic in your detection rules. Update threat intelligence subscriptions to include Vo1d/BADBOX 2.0/Popa botnet indicators. Document control gaps against NIST AC-20 (Use of External Systems) and CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), Android TV and

similar IoT-adjacent devices are frequently absent from enterprise asset inventories.

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate immediately to legal and compliance if Step 2 log analysis confirms successful authentications from Popa/NetNut residential proxy IPs against services storing PII, PHI, or payment data — this crosses breach notification thresholds under GDPR Article 33, HIPAA §164.412, or applicable state breach statutes; also escalate if any managed Android TV device is confirmed to be actively relaying traffic as a Vo1d/Popa proxy node, indicating a live compromise of enterprise-controlled infrastructure.
Recovery Notes	After eradicating trojanized applications from managed Android TV devices, maintain elevated monitoring of outbound traffic from all Android-based endpoint segments for a minimum of 30 days — Vo1d's modular plugin architecture allows reinfection via secondary dropper components that may survive app uninstallation if system-level persistence was achieved via rooted firmware paths. Verify that all rotated credentials and API keys from Step 3 show zero usage under the old values by auditing identity provider logs for any authentication events referencing revoked tokens. Do not restore sideloading capability or third-party app store access on Android TV devices until a formal application vetting process with cryptographic signature verification is documented and approved.
Forensic Artifacts	Android TV device ADB process dumps (`adb shell ps -A`) and installed package lists with timestamps (`adb shell dumpsys package`) captured at time of discovery — these reveal Vo1d's background service names, plugin component PIDs, and the sideload install timestamps of trojanized apps such as CRICFy, DooFlix, RoboVPN, and others named in the advisory | Network PCAP from the Android TV device segment showing outbound TCP connections to NetNut/Popa relay node IPs and associated DNS queries — Vo1d enrolls devices as proxy exit nodes, generating sustained outbound connection patterns to NetNut infrastructure on ports consistent with SOCKS5 proxy protocol | Web server and identity provider authentication logs (Event ID 4624/4625 on Windows; `/var/log/auth.log` on Linux) filtered for source IPs resolving to Android TV device ASNs or flagged by Spur as Popa egress nodes — these establish the account takeover or credential stuffing activity routed through hijacked residential IPs | Contents of `/data/data//` and `/data/app/` directories on affected Android TV devices, preserved before uninstallation — Vo1d stores downloaded plugin modules and C2 configuration files in app private storage that are destroyed when the parent APK is removed | Firewall and proxy egress logs showing bandwidth volume per Android TV device IP over the 30 days preceding discovery — Popa's proxy relay function produces an anomalous and sustained outbound bandwidth signature inconsistent with legitimate Android TV viewing behavior, distinguishable from normal streaming traffic patterns

Per-Action IR Details

Step 1: Containment — Block known NetNut residential proxy IP ranges at your perimeter and web application controls if your environment performs IP-reputation-based access decisions; flag or block traffic originating from residential proxy infrastructure associated with Popa egress nodes. Audit any services exposed to the internet that rely on IP reputation for account access or rate limiting, as hijacked residential IPs bypass conventional blocklists (NIST AC-4 — Information Flow Enforcement).

NIST Phase: Containment
Reference: NIST 800-61r3 §3.3 — Containment Strategy

Controls: NIST AC-4 (Information Flow Enforcement), CIS 4.4 (Implement and Manage a Firewall on Servers)

Compensating: Pull NetNut/Alarum ASN prefixes from Spur's free tier or BGP data (e.g., AS396507 and affiliated NetNut ASNs) and insert deny rules via iptables or Windows Firewall: `iptables -A INPUT -s -j DROP`. For web apps behind nginx, add `deny ;` blocks in the geo/access control stanza. Use the Spur Community feed or Nokia Deepfield published Popa egress CIDR lists as your blocklist source; review and update weekly as residential proxy IP pools rotate rapidly.

Evidence: Before implementing perimeter blocks, capture a full `netstat -ano` (Windows) or `ss -tunap` (Linux) snapshot and export active firewall connection-state tables to document any live sessions already transiting NetNut/Popa egress nodes into your environment. Preserve web server access logs (Apache: `/var/log/apache2/access.log`; nginx: `/var/log/nginx/access.log`) with originating IP, User-Agent, and timestamp fields intact — these are volatile if log rotation is imminent. Tag and archive before block rules are applied, as blocking will stop new entries but not preserve existing ones.

Step 2: Detection — Review authentication and access logs for anomalous login patterns originating from residential IP ranges, particularly those associated with Android TV device ASNs. Look for behavioral indicators consistent with T1110 (Brute Force) and T1199 (Trusted Relationship abuse): high-velocity login attempts from geographically dispersed residential IPs, account takeover patterns, and scraping signatures in web server logs. Query SIEM for connections to known Popa/Vo1d C2 infrastructure if threat intelligence feeds include those indicators. Cross-reference against Spur, Lumen, or Nokia Deepfield published IOC lists (NIST AU-6 — Audit Record Review, Analysis, and Reporting; CIS 8.2 — Collect Audit Logs).

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis

Controls: NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 8.2 (Collect Audit Logs)

Compensating: Without a SIEM, run this PowerShell one-liner against Windows Security Event Log to surface high-velocity residential-IP login failures: `Get-WinEvent -LogName Security | Where-Object {$_.Id -eq 4625} | Group-Object {$_.Properties[19].Value} | Where-Object {$_.Count -gt 20} | Sort-Object Count -Descending`. For Linux SSH, parse `/var/log/auth.log` with: `awk '/Failed password/{print $11}' /var/log/auth.log | sort | uniq -c | sort -rn | head -30`. Cross-reference output IPs against the Spur free residential proxy dataset or Lumen Black Lotus Labs published Popa/Vo1d IOC lists to identify botnet-sourced credential stuffing attempts specifically routed through hijacked Android TV device IPs.

Evidence: Capture and preserve the following before any account lockout or session termination actions: (1) Raw authentication logs — Windows Security Event Log Event ID 4624 (successful logon) and 4625 (failed logon) with source IP and logon type fields; Linux `/var/log/auth.log` or `/var/log/secure`; (2) Web application access logs filtered for POST requests to `/login`, `/api/auth`, or equivalent endpoints showing >10 attempts per IP per minute from geographically dispersed sources; (3) Current active session list from your identity provider or application layer before any forced logout is triggered. These records establish whether Popa-proxied IPs achieved successful account compromise and are required for breach notification threshold assessment.

Step 3: Eradication — For organizations managing Android TV device fleets (digital signage, hospitality, retail): audit sideloaded or third-party-sourced applications; remove any of the named trojanized apps (CRICFy, DooFlix, Sprozfy, RTS Tv, Flixoid, CyberFlix, Rapid Streamz, TvMob, HD/OceanStreams, RoboVPN); enforce application allowlisting restricted to official app store sources. For consumer-facing services: rotate any credentials or API keys potentially exposed via ATO-sourced access. Apply CIS 2.3 (Address Unauthorized Software) and CIS 4.7 (Manage Default Accounts on Enterprise Assets and Software) to Android TV and streaming device inventories.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: CIS 2.3 (Address Unauthorized Software), CIS 4.7 (Manage Default Accounts on Enterprise Assets and Software), NIST AC-6 (Least Privilege)

Compensating: Use Android Debug Bridge (ADB) to enumerate and remove named trojanized packages across managed Android TV devices: `adb shell pm list packages` to inventory, then `adb shell pm uninstall -k --user 0 ` for each identified app. For RoboVPN specifically, query `adb shell dumpsys package com.robovpn.android` (or equivalent package ID) to confirm installation state. After removal, run `adb shell pm list packages -f` to verify no residual APK files remain in `/data/app/`. For credential rotation, prioritize any API keys or service accounts whose access logs show activity correlated with the residential IP ranges identified in Step 2.

Evidence: BEFORE uninstalling any application or rotating credentials, capture on each affected Android TV device: (1) Full running process list via `adb shell ps -A` — Vo1d's modular architecture spawns persistent background services that may not appear in the app drawer; (2) List of all installed packages with install timestamps via `adb shell dumpsys package` — preserves evidence of when trojanized apps were sideloaded; (3) Network connection state via `adb shell netstat` or `adb shell cat /proc/net/tcp` to document active C2 connections at time of eradication; (4) Contents of `/data/data//` directories where Vo1d stores plugin components and configuration — these directories are destroyed upon uninstall. Preserve these artifacts before any removal action.

Step 4: Recovery — After removing identified malicious applications, verify device integrity by confirming no persistent plugin components remain (review running processes and scheduled tasks consistent with Vo1d's modular architecture). Monitor post-remediation for resumed proxy enrollment indicators: unexpected outbound connections to known relay node IP ranges, anomalous bandwidth consumption (T1496 — Resource Hijacking), or re-emergence of suspicious application processes. Validate that account lockout and MFA controls are functioning for externally exposed services (CIS 6.3 — Require MFA for Externally-Exposed Applications; NIST AC-7 — Unsuccessful Logon Attempts).

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: CIS 6.3 (Require MFA for Externally-Exposed Applications), NIST AC-7 (Unsuccessful Logon Attempts), CIS 4.6 (Securely Manage Enterprise Assets and Software)

Compensating: Establish a post-remediation monitoring baseline on Android TV devices using a cron job that runs every 15 minutes: `adb shell ps -A | grep -Ev '(system|root|shell)' > /tmp/proc_snapshot_$(date +%s).txt` and diffs against the clean post-remediation snapshot. For bandwidth anomaly detection without NDR tooling, deploy `vnstat` on the network segment hosting Android TV devices and alert on daily egress exceeding 500MB per device — Vo1d proxy nodes generate sustained outbound traffic characteristic of relay activity. For MFA validation, manually test lockout thresholds by attempting >5 failed logins against a test account on each externally exposed application and confirm lockout triggers per AC-7 policy.

Evidence: Before declaring recovery complete, capture a final clean-state snapshot: (1) `adb shell ps -A` output confirming no Vo1d-associated service names or PIDs are running; (2) `adb shell dumpsys activity services` to verify no background services associated with removed packages persist via Android service restart mechanisms; (3) Outbound network traffic sample via `tcpdump -i -w post_remediation_$(date +%s).pcap` on the Android TV network segment for a 30-minute window — examine for any connections to Popa/Vo1d C2 infrastructure or NetNut relay nodes that would indicate re-enrollment. Retain these artifacts for the post-incident review and to demonstrate eradication completeness.

Step 5: Post-Incident — Conduct a review of third-party application vetting processes for any Android-based devices in your environment, including digital signage, conferencing hardware, and hospitality endpoints. Evaluate whether residential proxy IP traffic is adequately distinguished from legitimate user traffic in your detection rules. Update threat intelligence subscriptions to include Vo1d/BADBOX 2.0/Popa botnet indicators. Document control gaps against NIST AC-20 (Use of External Systems) and CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory) — Android TV and similar IoT-adjacent devices are frequently absent from enterprise asset inventories.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity

Controls: NIST AC-20 (Use of External Systems), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 2.1 (Establish and Maintain a Software Inventory), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Conduct an ADB-based asset discovery sweep across all network segments that could host Android TV devices: use `nmap -p 5555 --open` to identify devices with ADB exposed, then `adb connect :5555 && adb shell getprop ro.product.model` to enumerate device make/model and add to asset inventory. Build a Sigma detection rule targeting residential proxy ASN login patterns using the free Sigma rule format and convert for your log platform via `sigmac`; base the ASN list on Spur's published NetNut/Popa-affiliated ranges. Schedule a quarterly review of the Lumen Black Lotus Labs, Nokia Deepfield, and Spur threat intelligence blogs for updated Vo1d/BADBOX 2.0 IOC releases.

Evidence: For the lessons-learned record, compile: (1) The full timeline from first Popa-proxied login attempt (from Step 2 log review) to containment, documenting dwell time; (2) Complete inventory of Android TV devices found in the environment versus those previously documented — the delta represents the asset inventory gap attributable to AC-20 and CIS 1.1 failures; (3) A list of any accounts or API keys confirmed or suspected to have been accessed via Popa-proxied IPs during the incident window, to support breach notification assessment if PII was accessible to those accounts. These records are required inputs for the lessons-learned meeting and for updating detection rules to recognize Vo1d re-enrollment patterns in future monitoring.

Detection Guidance

Detection focuses on three surfaces: (1) Outbound from managed Android TV or streaming devices, monitor for anomalous outbound connections to unfamiliar relay infrastructure, sustained high-bandwidth egress, or connections on non-standard ports inconsistent with legitimate streaming traffic; correlate with D3-LAM (Local Account Monitoring) and D3-SFA (System File Analysis) on managed device fleets. (2) Inbound to externally exposed services, query authentication logs for login attempts originating from residential ASNs at volumes or velocities inconsistent with normal user behavior; flag accounts accessed from geographically implausible IP sequences within short time windows (consistent with T1110 Brute Force and T1090.002 External Proxy). (3) Network-level, if your organization subscribes to Spur, Lumen Black Lotus Labs, or Nokia Deepfield threat intelligence feeds, import published Popa/Vo1d C2 and relay node indicators and apply them to firewall and IDS rules. Behavioral indicators include: unexpected plugin or APK downloads to Android TV devices (T1105, Ingress Tool Transfer), processes masquerading as system components (T1036.005), and sustained outbound proxy relay traffic (T1584.005). No specific CVE-based detection signatures apply; focus is behavioral and IOC-driven.

Indicators of Compromise

Type	Value	Context	Confidence
DOMAIN	`No specific IOCs disclosed in available source material`	Lumen Black Lotus Labs, Nokia Deepfield, Spur, and Qurium have published research linking Popa egress traffic to NetNut infrastructure; consult their published advisories directly for current indicator lists. Available source URLs do not surface discrete IOC values.	LOW

Framework Mappings

MITRE-ATTACK

- **T1110** — Brute Force
- **T1036.005** — Match Legitimate Resource Name or Location
- **T1199** — Trusted Relationship
- **T1105** — Ingress Tool Transfer
- **T1584.005** — Botnet
- **T1059.004** — Unix Shell
- **T1583.008** — Malvertising
- **T1190** — Exploit Public-Facing Application
- **T1071.001** — Web Protocols
- **T1090.002** — External Proxy
- **T1496** — Resource Hijacking
- **T1102** — Web Service

NIST-800-53R5

- **AC-7** — Unsuccessful Logon Attempts
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **CM-7** — Least Functionality
- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SI-2** — Flaw Remediation
- **SI-7** — Software, Firmware, and Information Integrity
- **AC-3** — Access Enforcement
- **AT-2** — Literacy Training and Awareness
- **SR-2** — Supply Chain Risk Management Plan

OWASP-TOP10-2021

- **A01:2021** — Broken Access Control

CIS-V8

- **6.1** — Establish an Access Granting Process
- **6.2** — Establish an Access Revoking Process
- **14.2** — Train Workforce Members to Recognize Social Engineering Attacks

- **15.1** — Establish and Maintain an Inventory of Service Providers

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(a)(1)** — Access Control

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities
- **A.5.21** — Managing information security in the ICT supply chain

NIST-CSF-2

- **GV.SC-01** — Cybersecurity supply chain risk management program

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1110	Brute Force	Credential-Access
T1036.005	Match Legitimate Resource Name or Location	Defense-Evasion
T1199	Trusted Relationship	Initial-Access
T1105	Ingress Tool Transfer	Command-And-Control
T1584.005	Botnet	Resource-Development
T1059.004	Unix Shell	Execution
T1583.008	Malvertising	Resource-Development
T1190	Exploit Public-Facing Application	Initial-Access
T1071.001	Web Protocols	Command-And-Control
T1090.002	External Proxy	Command-And-Control
T1496	Resource Hijacking	Impact
T1102	Web Service	Command-And-Control

Sources

Source	URL	Tier
Security News	https://krebsonsecurity.com/2026/06/popa-botnet-linked-to-publicly-...	T2
Vo1d botnet - Krebs on Security	https://krebsonsecurity.com/tag/vo1d-botnet/	T2
Security Researchers Link 'Popa' Botnet to Israeli Proxy Provider ...	https://www.wespeakiot.com/security-researchers-link-popa-botnet-to...	T3
WDTC Center for Cybersecurity | News and Events	https://www.wdt.edu/about/center-for-cybersecurity-education/news-e...	T1
BADBOX 2.0 and Vo1d Botnets: Android TV Streaming Box ...	https://www.rescana.com/post/badbox-2-0-and-vo1d-botnets-android-tv...	T3

Generated 2026-07-03 06:49 UTC by TJS Security Command Center