INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-21 18:39 UTC

# AryStinger Botnet Exploits End-of-Life D-Link Routers as Distributed Attack Infrastructure

**THREAT CAMPAIGN** | **HIGH** | CVSS 7.5

| | |
|---|---|
| **SCC Item ID** | SCC-CAM-2026-0529 |
| **Type** | Threat Campaign |
| **CVE ID** | CVE-2013-3307, CVE-2016-5681, CVE-2025-11837 |
| **Severity** | HIGH |
| **CVSS Base Score** | 7.5 |
| **EPSS Score** | 0.0562 (92th percentile) |
| **Affected Products** | D-Link DIR-850L, D-Link DIR-818LW (end-of-life routers); unspecified D-Link NAS devices |
| **Published** | 2026-06-21T10:14:22 |
| **Discovery Source** | Rss |

## Executive Summary

A botnet named AryStinger has compromised more than 4,000 end-of-life D-Link routers, converting them into attacker-controlled proxies used for distributed scanning, DNS hijacking, and traffic interception. Affected devices, including the DIR-850L and DIR-818LW, will never receive security patches from D-Link because they are no longer supported, making firmware remediation impossible. Organizations and consumers still running these models face permanent, unmitigable network exposure unless the hardware is replaced.

## Technical Analysis

AryStinger exploits three CVEs to compromise end-of-life D-Link hardware: CVE-2013-3307 and CVE-2016-5681 are legacy vulnerabilities with no available patches on affected models; CVE-2025-11837 is a newly identified CVE referenced in XLab Qianxin reporting. Affected models are D-Link DIR-850L and DIR-818LW. A secondary Go-based malware payload targets unspecified D-Link NAS devices, embedding open-source penetration testing tools to extend lateral movement capability. CWE classifications indicate authentication bypass without credentials (CWE-306), hidden or unsupported functionality (CWE-912), insecure default settings (CWE-1188), and OS command injection (CWE-78). MITRE ATT&CK techniques include T1190 (Exploit Public-Facing Application), T1046 (Network Service Discovery), T1557 (Adversary-in-the-Middle), T1090.002 (External Proxy), T1565.002 (Transmitted Data Manipulation), T1059 (Command and Scripting Interpreter), T1071.001 (Web Protocols C2), T1595.001 (Active Scanning, IP Block), T1584.008 (Compromised

Botnet Infrastructure), and T1583.005 (Botnet acquisition). EPSS score of 0.056 places this at the 91.9th percentile for exploitation likelihood. No CISA KEV listing as of configuration date. Threat actor is unattributed. Sources: XLab Qianxin blog and BleepingComputer reporting.

## Action Checklist

1. Step 1: Containment. Immediately identify all D-Link DIR-850L and DIR-818LW routers and unspecified D-Link NAS devices in your environment using asset inventory. Isolate any confirmed end-of-life D-Link devices from the network perimeter. Block outbound traffic from these devices to unknown external IPs at the firewall pending replacement.
2. Step 2: Detection. Query firewall and DNS resolver logs for anomalous outbound DNS resolution patterns and unexpected DNS server changes originating from D-Link device IPs. Look for high-volume outbound scanning traffic (T1595.001) and unusual proxy relay connections (T1090.002). Review DHCP logs for DNS hijacking indicators, client-reported DNS servers that differ from assigned servers. Check NAS device logs for Go-based process execution or presence of open-source penetration testing binaries. Monitor for C2 beaconing over HTTP/HTTPS (T1071.001) from router management IPs.
3. Step 3: Eradication. No firmware patch exists or will be issued for end-of-life DIR-850L, DIR-818LW, or affected NAS models. The only eradication path is hardware replacement with a supported device. For NAS devices, perform full factory reset and audit for unauthorized binaries before redeployment. Reset all credentials that may have traversed the compromised network segment. Update DNS settings on all clients that used a potentially hijacked resolver.
4. Step 4: Recovery. After hardware replacement, verify DNS resolution is operating correctly for all network clients. Confirm no residual C2 traffic is leaving the network segment. Audit downstream systems for signs of lateral movement originating from the compromised router or NAS. Re-enable network monitoring baselines and confirm log integrity for the affected segment. Validate multi-factor authentication is enforced on all remote access paths that traversed the affected infrastructure.
5. Step 5: Post-Incident. This campaign exposes a systematic gap: end-of-life network devices remaining in production without a hardware refresh cycle. Implement a formal asset lifecycle policy requiring decommission timelines for hardware approaching or past vendor end-of-support dates. Establish a vulnerability management process that flags EOL assets as unmitigable-risk items requiring escalation. Review whether perimeter devices are included in the software inventory and patch management processes.

## IR / Forensic Enrichment

| | |
|---|---|
| **Triage Priority** | IMMEDIATE |
| **Escalation Criteria** | Escalate immediately to senior IR leadership and legal/compliance if any client system transmitted authentication credentials, PII, or PHI through a DNS-hijacked resolver served by a compromised D-Link device, as this constitutes a data-interception event that may trigger breach notification obligations under HIPAA, GDPR, or applicable state privacy law; additionally escalate if AryStinger lateral movement indicators are detected on internal hosts beyond the router/NAS segment, or if the organization lacks the asset inventory visibility to confirm the full scope of affected EOL D-Link devices within 4 hours. |

| | |
|---|---|
| **Recovery Notes** | After replacing affected DIR-850L, DIR-818LW, and NAS hardware, maintain elevated DNS monitoring on the replacement gateway for a minimum of 30 days — AryStinger's DNS hijacking capability means downstream clients may have cached malicious resolver assignments or had DNS-delivered payloads staged before containment. Audit all remote-access VPN and administrative sessions that passed through the compromised segment during the estimated infection window, treating any credentials used over that path as rotated-but-suspect until downstream systems confirm no unauthorized access. Verify replacement device firmware is current at deployment and enrolled in the vendor's security advisory notification system to prevent recurrence of an unmonitored EOL condition. |
| **Forensic Artifacts** | D-Link NAS /tmp and /var/packages directory listings: AryStinger drops Go-compiled malware binaries and open-source scanning tools (Masscan, fscan) in world-writable temp directories on compromised NAS devices — file timestamps and ELF binary headers identify the dropper and implant versions \| Firewall/NAT session logs filtered on DIR-850L and DIR-818LW management IPs: high-frequency outbound connections to non-RFC1918 addresses on port 53 (DNS hijacking relay) and sequential /16 or /24 sweeps on port 80/443/22/23 (AryStinger distributed scanning behavior exploiting the router as a proxy node) are the primary network-layer indicators \| DHCP server Option 6 (DNS Server) assignment history: records which clients received DNS server addresses controlled by the AryStinger-hijacked D-Link router, establishing the scope of DNS interception and identifying all systems whose DNS queries may have been observed or manipulated by the threat actor \| DNS resolver cache dump from internal resolvers and client workstations: malicious or unexpected PTR/A record resolutions cached during the compromise window — particularly lookups for internal hostnames resolved through the hijacked D-Link DNS relay — may reveal reconnaissance targeting or credential-capture redirection \| NAS device syslog (/var/log/messages or equivalent) and process accounting records: unauthorized admin panel access attempts leveraging CVE-2013-3307 (remote code execution via malformed HNAP request) or CVE-2016-5681 (UPnP stack buffer overflow) will appear as malformed HTTP POST requests to /HNAP1/ or UPnP SOAP endpoints in the web server access log prior to the Go implant execution |

### Per-Action IR Details

**Step 1: Containment — Immediately identify all D-Link DIR-850L and DIR-818LW routers and unspecified D-Link NAS devices in your environment using asset inventory (CIS 1.1). Isolate any confirmed end-of-life D-Link devices from the network perimeter. Block outbound traffic from these devices to unknown external IPs at the firewall pending replacement (CIS 4.4).**

**NIST Phase:** Containment

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

**Controls:** CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 4.4 (Implement and Manage a Firewall on Servers), NIST AC-4 (Information Flow Enforcement)

**Compensating:** Run an ARP scan or nmap fingerprint sweep (`nmap -O --osscan-guess 192.168.x.0/24`) to identify D-Link OUI prefixes (1C:7E:E5, B0:C5:54, 14:D6:4D) on the wire. Cross-reference MAC OUI against the D-Link vendor list offline. For immediate egress blocking without enterprise firewall management, apply host-level ACLs on the upstream switch using port isolation or a VLAN quarantine PVLAN — achievable with a managed switch CLI in under 10 minutes.

**Evidence:** Before isolating any device, capture: (1) active ARP table from the upstream gateway (`arp -a` or `show arp` on the switch) to map device-to-IP/MAC bindings; (2) current firewall/NAT session table showing active outbound connections from DIR-850L/DIR-818LW management IPs, specifically noting any sessions to non-RFC1918 destinations on ports 80, 443, 23, or 53; (3) DHCP lease table identifying all clients that received a DNS server assignment from a potentially hijacked D-Link device. These are volatile — session state is lost the moment the device

is isolated or power-cycled.

**Step 2: Detection — Query firewall and DNS resolver logs for anomalous outbound DNS resolution patterns and unexpected DNS server changes originating from D-Link device IPs. Look for high-volume outbound scanning traffic (T1595.001) and unusual proxy relay connections (T1090.002). Review DHCP logs for DNS hijacking indicators — client-reported DNS servers that differ from assigned servers. Check NAS device logs for Go-based process execution or presence of open-source penetration testing binaries (D3-SFA system file analysis). Monitor for C2 beaconing over HTTP/HTTPS (T1071.001) from router management IPs.**

**NIST Phase:** Detection Analysis

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

**Controls:** NIST AU-2 (Event Logging), NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 8.2 (Collect Audit Logs)

**Compensating:** Without a SIEM, use the following targeted queries: (1) On pfSense/OPNsense, filter firewall logs by source IP matching DIR-850L/DIR-818LW management addresses and destination port 53 to catch DNS redirection attempts — `grep '' /var/log/filter.log | grep ':53'`; (2) Run `tcpdump -i eth0 -nn 'src host and port 53' -w arystinger_dns.pcap` on the upstream gateway for 30 minutes to capture DNS hijacking traffic; (3) For NAS devices, pull `/var/log/messages` or equivalent syslog and grep for unexpected process names with Go runtime signatures (`grep -E '(goroutine|go build)' /var/log/messages`); (4) Use Wireshark display filter `dns.qry.name and ip.src == ` on the captured pcap to identify anomalous resolver behavior consistent with AryStinger C2 DNS patterns.

**Evidence:** This is a detection step that does not alter live state — no volatile pre-capture is required before querying logs. However, document and preserve: (1) DNS resolver cache contents from any internal resolver that received queries relayed through the D-Link device (`rndc dumpdb -cache` for BIND, or `ipconfig /displaydns` on Windows clients); (2) NetFlow or firewall session logs showing high-frequency outbound connections on port 53 or scanning bursts (>100 unique destination IPs per minute) from D-Link device IPs, which would indicate AryStinger's distributed scanning role; (3) DHCP server logs showing Option 6 (DNS Server) fields delivered to clients — compare against authorized DNS server list to identify hijacked resolver assignments.

**Step 3: Eradication — No firmware patch exists or will be issued for end-of-life DIR-850L, DIR-818LW, or affected NAS models. The only eradication path is hardware replacement with a supported device. For NAS devices, perform full factory reset and audit for unauthorized binaries before redeployment. Reset all credentials that may have traversed the compromised network segment (D3-CRO credential rotation). Update DNS settings on all clients that used a potentially hijacked resolver.**

**NIST Phase:** Eradication

**Reference:** NIST 800-61r3 §3.4 — Eradication

**Controls:** CIS 4.7 (Manage Default Accounts on Enterprise Assets and Software), CIS 5.2 (Use Unique Passwords), NIST AC-2 (Account Management)

**Compensating:** Before factory-resetting any D-Link NAS, image the device storage if possible: attach the NAS drive to a forensic workstation and run `dd if=/dev/sdX of=nas_image.dd bs=4M status=progress` for binary preservation. Enumerate suspicious files with `find / -newer /etc/passwd -type f -exec file {} \; | grep -i ELF` to identify Go-compiled binaries dropped by AryStinger. For credential rotation without enterprise PAM tooling, generate a forced password reset list from Active Directory (`Get-ADUser -Filter * -Properties PasswordLastSet | Where-Object {$_.Enabled -eq $true}`) and prioritize accounts that authenticated through the compromised segment's proxy path. Push DNS server override to all DHCP clients by updating the DHCP scope options immediately after hardware replacement.

**Evidence:** Before factory-resetting the NAS or rotating credentials, capture: (1) Full directory listing of `/var/packages`, `/usr/local/bin`, and `/tmp` on the NAS via SSH — AryStinger drops Go-compiled binaries and open-source pentest tools (e.g., Masscan, fscan) in these locations; (2) Running process list from the NAS (`ps aux` or equivalent) before power-cycle or reset — Go-based malware processes will appear with generic names or numeric PIDs without associated package entries; (3) Network connection state from the NAS (`netstat -antp` or `ss -tulnp`) showing active C2 connections — critical volatile evidence lost on reset; (4) Any local syslog or `/var/log/auth.log` entries showing unauthorized SSH or admin panel access leveraging CVE-2013-3307 (remote code execution via malformed request) or CVE-2016-5681 (stack buffer overflow in UPnP). These must be preserved before the device is wiped.

**Step 4: Recovery — After hardware replacement, verify DNS resolution is operating correctly for all network clients. Confirm no residual C2 traffic is leaving the network segment. Audit downstream systems for signs of lateral movement originating from the compromised router or NAS. Re-enable network monitoring baselines (NIST AU-6) and confirm log integrity for the affected segment. Validate MFA is enforced on all remote access paths that traversed the affected infrastructure (CIS 6.4, D3-MFA).**

**NIST Phase:** Recovery

**Reference:** NIST 800-61r3 §3.5 — Recovery

**Controls:** NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 6.4 (Require MFA for Remote Network Access), CIS 6.3 (Require MFA for Externally-Exposed Applications)

**Compensating:** For DNS verification without enterprise monitoring tooling: run `nslookup google.com ` from multiple client segments and confirm responses match authoritative resolver output — any discrepancy indicates residual DNS poisoning or misconfiguration. For C2 traffic validation, run a 24-hour `tcpdump -i -nn 'not src net 10.0.0.0/8 and not src net 192.168.0.0/16' -w post_recovery.pcap` on the replacement gateway and analyze with `tshark -r post_recovery.pcap -qz endpoints,ip` to identify any unexpected external communication patterns. For lateral movement detection on Windows downstream hosts, query the Security Event Log for Event ID 4624 (Logon) with Logon Type 3 (Network) sourced from the former router/NAS IP addresses during the compromise window.

**Evidence:** Recovery verification is not a live-state-altering step, but confirm before closing the incident: (1) DNS resolution test results from all client VLANs documenting that Option 6 DHCP entries now point to authorized resolvers only; (2) Firewall session log snapshot from the replacement device showing zero outbound connections to the external IPs identified during Detection (Step 2) as AryStinger C2 or scanning destinations; (3) Authentication logs from downstream systems (Windows Event ID 4624/4625, Linux `/var/log/auth.log`) filtered for source addresses matching the former D-Link device IPs, covering the full compromise window to identify any credential-relay or pass-through authentication that AryStinger may have facilitated as a proxy.

**Step 5: Post-Incident — This campaign exposes a systematic gap: end-of-life network devices remaining in production without a hardware refresh cycle. Implement a formal asset lifecycle policy requiring decommission timelines for hardware approaching or past vendor end-of-support dates (CIS 1.1, CIS 2.2). Establish a vulnerability management process that flags EOL assets as unmitigable-risk items requiring escalation (CIS 7.1). Review whether perimeter devices are included in the software inventory and patch management processes (CIS 2.1, CIS 7.3).**

**NIST Phase:** Post Incident

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

**Controls:** CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 2.1 (Establish and Maintain a Software Inventory), CIS 2.2 (Ensure Authorized Software is Currently Supported), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.3 (Perform Automated Operating System Patch Management)

**Compensating:** For a 2-person team, build a lightweight EOL tracking spreadsheet seeded from D-Link's published end-of-support list (publicly available on the D-Link support portal) and cross-reference against the asset inventory MAC OUI scan results from Step 1. Set a calendar-triggered quarterly review. For automated EOL flagging without enterprise tooling, configure a free Shodan Monitor alert for your external IP ranges filtered on D-Link device banners — this catches EOL devices with internet-exposed management interfaces before threat actors do. Use the CISA Known Exploited Vulnerabilities (KEV) catalog as a standing query source: CVE-2013-3307, CVE-2016-5681, and CVE-2025-11837 are candidates for KEV listing given active AryStinger exploitation.

**Evidence:** Post-incident documentation to preserve for lessons learned and potential regulatory reporting: (1) Full timeline of device compromise window reconstructed from firewall session logs and DHCP lease history, establishing when AryStinger-controlled DNS hijacking began; (2) List of all client IPs that received DNS assignments from the compromised D-Link device, for downstream breach impact scoping — particularly relevant if those clients transmitted credentials or PII through the hijacked resolver; (3) Inventory delta report showing EOL D-Link devices identified versus what was previously documented in asset inventory, quantifying the visibility gap that enabled AryStinger persistence; (4) Preserved binary samples or process names recovered from NAS devices (Step 3) for submission to internal threat intel or sharing via ISACs relevant to your sector.

## Detection Guidance

Primary detection focus is DNS hijacking and anomalous outbound proxy traffic from router management IPs. Query DNS resolver logs for responses returning unexpected authoritative servers, compare resolved DNS server IPs against configured upstream resolvers. Look for high-rate outbound SYN packets or ICMP sweeps from router source IPs (T1595.001 active scanning). In firewall logs, filter for traffic where the source is a D-Link device IP routing to external IPs on non-standard ports, particularly associated with known botnet C2 infrastructure patterns. For NAS devices, audit running processes and installed binaries for Go-compiled executables or known open-source pentesting tool names (nmap, masscan, sqlmap, etc.) that have no legitimate justification. Behavioral indicator: clients reporting DNS resolution failures or unexpected redirects while upstream connectivity appears healthy may indicate active DNS hijacking. If SIEM is available, build a rule correlating DNS server changes on client DHCP leases with the timeframe of any D-Link device joining the network. Monitor XLab Qianxin and BleepingComputer for IOC releases as they become available.

## Indicators of Compromise

| Type | Value | Context | Confidence |
|---|---|---|---|
| DOMAIN | `blog.xlab.qianxin.com/arystinger-botnet-hijacks-legacy-routers-for-global-attacks-en/` | Primary technical analysis source — XLab Qianxin AryStinger campaign report | MEDIUM |

## Framework Mappings

### MITRE-ATTACK

- **T1565.002** — Transmitted Data Manipulation
- **T1584.008** — Network Devices
- **T1046** — Network Service Discovery
- **T1190** — Exploit Public-Facing Application
- **T1071.001** — Web Protocols
- **T1090.002** — External Proxy
- **T1557** — Adversary-in-the-Middle
- **T1059** — Command and Scripting Interpreter
- **T1595.001** — Scanning IP Blocks
- **T1583.005** — Botnet

### NIST-800-53R5

- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SC-7** — Boundary Protection
- **SI-2** — Flaw Remediation

- **SI-7** — Software, Firmware, and Information Integrity
- **CM-7** — Least Functionality
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **IA-2** — Identification and Authentication (Organizational Users)
- **SI-10** — Information Input Validation

### OWASP-TOP10-2021

- **A07:2021** — Identification and Authentication Failures
- **A03:2021** — Injection

### CIS-V8

- **6.3** — Require MFA for Externally-Exposed Applications
- **2.5** — Allowlist Authorized Software
- **16.10** — Apply Secure Design Principles in Application Architectures
- **7.3** — Perform Automated Operating System Patch Management
- **7.4** — Perform Automated Application Patch Management

### ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities

## MITRE ATT&CK Mapping

| Technique ID | Technique Name | Tactic |
|---|---|---|
| T1565.002 | Transmitted Data Manipulation | Impact |
| T1584.008 | Network Devices | Resource-Development |
| T1046 | Network Service Discovery | Discovery |
| T1190 | Exploit Public-Facing Application | Initial-Access |
| T1071.001 | Web Protocols | Command-And-Control |
| T1090.002 | External Proxy | Command-And-Control |
| T1557 | Adversary-in-the-Middle | Credential-Access |
| T1059 | Command and Scripting Interpreter | Execution |
| T1595.001 | Scanning IP Blocks | Reconnaissance |
| T1583.005 | Botnet | Resource-Development |

## Sources

| Source | URL | Tier |
|---|---|---|
| **Security News** | https://www.bleepingcomputer.com/news/security/arystinger-botnet-in... | T3 |
| **CVE-2025-9357 Detail - NVD** | https://nvd.nist.gov/vuln/detail/cve-2025-9357 | T1 |
| **CVE-2025-9357: Linksys RE6250 Buffer Overflow Vulnerability** | https://www.sentinelone.com/vulnerability-database/cve-2025-9357/ | T3 |
| **Linksys RE Series Stack Buffer Overflow (CVE-2025-8817) - ZeroPath** | https://zeropath.com/blog/cve-2025-8817-linksys-stack-buffer-overflow | T3 |
| **More Than 4,000 Legacy Routers Compromised by AryStinger ...** | https://blog.xlab.qianxin.com/arystinger-botnet-hijacks-legacy-rout... | T3 |
| **NVD** | https://nvd.nist.gov/vuln/detail/CVE-2013-3307, CVE-2016-5681, CVE-... | T1 |



Generated 2026-06-21 18:39 UTC by TJS Security Command Center