GitHub - jrm360seclab/aodin-vo1d-malware: AODIN X1BQ projector ships with Vo1d botnet malware - security disclosure

By jrm360seclab

Archived: 2026-04-05 19:33:42 UTC

Public Security Disclosure | February 2026

⚠️ Warning to Amazon Buyers

If you purchased an **AODIN X1BQ projector** (Amazon ASIN: **B0DGX51JPC**), your device may be **pre-infected with Vo1d botnet malware** installed at the factory before you ever received it.

The device streams video perfectly with zero visible symptoms. The malware can only be detected with enterprise-grade network monitoring tools. **The average consumer has no way to know their device is infected.**

Summary

Field	Detail
Device	AODIN X1BQ Smart Projector
Amazon ASIN	B0DGX51JPC
Purchase Date	December 7, 2025
Malware Family	Vo1d Botnet (residential proxy variant)
Firmware	projector.20250910.101755
Firmware Date	September 10, 2025 — pre-infected at factory
OS	LuminaOS (Android fork)
Detection Date	February 2026
Time Undetected	2+ months of active daily use
Independent Verification	VirusTotal 11/93 · ThreatYeti 9.2/10

What Is Vo1d?

Vo1d is a botnet that infects Android-based devices at the firmware or supply chain level. Once active, it silently enrolls the device as a **residential proxy node** — routing criminal internet traffic through the victim's home IP address without their knowledge or consent.

The original Vo1d research was published by QiAnXin X-Lab. This disclosure documents a **new delivery vector**: factory pre-infection of consumer projectors sold on Amazon.

What criminal operators can do with your infected device:

- Route their traffic through your home IP address (your IP gets flagged for abuse, not theirs)
- Sell access to your residential IP to other criminal actors
- Conduct fraud, credential stuffing, or scraping that traces back to you legally
- Maintain persistent remote access to a device inside your home network

---

How It Was Discovered

The device was used daily for streaming (Netflix, Hulu, Amazon Prime, Peacock) for **over two months** with zero visible symptoms. No alert fired. No automated system flagged anything. The malware was completely invisible.

Discovery came through **proactive threat hunting** — not an automated alert. As part of learning network security, a manual packet capture was performed on the home network with no specific lead and no prior suspicion of the projector. While reviewing the captured traffic by hand, two patterns stood out:

1. **A consumer projector was generating DNS queries on a precise ~65-second cycle** — machine-perfect timing that no human activity produces. The domain: `.o.fecebbbk[.xyz]`, designed to look like `.o.facebook.[com]` at a quick glance
2. **The same device was sending traffic to an AWS IP address** (44[.]205[.]227[.]254) with no user interaction

No IDS rule triggered this. No firewall alert fired. **The malware was found because I was looking** — manually reviewing raw traffic with enough pattern recognition to notice that a projector had no business querying the same domain every 65 seconds.

This is the core value of threat hunting: finding what automated systems miss. This malware had evaded detection for over two months on a network with OPNsense and Security Onion deployed. Human analysis found it in a single manual capture session.

The home lab tools used for investigation once the hunt began:

- **OPNsense** — firewall with full traffic logging for deep-dive analysis
- **Security Onion** — IDS/IPS for correlation and additional capture
- **Wireshark** — packet-level protocol analysis
- **RustScan** — active port scanning of the device
- **RapidHostBaseline** -A lightweight Windows host baseline collector for defenders and investigators

---

Technical Findings

Device Identifiers

Identifier	Value
MAC Address	DC:95:07:CC:E0:FF
Firmware Version	projector.20250910.101755
Firmware Build Date	September 10, 2025
Device IMEI	1c001044f6828801f5a
Device UDID	44_SD-627de7eb1f73704e4497f3a6bbd9698c

The firmware build date of **September 10, 2025** pre-dates the December 2025 purchase. This confirms a **supply chain compromise** — the infection was present before the device was sold.

Three-Tier C2 Infrastructure

The malware operates a three-tier command and control system, with each tier serving a distinct purpose:

Tier 1 — Device Registration (Disguised as Firmware Update)

Within **2.17 seconds of powering on** — before any user touches the remote — the device contacts `ota.triplesai.[com]:8080` over HTTP. The traffic mimics a legitimate over-the-air firmware update check, but the payload contains the device's complete fingerprint: MAC address, IMEI, firmware version, and unique device ID.

This registers the device in the botnet operator's inventory. Every infected AODIN device phones home to this server the moment it boots.

Field	Value
Domain	`ota.triplesai.[com]`
IP	111[.]230[.]36[.]129 (Tencent Cloud)
Port	8080
Protocol	HTTP POST
Timing	2.17 seconds after boot

Tier 2 — Proxy Role Assignment

The C2 infrastructure responds to the registration by assigning the device a specific proxy role. The response is a structured data object containing a proxy host and port that the device will use to route criminal traffic through the victim's home internet connection.

Field	Value
Domain	`sd002.jaguar-distributor.syslogcollector.[com]`
IP	38[.]55[.]17[.]113
Port	12000
Protocol	HTTP
VirusTotal	11/93 vendors flag as malicious
ThreatYeti	Risk score 9.2 / 10.0

Tier 3 — Persistent Heartbeat Channel

The most sophisticated component. The device maintains a continuous keep-alive channel to a third C2 server using a **custom binary UDP protocol**. This channel operates 24 hours a day, 7 days a week, regardless of whether anyone is using the projector.

Field	Value
Domain	`.o.fecebbbk[.xyz]` (typosquatting — mimics .o.facebook.[com])
IP	44[.]205p[.]227[.]254 (AWS us-east-1)
Port	16000
Protocol	Custom binary UDP
Beacon interval	Every ~65 seconds

DNS Beaconing — Observed Behavior

The device queries `o.fecebbbk[.xyz]` with programmatic regularity around the clock. Over a 3.5-minute observation window, four queries were captured:

```
 17:55:08  →  DNS query: .o.fecebbbk[.xyz]  resolves to  44[.]205p[.]227[.]254
17:56:15  →  DNS query: .o.fecebbbk[.xyz]  resolves to  44[.]205p[.]227[.]254  (+67 seconds)
17:57:19  →  DNS query: .o.fecebbbk[.xyz]  resolves to  44[.]205p[.]227[.]254  (+64 seconds)
17:58:27  →  DNS query: .o.fecebbbk[.xyz]  resolves to  44[.]205p[.]227[.]254  (+68 seconds)

Average interval: 65 seconds
```

This regularity is machine-generated. No human activity produces timing this consistent.

The DNS responses are configured with a deliberate **60-second TTL (time-to-live)**. This is an evasion technique: by expiring the cached IP every minute, the botnet operators can migrate their C2 infrastructure to new IP addresses at any time and every infected device worldwide automatically follows within 60 seconds. Blocking a single IP is not sufficient defense.

The domain `o.fecebbbk[.xyz]` is a **typosquatting domain** designed to look like Facebook's mobile API endpoint `o.facebook.[com]` at a quick glance. The misspelling (`fecebbbk` vs `facebook`) is subtle enough to fool a network administrator scanning logs.

Custom Binary Heartbeat Protocol — Observed Behavior

Immediately after each DNS resolution, the device sends UDP traffic to port 16000 using a custom binary protocol with an identifiable structure. The following describes the observed protocol behavior without reproducing raw capture data:

Device Check-In Message (32 bytes): The device sends a fixed-size 32-byte packet containing a protocol magic identifier (`0x0000CD`) at a consistent offset, followed by a message type field indicating a check-in/ping (`0x0001`). The remainder of the packet is empty — the device is simply announcing it is online and requesting any pending commands.

C2 Server Acknowledgment (36 bytes): The C2 server responds with a 36-byte packet using the same magic identifier and a response message type (`0x0002`). A status field filled with `0xFF` bytes signals no pending commands. A 4-byte field at the end of each response contained the victim's public IP address — confirming the botnet operators had logged this home's IP in their proxy inventory.

The magic identifier `0x0000CD` is the Vo1d protocol's fingerprint. Any UDP traffic on port 16000 containing these bytes at the correct offset is Vo1d botnet heartbeat traffic. This is the basis for the detection signatures below.

The device retried the heartbeat every **9 to 21 seconds** with gradually increasing intervals (exponential backoff), indicating the malware was attempting to establish a persistent proxy tunnel.

Open Port Profile (RustScan)

An active scan of the device revealed **13 simultaneously open network ports** — an exact match to the documented Vo1d botnet signature:

```
 7000   7002   7102   7889   7890   8890   9528
10008  10012  10013  45199  55556  62110
```

No legitimate consumer projector requires 13 open network ports. This port profile is a standalone indicator of compromise. Any device on your network matching this profile should be treated as infected.

Residential Proxy Confirmation

The C2 server's response packets contained the victim's **public IP address** embedded as session data. This confirms that the botnet operators had successfully registered this home's IP in their proxy catalog. The device had been actively routing traffic through this residential IP address for the entire 2+ months it was running.

Independent Verification

All findings can be independently verified right now:

Platform	What to Check	Result
VirusTotal	jaguar-distributor.syslogcollector.[com]	11 of 93 vendors flag as malicious
ThreatYeti	38[.]55[.]17[.]113	Risk score 9.2 / 10.0
RustScan	Scan any AODIN X1BQ at `[device-ip]`	Will show 13 Vo1d-signature ports

---

Indicators of Compromise (IOC)

Malicious Domains

```
 ota.triplesai.[com]
syslogcollector.[com]
jaguar-distributor.syslogcollector.[com]
sd001.jaguar-distributor.syslogcollector.[com]
sd002.jaguar-distributor.syslogcollector.[com]
sd003.jaguar-distributor.syslogcollector.[com]
.o.fecebbbk[.xyz]
fecebbbk[.xyz]
```

Malicious IP Addresses

```
 111[.]230[.]36[.]129    Tencent Cloud     Fake OTA server
38[.]55[.]17[.]113      Unknown           C2 registration / proxy assignment
38.55.17.150      Unknown           Proxy traffic endpoint
44[.]205p[.]227[.]254    AWS us-east-1     UDP heartbeat C2
```

Malicious Ports

```
 8080   Fake OTA HTTP registration
12000  C2 proxy assignment
```

```
21001  Proxy traffic routing
16000  Vo1d UDP heartbeat protocol
```

Vo1d Port Signature (device scan)

```
 7000, 7002, 7102, 7889, 7890, 8890, 9528,
10008, 10012, 10013, 45199, 55556, 62110
```

Binary Protocol Fingerprint

```
 UDP traffic to port 16000 containing bytes 0x00 0x00 0xCD at payload offset 1-3
= Vo1d botnet heartbeat protocol
```

Detection Rules (Suricata / Security Onion)

```
 # Vo1d DNS beacon detection
alert dns any any -> any any (
  msg:"Vo1d Botnet DNS Beacon - fecebbbk[.xyz]";
  dns.query; content:"fecebbbk[.xyz]";
  sid:1000030; rev:1;
)

# Vo1d binary protocol magic bytes
alert udp any any -> any 16000 (
  msg:"Vo1d Botnet UDP Heartbeat - Magic Bytes";
  content:"|00 00 cd|"; offset:1; depth:3;
  sid:1000031; rev:1;
)

# Vo1d fake OTA registration
alert http any any -> 111[.]230[.]36[.]129 8080 (
  msg:"Vo1d Botnet Fake OTA Registration";
  sid:1000032; rev:1;
)

# Vo1d C2 registration server
alert tcp any any -> 38[.]55[.]17[.]113 12000 (
  msg:"Vo1d Botnet C2 Registration";
  sid:1000033; rev:1;
)

# DNS beaconing pattern threshold (3+ queries in 5 minutes)
alert dns any any -> any 53 (
```

```
  msg:"Vo1d Botnet DNS Beaconing Pattern";
  dns.query; content:"fecebbbk";
  threshold: type both, track by_src, count 3, seconds 300;
  sid:1000034; rev:1;
)
```

Recommended Actions

If You Own This Device

1. **Power it off immediately** — disconnect from your network now
2. Do not factory reset — the malware lives in firmware, not user data
3. Contact Amazon for a full refund citing pre-installed malware
4. Check your router DNS logs for queries to any of the IOC domains above
5. Contact your ISP — your IP may have been flagged for abuse traffic generated by this device
6. Consider filing a report with the FBI Internet Crime Complaint Center: ic3.gov

If You Are a Network Administrator

1. Block all IOC domains and IPs at your perimeter firewall immediately
2. Load the Suricata rules above into your IDS
3. Scan your network for devices matching the 13-port Vo1d signature
4. Alert any users who may have purchased AODIN devices

If You Are a Security Researcher

Machine-readable IOC files are in the `/iocs/` directory. Detection rules are in `/mitigation/`. If you have additional findings about AODIN devices or Vo1d variants, please open an issue or submit a pull request.

Investigation Timeline

Date	Event
Sept 10, 2025	Malware baked into firmware (confirmed by firmware build timestamp)
Dec 7, 2025	Device purchased on Amazon, listed as new
Dec 2025 – Feb 2026	Device used daily for streaming — malware active, completely undetected
Feb 2026	Manual packet capture performed as a proactive threat hunting exercise
Feb 2026	DNS beaconing pattern identified by hand — no automated alert triggered
Feb 2026	Full investigation completed — device permanently powered off

Date	Event
Feb 2026	Public disclosure published

About This Disclosure

This disclosure was conducted by a private individual who purchased this device as a consumer. The investigation began as a **proactive threat hunting exercise** — a manual packet capture performed with no prior suspicion, as part of a self-directed learning journey in network security.

No automated alert triggered this investigation. The malware was identified through manual traffic analysis: recognizing that a consumer projector was querying the same domain every 65 seconds with machine-perfect timing. That pattern recognition, applied to a routine packet capture, uncovered factory-installed botnet malware that had operated silently for over two months.

All findings were independently verified through public threat intelligence platforms before disclosure. The Amazon product listing was confirmed active at time of publication. A formal complaint has been submitted to Amazon requesting immediate removal of ASIN B0DGX51JPC.

Raw network capture files are not published in this repository. Traffic analysis was performed and documented, but raw captures are withheld to protect victim privacy. The behavioral descriptions above accurately and completely represent all observed malicious activity.

Related Research

- QiAnXin X-Lab — Original Vo1d Botnet Research
- VirusTotal — jaguar-distributor.syslogcollector.[com]
- ThreatYeti — 38.55.17.113

Contributing

If you own an AODIN device and want to check whether it is infected, see CONTRIBUTING.md for step-by-step instructions. Community verification of additional affected devices is welcome.

Published for public safety and security research purposes.
