INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-03-29 18:42 UTC

Joint Law Enforcement Action Dismantles Four DDoS-for-Hire Botnets Controlling 3M+ IoT Devices

THREAT CAMPAIGN | **CRITICAL** | CVSS 9.5

SCC Item ID	SCC-CAM-2026-0046
Type	Threat Campaign
Severity	CRITICAL
CVSS Base Score	9.5
Affected Products	IoT devices broadly (web cameras, DVRs, WiFi routers); DoD Information Network (DoDIN); telecommunications sector organizations; cloud-based DDoS mitigation services
Published	2026-03-21

Executive Summary

A joint U.S., German, and Canadian law enforcement operation dismantled the command and control infrastructure of four DDoS-for-hire botnets, Aisuru, KimWolf, JackSkid, and Mossad, that collectively compromised more than three million IoT devices and executed over 315,000 attack commands. The Aisuru botnet generated a verified peak of 31.4 Tbps in December 2025, demonstrating attack capacity capable of disabling enterprise and carrier-grade infrastructure. This takedown is a temporary disruption; according to law enforcement analysis, similar infrastructure has historically reconstituted within weeks. The underlying devices remain unpatched and internet-exposed.

Technical Analysis

The four botnets, Aisuru, KimWolf, JackSkid, and Mossad, operated as DDoS-as-a-Service platforms, renting volumetric attack capacity to third-party criminal actors. Collective device compromise exceeded 3 million nodes, predominantly consumer and enterprise IoT hardware including web cameras, DVRs, and WiFi routers. The Aisuru botnet generated a verified peak of 31.4 Tbps (December 2025), the largest recorded DDoS event globally at that time. Device compromise relied on three recurring weakness classes: hardcoded credentials (CWE-798), insecure default configurations (CWE-1188), and missing authentication on critical functions (CWE-306). No CVE is associated with this campaign; exploitation targeted endemic IoT design flaws rather than a discrete patched vulnerability. Relevant MITRE ATT&CK techniques include Network Denial of Service (T1498), Reflection Amplification (T1498.002), Direct Network Flood (T1498.001), Endpoint Denial of Service (T1499), botnet acquisition via Botnets (T1583.005) and Serverless Infrastructure (T1583.004), Compromise

Infrastructure via Botnets (T1584.005), Exploit Public-Facing Application (T1190), and Default Accounts (T1078.001). Akamai was a named private sector partner in the disruption. No patches are applicable at the campaign level; remediation is device-specific and configuration-driven. C2 infrastructure has been seized, but compromised devices remain active and recruitable by successor infrastructure.

Action Checklist

1. Step 1, Immediate: Audit internet-facing IoT devices (cameras, DVRs, routers) for hardcoded or default credentials; change all default passwords and disable unnecessary remote management interfaces before the next business day.
2. Step 2, Immediate: Block inbound and outbound traffic to known C2 ranges associated with Aisuru, KimWolf, JackSkid, and Mossad at perimeter and cloud-layer controls; monitor Akamai threat intelligence and CISA advisories for published IOC lists as they are released post-seizure.
3. Step 3, Detection: Query firewall, NetFlow, and DNS logs for IoT device nodes generating anomalous outbound connection volume, contacting non-business destinations, or exhibiting port-scan patterns consistent with botnet beaconing; flag devices communicating on ports historically associated with Mirai-family C2 propagation (TCP 23, 2323, 7547, 5555) or other anomalous management interfaces. Cross-reference against Akamai's published IOC list as available.
4. Step 4, Assessment: Inventory all IoT devices on the network, including shadow IT and OT-adjacent segments, and identify those running end-of-life firmware with no available updates; prioritize isolation or replacement for devices that cannot be patched.
5. Step 5, Communication: Notify relevant stakeholders (CISO, network operations, procurement) of the reconstitution risk; document current IoT exposure baseline for future comparison and include IoT device lifecycle management in the next GRC review cycle.
6. Step 6, Long-term: Enforce network segmentation for all IoT devices using dedicated VLANs with deny-by-default outbound policies; establish a firmware update cadence and procurement standard requiring vendors to document credential management and authentication controls (addressing CWE-798, CWE-1188, CWE-306) before purchase approval.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to external IR firm or law enforcement coordination (FBI/CISA) if forensic analysis of internal logs reveals any confirmed compromise of corporate networks or sustained C2 communication from internal hosts post-takedown; escalate to executive leadership and legal if IoT compromise resulted in lateral movement to critical systems or data exfiltration.
Recovery Notes	Post-containment recovery requires: (1) re-baseline network telemetry (firewall logs, NetFlow, DNS queries) for 7 days to confirm no residual C2 activity or beaconing; (2) validate that all IoT devices with patched firmware are functioning normally and no regressions occurred; (3) conduct a lessons-learned meeting with NetOps and Security to document gaps in visibility and coverage (e.g., 'we lacked real-time DNS monitoring') and commit to remediation within 90 days. Decommission isolated or end-of-life devices; document disposition (recycling/destruction) with signed asset recovery forms for compliance.

Forensic Artifacts	Firewall deny logs and connection logs (syslog, CEF, or native format) for 30+ days covering pre-block and post-block periods — key for establishing whether internal hosts were compromised | NetFlow/sFlow export records (binary .nfcapd files and/or CSV exports) showing outbound connection volumes, destination IPs, and port usage from IoT CIDR ranges | DNS query logs (Bind query logs, Windows Event Log 3008, or syslog from DNS forwarder) to identify beaconing to C2 domains and fast-flux behavior over 30-day window | Device management interface screenshots and firmware version dumps (via web UI, SSH, or SNMP sysDescr) to establish baseline firmware versions at time of incident and confirm patches applied | Packet captures (PCAP files from tcpdump or Wireshark) on IoT-sensitive ports (23, 2323, 7547, 5555, 8080, 8443) for 24-48 hours post-detection to preserve C2 handshake and command packets for analysis

Per-Action IR Details

Step 1 — Immediate: Audit internet-facing IoT devices (cameras, DVRs, routers) for hardcoded or default credentials; change all default passwords and disable unnecessary remote management interfaces before the next business day.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.1 (preparation phase); §3.2.1 (detection and analysis, credential inventory)

Controls: NIST 800-53 AC-2 (Account Management), NIST 800-53 AC-3 (Access Enforcement), CIS Controls 5.4 (Restrict Administrative Privileges), CIS Controls 6.2 (Address Unauthorized Software)

Compensating: Use nmap with default credential dictionaries: `nmap -p 80,443,8080,8443 --script http-default-accounts ` to identify devices with factory credentials. Cross-reference against CISA IoT default credential advisories. For each device, SSH/telnet in (if accessible) and manually verify /etc/passwd, /etc/shadow hashes, and web UI login pages. Document findings in a spreadsheet with device MAC, IP, model, and current credential status. If remote management ports (e.g., SSH 22, Telnet 23, HTTP 8080) are business-unnecessary, block at the edge firewall with explicit deny rules and document justification.

Evidence: Before credential changes: capture ARP table (`arp -a` on Windows, `ip neigh show` on Linux) to inventory device MAC/IP pairs; screenshot web UI login pages to document default manufacturer credentials; extract device firmware version strings from web interfaces or SNMP queries (`snmpwalk -v2c -c public `); photograph physical device labels for serial numbers and model identification. Store in centralized asset database with timestamp and analyst name for chain of custody.

Step 2 — Immediate: Block inbound and outbound traffic to known C2 ranges associated with Aisuru, KimWolf, JackSkid, and Mossad at perimeter and cloud-layer controls; monitor Akamai threat intelligence and CISA advisories for published IOC lists as they are released post-seizure.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.2.5 (containment); §3.2.6 (eradication, C2 blocking)

Controls: NIST 800-53 AC-4 (Information Flow Enforcement), NIST 800-53 SI-4 (Information System Monitoring), CIS Controls 13.1 (Network Segmentation), CIS Controls 13.2 (Network Intrusion Prevention)

Compensating: Monitor CISA alert mailing list (subscribe at alerts.cisa.gov) and check alerts.us-cert.gov/ltg daily for IoC releases. Once IOCs are published, create firewall rules at perimeter: create inbound deny ACLs for known C2 IP blocks and egress deny rules for destination IPs/ports. Use `whois` and `bgp.he.net` to identify ASN ranges if CIDR blocks are published. For cloud workloads, configure WAF/DDoS mitigation service (AWS Shield, Cloudflare, Akamai) to block at ingress. Log all blocked connections to syslog (firewall deny logs, VPC Flow Logs) with timestamps, source/dest IPs, and port/protocol for post-incident analysis. Create a 'botnet IOC' lookup table in Excel referencing CISA alert ticket numbers for audit trail.

Evidence: Capture baseline firewall rulesets before adding C2 blocks using `show running-config` (Cisco) or equivalent; export existing deny rules to a version-controlled file. Document the date and source (CISA alert URL) for each IOC block added. Collect firewall deny logs 24 hours pre-block and 48 hours post-block to establish whether internal hosts were communicating with C2 infrastructure before containment. Preserve these logs in read-only storage

with analyst signature and timestamp.

Step 3 — Detection: Query firewall, NetFlow, and DNS logs for IoT device nodes generating anomalous outbound connection volume, contacting non-business destinations, or exhibiting port-scan patterns consistent with botnet beaconing; flag devices communicating on ports associated with Mirai-variant C2 (TCP 23, 2323, 7547, 5555).

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2.2 (detection and analysis, log review); §3.2.3 (analysis, anomaly detection)

Controls: NIST 800-53 AU-12 (Audit Generation), NIST 800-53 SI-4 (Information System Monitoring), NIST 800-53 CA-7 (Continuous Monitoring), CIS Controls 8.2 (Collect Data on Network Traffic), CIS Controls 8.3 (Deploy Network Intrusion Detection)

Compensating: Export NetFlow/sFlow records from router or TAP if available; parse with `nfcapd` and `nfdump`: `nfdump -r -c 100 'dstport 23 or 2323 or 7547 or 5555' > c2_candidates.txt`. Query firewall logs using `grep` or `awk` for outbound conns from internal IoT subnets to external destinations; flag any internal device making >100 connections/hour to unique external IPs. Query DNS logs (`grep` syslog or export Bind query logs) for DNS queries from IoT device IPs to known malicious domains (use freely available blocklists from Abuse.ch, OpenPhish). Correlate results: if a device appears in multiple queries (high-volume outbound, port 23/2323/7547/5555, malicious DNS), escalate as likely compromised. Use `zeek` (free IDS) to tag suspicious flow patterns if SIEM unavailable. Document findings with timestamp, source IP, destination IP/domain, port, byte volume, and packet count.

Evidence: Preserve raw NetFlow/sFlow binary files and exported CSV dumps in append-only storage. Extract and store 30 days of DNS query logs (before detection date) to identify beaconing patterns and DNS fast-flux behavior. Capture firewall logs covering the same 30-day window in a searchable format. If possible, capture packet captures (tcpdump or Wireshark) for flagged IoT devices on ports 23, 2323, 7547, 5555 for 24-hour post-detection window to preserve C2 handshake packets and command payloads. Hash all logs with `sha256sum` and store hashes separately for integrity verification.

Step 4 — Assessment: Inventory all IoT devices on the network — including shadow IT and OT-adjacent segments — and identify those running end-of-life firmware with no available updates; prioritize isolation or replacement for devices that cannot be patched.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.1 (preparation, asset inventory); NIST 800-53r5 CM-2 (Baseline Configuration)

Controls: NIST 800-53 AM-2 (Inventory of Assets), NIST 800-53 CM-8 (Information System Component Inventory), CIS Controls 1.1 (Hardware Inventory), CIS Controls 2.1 (Software Inventory)

Compensating: Conduct active network scanning: use `nmap -sV -p 80,443,22,23,8080,8443 --script smb-os-discovery,snmp-sysinfo ` to identify device types and OS versions. Cross-reference results against CISA EOL device list (cisa.gov/iot). Create a CSV inventory with columns: device IP, MAC, model, firmware version, last-known vendor support date, CVSS score of unpatched vulns. Use open-source SHODAN alternative: `censys.io` API (free tier available) to query external-facing IoT for cross-validation. For devices inside network: use SNMP (`snmpwalk -v2c -c public 1.3.6.1.2.1.1`) to extract sysDescr and sysObjectID to identify OS/firmware. Document EOL devices separately; flag for isolation or replacement in procurement request with business justification (risk score × replacement cost).

Evidence: Export network scanning output to structured format (XML from nmap, CSV from custom script). Store baseline inventory snapshots (timestamp, analyst name) in version control. For each EOL device, document the vendor EOL announcement URL, last security patch date, and known CVE count to establish evidence of unpatched state. Photograph or screenshot device management interfaces showing firmware version. Store firmware binaries (if available) in secure archive with hash values for forensic verification.

Step 5 — Communication: Notify relevant stakeholders (CISO, network operations, procurement) of the reconstitution risk; document current IoT exposure baseline for future comparison and include IoT device lifecycle management in the next GRC review cycle.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §3.4 (post-incident activity, lessons learned); NIST 800-53r5 IR-4 (Incident Handling)

Controls: NIST 800-53 IR-2 (Incident Response Training), NIST 800-53 IR-6 (Incident Reporting), CIS Controls 19.7 (Conduct After-Action Reviews), CIS Controls 3.3 (Address Unauthorized Software)

Compensating: Prepare executive summary: 1-page memo with metrics — number of IoT devices inventoried, % running EOL firmware, % with default credentials changed, % blocked from C2 ranges. Include risk statement: 'X% of IoT devices remain at high risk of re-compromise due to unpatched firmware' with dollar impact (cost of DDoS mitigation service, potential downtime cost). Schedule stakeholder briefing (CISO, NetOps, Procurement, GRC) within 48 hours. Propose formal IoT lifecycle policy: require 3-year vendor support commitment at procurement, quarterly firmware audits, and hardware refresh plan for EOL devices within 12 months. Document baseline metrics (device count, firmware EOL %, credential compliance %) in a spreadsheet for comparison in future audits. Include in next GRC assessment cycle as a control gap (AC-2, CM-8, SI-2 implementation). Send summary memo with sign-off from CISO to executive steering committee.

Evidence: Retain all stakeholder communication logs (emails, meeting notes, attendee list) with timestamps. Create and version-control the IoT device inventory spreadsheet; sign off and timestamp each baseline snapshot. Document the proposed IoT lifecycle policy in a change request ticket with approval workflow. Store executive summary memo in secure repository with distribution list.

Step 6 — Long-term: Enforce network segmentation for all IoT devices using dedicated VLANs with deny-by-default outbound policies; establish a firmware update cadence and procurement standard requiring vendors to document credential management and authentication controls (addressing CWE-798, CWE-1188, CWE-306) before purchase approval.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.3 (recovery, system restoration); NIST 800-53r5 SC-7 (Boundary Protection); NIST SP 800-171 §3.13.1 (System and Communications Protection)

Controls: NIST 800-53 SC-7 (Boundary Protection), NIST 800-53 AC-4 (Information Flow Enforcement), NIST 800-53 SI-2 (Flaw Remediation), NIST 800-53 CM-5 (Access Restrictions for Change), CIS Controls 6.2 (Address Unauthorized Software), CIS Controls 13.1 (Network Segmentation)

Compensating: Create dedicated IoT VLAN(s) (e.g., 192.168.100.0/24) with separate access control lists (ACLs). Apply deny-by-default egress rules: explicitly allow only business-necessary outbound destinations (NTP for time sync on UDP 123, DNS on UDP 53, firmware update servers documented by vendor). Block all other outbound traffic and log to syslog. Test with `traceroute` and `tcpdump` from sample IoT devices to verify policy enforcement. Establish firmware update process: designate a 'firmware change window' (e.g., 2nd Tuesday of month, 02:00-04:00 UTC) and require change request tickets with rollback plan before deployment. For procurement: create a vendor questionnaire requiring documentation of: (1) hardcoded credentials audit results, (2) authentication mechanism (CWE-306 remediation), (3) 3-year security patch commitment, (4) firmware signing/verification controls. Score vendors against checklist; award purchases only to vendors meeting ≥80% compliance. Document all segmentation config changes in change management system with rollback procedures. Maintain firmware change log with device IP, old version, new version, change ticket number, and technician name.

Evidence: Export baseline network segmentation config (VLAN definitions, ACL rules) from switches/routers before and after implementation. Capture packet captures demonstrating denied egress attempts from IoT VLAN (use tcpdump filter `src 192.168.100.0/24 and dst not (53,123,)`). Store all vendor questionnaire responses and compliance scores in procurement system with audit trail. Version-control all firewall/switch configs using Git or equivalent; link each change to change ticket and IR incident number for traceability.

Detection Guidance

Focus detection on behavioral anomalies from IoT device segments rather than static IOC matching, as C2 infrastructure will reconstitute with new addresses. Key indicators: (1) IoT devices generating sustained high-volume outbound UDP or TCP traffic to non-business destinations, threshold anomalies above device-class baseline warrant investigation. (2) Devices initiating outbound connections on Telnet (TCP 23,

2323), TR-069 (TCP 7547), or ADB (TCP 5555), which are common Mirai-family propagation vectors. (3) DNS queries from IoT segments resolving to newly registered domains or domains with low Umbrella/Alexa rank, botnet C2 frequently uses fast-flux DNS. (4) NetFlow records showing IoT nodes participating in coordinated outbound bursts toward a common external destination, consistent with receiving and executing attack commands. (5) Authentication log entries showing successful logins to IoT management interfaces using default credential strings. For SIEM queries, filter on source IP ranges assigned to IoT VLANs, flag outbound connection counts exceeding a per-device hourly threshold (baseline varies by device class), and alert on any IoT device resolving domains registered within the past 30 days. Cross-reference against published C2 IOCs from CISA advisories, Akamai's security research blog, and law enforcement partners; IOC specificity typically improves in the days and weeks following disruption announcements.

Indicators of Compromise

Type	Value	Context	Confidence
DOMAIN	`Not yet published`	C2 domains for Aisuru, KimWolf, JackSkid, and Mossad botnets have not been publicly released as of this item's creation. Monitor Akamai security research blog and CISA for post-seizure IOC disclosure.	LOW
IP	`Not yet published`	C2 IP infrastructure was seized during the joint law enforcement operation. Specific addresses have not been publicly attributed. Watch for CISA and Akamai IOC releases.	LOW
URL	`https://www.akamai.com/blog/security-research/akamai-helps-disrupt-worlds-largest-iot-botnets`	Akamai named private sector partner post — primary source for technical IOC disclosure as investigation details are released. Validate this URL before use; listed as T3 source in item data.	MEDIUM

Framework Mappings

MITRE-ATTACK

- **T1498.002** — Reflection Amplification
- **T1499** — Endpoint Denial of Service
- **T1583.005** — Botnet
- **T1583.004** — Server
- **T1190** — Exploit Public-Facing Application
- **T1498.001** — Direct Network Flood
- **T1498** — Network Denial of Service
- **T1584.005** — Botnet
- **T1078.001** — Default Accounts

NIST-800-53R5

- **SC-5** — Denial-of-Service Protection
- **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
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management

OWASP-TOP10-2021

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

CIS-V8

- **6.3**
- **16.10**
- **7.3** — Perform Automated Operating System Patch Management
- **7.4** — Perform Automated Application Patch Management

ISO-27001-2022

- **A.8.28** — Secure coding
- **A.8.8** — Management of technical vulnerabilities

HIPAA-SECURITY

- **164.312(d)** — Person or Entity Authentication

SOC2-TSC

- **CC6.1** — Logical access security software, infrastructure, and architectures

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1498.002	Reflection Amplification	Impact
T1499	Endpoint Denial of Service	Impact
T1583.005	Botnet	Resource-Development
T1583.004	Server	Resource-Development
T1190	Exploit Public-Facing Application	Initial-Access
T1498.001	Direct Network Flood	Impact
T1498	Network Denial of Service	Impact

Technique ID	Technique Name	Tactic
T1584.005	Botnet	Resource-Development
T1078.001	Default Accounts	Defense-Evasion

Sources

Source	URL	Tier
Security News	https://www.bleepingcomputer.com/news/security/aisuru-kimwolf-jacks...	T3
Akamai Helps Authorities Disrupt the World's Largest IoT Botnets	https://www.akamai.com/blog/security-research/akamai-helps-disrupt-...	T3
Hacked Cameras, DVRs Powered Today's Massive Internet Outage	https://krebsonsecurity.com/2016/10/hacked-cameras-dvrs-powered-tod...	T3
Attackers Abuse UPnP Devices in DDoS Attacks, Akamai Warns	https://www.securityweek.com/attackers-abuse-upnp-devices-ddos-atta...	T3
How infected IoT devices are used for massive DDoS attacks	https://fedscoop.com/ddos-attacks-internet-of-things-cybersecurity/	T3

Generated 2026-03-29 18:42 UTC by TJS Security Command Center