INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-03-29 18:41 UTC

Four-Botnet Takedown Exposes the Industrial Scale of DDoS-as-a-Service: What Defenders Need Now

THREAT CAMPAIGN | **CRITICAL** | CVSS 9.5

SCC Item ID	SCC-CAM-2026-0053
Type	Threat Campaign
Severity	CRITICAL
CVSS Base Score	9.5
Affected Products	IoT devices broadly (IP cameras, DVRs, WiFi routers); DoD Information Network (DoDIN); telecommunications sector; cloud DDoS mitigation providers including Akamai
Published	2026-03-21

Executive Summary

A joint US-Germany-Canada law enforcement operation dismantled four major DDoS botnets, Aisuru, KimWolf, JackSkid, and Mossad, that collectively controlled over three million compromised IoT devices and launched more than 315,000 attack commands, including a record 31.4 Tbps strike against US Department of Defense network infrastructure in December 2025. The campaign confirms a mature, commercial-grade DDoS-for-hire economy that weaponizes unmanaged IoT devices, cameras, DVRs, and routers, that routinely fall outside enterprise and ISP security visibility. Organizations with IoT deployments, telecommunications exposure, or dependencies on internet-facing infrastructure face elevated residual risk as takedown operations rarely eliminate all botnet infrastructure or the underlying recruitment mechanisms.

Technical Analysis

The four botnets exploited a consistent set of weaknesses in consumer and prosumer IoT devices. Relevant CWEs: CWE-306 (missing authentication for critical function), CWE-1188 (insecure default initialization), CWE-521 (weak password requirements), and CWE-494 (download of code without integrity check). No CVE is associated with this campaign item, exploitation relied on class-level device weaknesses rather than a single discrete vulnerability. Attack techniques mapped to MITRE ATT&CK include: T1498 (Network Denial of Service), T1498.001 (Direct Network Flood), T1498.002 (Reflection Amplification), T1499 (Endpoint Denial of Service), T1583.005 (Botnet infrastructure acquisition), T1584.005 (Compromise of existing botnet infrastructure), T1608 (Stage Capabilities), T1587.001 (Develop Malware), T1071 and T1071.001 (Application

Layer Protocol, HTTP/S C2 communication), and T1562.001 (Impair Defenses). The Aisuru botnet peaked at 31.4 Tbps in December 2025, targeting DoD Information Network (DoDIN) infrastructure, a scale that saturates most upstream transit capacity. C2 infrastructure has been seized, but device-level compromise persists on enrolled endpoints until firmware is patched or devices are factory-reset. Device classes confirmed affected: IP cameras, DVRs, and WiFi routers with default credentials or missing authentication. No patch status is centrally trackable given the breadth of affected manufacturers; remediation is device-specific.

Action Checklist

1. Step 1, Immediate: Conduct an emergency inventory of all IoT devices on your network (cameras, DVRs, routers, and operational technology controllers). Identify any devices with default credentials, vendor-shipped passwords, or no authentication requirement on management interfaces (CWE-306, CWE-1188, CWE-521).
2. Step 2, Immediate: Force credential rotation on all discovered IoT devices. Disable remote management interfaces (Telnet, HTTP admin panels) that are not required for operations. Where firmware updates are available from the manufacturer, apply them now.
3. Step 3, Detection: Query firewall and flow logs for IoT device endpoints initiating outbound connections to non-standard ports, high-frequency SYN or UDP floods originating from internal segments, and unexpected DNS lookups or HTTP callbacks to external IPs from device subnets. Flag any device generating sustained outbound traffic volumes inconsistent with its function.
4. Step 4, Assessment: Segment IoT devices onto isolated VLANs with egress filtering. Block outbound traffic from IoT segments to destinations outside required operational scope. Verify that DDoS mitigation contracts (upstream ISP scrubbing, CDN-layer protection) cover your current peak ingress capacity. Note the record 31.4 Tbps volumetric attack observed in this campaign when evaluating your SLA adequacy.
5. Step 5, Communication: Notify network operations and SOC teams of the botnet TTPs and device classes involved. If your organization manages telecommunications infrastructure or operates DoDIN-adjacent systems, assess whether targeted sector advisories apply and brief relevant stakeholders.
6. Step 6, Long-term: Establish a formal IoT asset lifecycle policy requiring: default credential elimination before deployment, firmware update cadence tied to vendor advisories, and decommission procedures for end-of-life devices that no longer receive security updates. Review DDoS response playbooks against current volumetric thresholds and validate ISP-level mitigation SLAs.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to CISO and legal if any IoT device evidence of active botnet participation is detected (outbound DDoS traffic, C&C callback signatures); escalate to external IR firm if containment cannot be completed within 4 hours or if forensic evidence suggests attacker persistence beyond device compromise.

Recovery Notes	After all compromised IoT devices are isolated or patched, conduct 72-hour monitoring window: verify no devices resume C&C callbacks, confirm outbound traffic to non-approved destinations remains zero, validate that DDoS traffic against your organization and upstream (DoD, telecom) has ceased. Decompress isolated VLANs back into operations only after egress filtering rules are validated live. Schedule post-incident review within 1 week to document what detection failures occurred (why were sustained outbound connections not flagged sooner) and update detection playbooks and training.
Forensic Artifacts	Firewall/router netflow logs (syslog) for IoT device segments spanning 30 days pre-incident and 7 days post-remediation | DNS query logs with source MAC/IP for IoT devices, especially queries to non-.local domains during suspected C&C window | Device memory/configuration dumps (if accessible via TFTP or CLI) showing process lists, open ports, running services, and scheduled tasks (for Linux-based IoT devices) | DHCP server lease logs with device MAC, assigned IP, hostname, lease duration, and client version strings | Packet capture (PCAP) from IoT segment gateway showing full TCP/UDP headers and payload samples for any outbound non-standard-port connections (preserve at least 100 packets per suspicious flow for potential malware analysis)

Per-Action IR Details

Step 1 — Immediate: Conduct an emergency inventory of all IoT devices on your network (cameras, DVRs, routers, OT-adjacent devices). Identify any devices with default credentials, vendor-shipped passwords, or no authentication requirement on management interfaces (CWE-306, CWE-1188, CWE-521).

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.1 (preparation phase: asset inventory and baseline security configuration)

Controls: NIST 800-53 CM-2 (baseline configuration), NIST 800-53 IA-2 (authentication), CIS 6.1 (inventory of authorized devices)

Compensating: Use NMAP with nmap-services to scan for open management ports (Telnet 23, HTTP 80, HTTPS 443) on known IoT subnets: `nmap -p 23,80,443,8080,8443,9200 --open `. Cross-reference discovered IPs with DHCP logs and ARP tables. Document default credentials by vendor using CIRT.net and manufacturer datasheets. For teams without asset management tools, maintain a spreadsheet indexed by MAC address, model, firmware version, and credential status.

Evidence: Capture BEFORE enumeration: (1) baseline ARP table (`arp -a` or `ip neigh show`), (2) DHCP server lease logs with device hostnames and MAC addresses, (3) firewall rule logs showing allowed management ports, (4) router configuration backups. Store in write-protected forensic container with timestamp.

Step 2 — Immediate: Force credential rotation on all discovered IoT devices. Disable remote management interfaces (Telnet, HTTP admin panels) that are not required for operations. Where firmware updates are available from the manufacturer, apply them now.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.2.3 (containment: limiting scope of compromise); NIST 800-61r3 §4.1 (eradication: removing attacker artifacts)

Controls: NIST 800-53 IA-4 (credential management), NIST 800-53 AC-2 (account management), NIST 800-53 SI-2 (flaw remediation), CIS 6.2 (configuration hardening)

Compensating: For devices without centralized credential management: (1) document each device model's management interface and credential reset procedure before changes, (2) rotate credentials sequentially in staging environment first (if available) or on isolated test device of same model, (3) disable Telnet via device admin interface; verify disabled state persists after power cycle, (4) check manufacturer security advisories via vendor website or NVD for firmware CVEs; prioritize firmware versions with known DDoS-related RCE fixes. Use spreadsheet to track pre/post credential hashes (MD5 of username+password for audit trail, not for comparison).

Evidence: Capture BEFORE credential rotation: (1) CLI screenshots or API dumps of current device configurations including enabled protocols, (2) firmware version strings from device web interface or CLI (`show version` equivalent), (3) firewall logs showing current access to device management ports, (4) syslog or device activity logs showing last admin login timestamp. Preserve in timestamped evidence folder with device serial number as filename prefix.

Step 3 — Detection: Query firewall and flow logs for IoT device endpoints initiating outbound connections to non-standard ports, high-frequency SYN or UDP floods originating from internal segments, and unexpected DNS lookups or HTTP callbacks to external IPs from device subnets. Flag any device generating sustained outbound traffic volumes inconsistent with its function.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.1 (detection and analysis: identifying indicators of compromise); NIST 800-61r3 §3.1.2 (anomaly-based detection)

Controls: NIST 800-53 SI-4 (information system monitoring), NIST 800-53 AU-2 (audit events), CIS 8.4 (monitoring and alerting)

Compensating: Without SIEM: (1) Export firewall netflow/syslog to CSV and filter by source subnet (IoT VLAN) and destination port NOT IN (53, 80, 443, NTP 123). Use `grep` and `awk` to isolate outbound sessions: `grep '^' firewall.log | grep -v ':53 ' | grep -v ':80 ' | grep -v ':443 ' | awk '{print $NF}' | sort | uniq -c | sort -rn`. (2) Query DNS logs (Pi-hole, internal DNS server logs) for unexpected external domains queried from camera/DVR MACs: `grep /var/log/dnsmasq.log | grep -v '.local' | awk '{print $NF}'`. (3) Baseline normal traffic: measure average outbound bytes/hour per camera type over 1 week of clean operation; flag devices exceeding 2x baseline sustained for >5 min.

Evidence: Capture BEFORE filtering/analysis: (1) full firewall netflow/syslog for last 30 days of IoT segment activity (store in syslog server or exported PCAP), (2) complete DNS query logs with source MAC/IP for same period, (3) baseline traffic profile: calculate average MB/hour per device type during normal hours (9-17) for 5-day period, (4) any alerts from IDS/IPS (Snort, Suricata rules for botnet callbacks or DDoS tool signatures), (5) raw PCAP from IoT segment gateway during 1-hour capture window.

Step 4 — Assessment: Segment IoT devices onto isolated VLANs with egress filtering. Block outbound traffic from IoT segments to destinations outside required operational scope. Verify that DDoS mitigation contracts (upstream ISP scrubbing, CDN-layer protection) cover your current peak ingress capacity given the 31.4 Tbps benchmark established by Aisuru.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.2.4 (containment: network isolation); NIST 800-53 SC-7 (boundary protection)

Controls: NIST 800-53 SC-7(5) (deny by default), NIST 800-53 AC-4 (flow control), CIS 1.1 (network segmentation)

Compensating: For teams without managed switches: (1) Create static VLAN on existing switch using vendor CLI (e.g., `vlan 10`, assign ports); if no VLAN support, use separate physical network with dedicated gateway router, (2) Build egress ACL on gateway device (Linux iptables or router ACL): block all outbound from IoT segment except: DNS (53), NTP (123), firmware update host (specific vendor IP), and operational data server. Whitelist by IP, not hostname: `iptables -A FORWARD -s -d ! -j REJECT`, (3) Verify mitigation SLA: contact ISP/CDN provider, request current DDoS scrubbing capacity in writing; compare to your peak ingress (query NetFlow for max 5-min inbound rate last year); request capacity increase if current SLA < 10x peak observed.

Evidence: Capture BEFORE segmentation: (1) current network diagram with device IP ranges, (2) baseline firewall rules for IoT device access (export full rule set), (3) DDoS mitigation SLA documents from ISP and CDN providers with capacity limits highlighted, (4) NetFlow data showing historical peak inbound traffic rate (5-min average), (5) list of required operational destinations for each IoT device type (e.g., firmware update server, NVR heartbeat host) with IP and port.

Step 5 — Communication: Notify network operations and SOC teams of the botnet TTPs and device classes involved. If your organization manages telecommunications infrastructure or operates DoDIN-adjacent systems, assess whether targeted sector advisories apply and brief relevant stakeholders.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.3 (containment phase notification); NIST 800-61r3 §6 (post-incident: sharing lessons learned)

Controls: NIST 800-53 IR-6 (incident reporting), NIST 800-53 IR-4(1) (incident handling coordination)

Compensating: Create a one-page TLP:WHITE threat summary including: (1) botnet names (Aisuru, KimWolf, JackSkid, Mossad) and TTPs (DDoS via compromised IoT, C&C communication patterns), (2) IOCs relevant to your sector (CISA advisories for DoDIN-adjacent orgs), (3) affected device classes in your environment, (4) detection signatures SOC should monitor (specific outbound port/protocol combinations from IoT VLAN). Distribute via secure email or post to internal threat intelligence wiki with access control. Schedule 15-min briefing for NOC and SOC leads with incident response lead present.

Evidence: Preserve for post-incident review: (1) time-stamped communication log showing notification recipients and timestamp, (2) slideshow or briefing document with detection thresholds and escalation criteria, (3) acknowledgment from each stakeholder (SOC, NOC, management) that briefing was received, (4) CISA advisory downloads (save HTML snapshots) relevant to your sector.

Step 6 — Long-term: Establish a formal IoT asset lifecycle policy requiring: default credential elimination before deployment, firmware update cadence tied to vendor advisories, and decommission procedures for end-of-life devices that no longer receive security updates. Review DDoS response playbooks against current volumetric thresholds and validate ISP-level mitigation SLAs.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4.4 (post-incident: lessons learned); NIST 800-53 CM-3 (change control), NIST 800-53 PL-4 (security planning)

Controls: NIST 800-53 CM-2 (baseline configuration), NIST 800-53 SI-2 (flaw remediation), NIST 800-53 IR-4(1) (incident handling coordination), CIS 2.1 (asset inventory policy)

Compensating: Draft IoT lifecycle policy (1-2 pages) including: (1) pre-deployment checklist: all devices must have default credentials changed, management interfaces disabled except required, firmware at current patch level documented, (2) ongoing: monthly check for vendor security bulletins (set calendar reminder for each device model EOL date), apply patches within 30 days of release (prioritize RCE/botnet-related), (3) decommission: end-of-life devices (vendor support ends) must be isolated to separate VLAN or powered down within 90 days. Assign a named owner. Review DDoS playbook against new 31.4 Tbps benchmark: test ISP failover scenario (manually confirm backup ISP contact, SLA, capacity). Schedule annual tabletop exercise (2 hours) with NOC, SOC, and ISP incident coordinator.

Evidence: Create and preserve: (1) signed/dated IoT lifecycle policy document with version number and approval signatures, (2) device inventory spreadsheet with EOL date, firmware version, last patch date, policy compliance status for each device, (3) DDoS playbook version history showing date updated, personnel reviewed, and baseline volumetric assumptions, (4) ISP SLA contracts with highlighted capacity/response time terms, (5) meeting notes from post-incident review (lessons learned) session documenting why initial segmentation/egress filtering was delayed and what process changes will prevent recurrence.

Detection Guidance

Behavioral indicators to hunt for in your environment: (1) IoT device endpoints generating sustained outbound UDP or TCP SYN traffic, especially from camera, DVR, or router subnets, at volumes inconsistent with normal operation; (2) repeated outbound connection attempts from IoT segments to external IPs on ports 23 (Telnet), 2323, 7547, or uncommon high-number ports used for C2 callback; (3) DNS queries from IoT devices to domains not consistent with manufacturer update infrastructure; (4) NetFlow or sFlow data showing asymmetric traffic ratios (high outbound, minimal inbound) from IoT device IPs. For log-based detection: search firewall deny logs for blocked outbound flows from IoT subnets, and check DHCP/NAC logs for device classes (IP cameras, DVRs, routers) that have not been formally inventoried. If your SIEM supports asset classification, create a watchlist for all IoT device MACs/IPs and alert on any outbound traffic outside approved destination groups.

Note: C2 infrastructure for these four botnets has been disrupted per the law enforcement action, but specific IOC values (C2 IPs, domains, malware hashes) have not been publicly released in verified form as of this item's source date. Do not rely on static IOC blocking alone; behavioral detection is the durable control here. Check CISA.gov and law enforcement agency advisories (FBI IC3, Interpol) for any IOC updates or C2 infrastructure indicators published after this item's creation date, as such data is typically released on a delayed basis.

Indicators of Compromise

Type	Value	Context	Confidence
NOTE	`No verified IOCs available`	Specific C2 IPs, domains, or malware hashes for Aisuru, KimWolf, JackSkid, or Mossad botnets have not been released in verified form across the available sources. Source quality score for this item is 0.56 (T3 sources only). Do not fabricate or infer IOC values. Monitor Akamai Security Research, Trend Micro Threat Intelligence, and DOJ/CISA advisories for published IOC packages following the takedown.	LOW

Framework Mappings

MITRE-ATTACK

- **T1608** — Stage Capabilities
- **T1583.005** — Botnet
- **T1071.001** — Web Protocols
- **T1587.001** — Malware
- **T1498** — Network Denial of Service
- **T1071** — Application Layer Protocol
- **T1498.001** — Direct Network Flood
- **T1498.002** — Reflection Amplification
- **T1499** — Endpoint Denial of Service
- **T1562.001** — Disable or Modify Tools
- **T1584.005** — Botnet

NIST-800-53R5

- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **SI-4** — System Monitoring
- **SC-5** — Denial-of-Service Protection
- **IA-2** — Identification and Authentication (Organizational Users)
- **SI-7** — Software, Firmware, and Information Integrity

- **CM-3** — Configuration Change Control

OWASP-TOP10-2021

- **A07:2021** — Identification and Authentication Failures
- **A08:2021** — Software and Data Integrity Failures

CIS-V8

- **6.3**
- **2.5**
- **2.6**
- **7.3** — Perform Automated Operating System Patch Management
- **7.4** — Perform Automated Application Patch Management

HIPAA-SECURITY

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

SOC2-TSC

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

ISO-27001-2022

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1608	Stage Capabilities	Resource-Development
T1583.005	Botnet	Resource-Development
T1071.001	Web Protocols	Command-And-Control
T1587.001	Malware	Resource-Development
T1498	Network Denial of Service	Impact
T1071	Application Layer Protocol	Command-And-Control
T1498.001	Direct Network Flood	Impact
T1498.002	Reflection Amplification	Impact
T1499	Endpoint Denial of Service	Impact
T1562.001	Disable or Modify Tools	Defense-Evasion
T1584.005	Botnet	Resource-Development

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
IoT Botnet Linked to Large-scale DDoS Attacks Since the End of 2024	https://www.trendmicro.com/en_us/research/25/a/iot-botnet-linked-to...	T3
Addressing Vulnerabilities Introduced by IoT Devices in Telecom ...	https://www.iotforall.com/iot-telecom-vulnerabilities	T3
Akamai: Rise of IoT Devices Causes Some Security Concerns	https://www.radioworld.com/news-and-business/akamai-rise-of-iot-dev...	T3

Generated 2026-03-29 18:41 UTC by TJS Security Command Center