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

Four Major DDoS Botnets Dismantled: 3 Million Compromised IoT Devices, 31.4 Tbps Record Attack Neutralized

THREAT CAMPAIGN | **CRITICAL** | CVSS 9.5

SCC Item ID	SCC-CAM-2026-0068
Type	Threat Campaign
Severity	CRITICAL
CVSS Base Score	9.5
Affected Products	IoT devices (web cameras, DVRs, WiFi routers), 3 million+ compromised endpoints; targets included U.S. DoD Information Network (DoDIN), telecommunications providers, and cloud-based DDoS mitigation services including Akamai
Published	2026-03-21

Executive Summary

A coordinated U.S., German, and Canadian law enforcement operation dismantled four DDoS-for-hire botnets, Aisuru, KimWolf, JackSkid, and Mossad, that had compromised over 3 million IoT devices and issued more than 315,000 attack commands. The Aisuru botnet reached a recorded peak of 31.4 Tbps in December 2025 targeting U.S. DoD infrastructure; other targets included telecommunications providers and cloud DDoS mitigation services. While C2 infrastructure has been disrupted, the 3 million compromised endpoints remain at risk of re-enrollment into successor botnets unless remediated at the device level.

Technical Analysis

Four botnets operated under a cybercrime-as-a-service model, selling volumetric DDoS capacity to third-party customers. Compromise vectors relied on weak or default credentials and insecure network service configurations across consumer and enterprise IoT devices, specifically web cameras, DVRs, and WiFi routers. Associated CWEs: CWE-1188 (insecure default initialization), CWE-306 (missing authentication for critical functions), CWE-400 (uncontrolled resource consumption), CWE-770 (allocation of resources without limits). No CVEs are identified in the source data. MITRE ATT&CK techniques include T1498 / T1498.001 / T1498.002 (Network DoS, direct and reflection/amplification), T1499 (Endpoint DoS), T1190 (Exploit Public-Facing Application), T1584.005 / T1583.005 (botnet infrastructure acquisition and compromise), T1665 (Hide Infrastructure), T1071.001 (C2 via Web Protocols), and T1609 (Container Administration Command). Disruption

targeted the C2 layer; device-level compromise is not resolved by the takedown. Akamai served as named private sector partner. No patch is applicable, vulnerability is configuration-based.

Action Checklist

1. Step 1, Immediate: Audit all internet-facing IoT devices (cameras, DVRs, routers) for default or weak credentials; force credential rotation on any device using factory defaults. Priority on perimeter and OT-adjacent devices.
2. Step 2, Detection: Review outbound traffic logs for IoT device endpoints showing anomalous DNS lookups, unexpected outbound TCP/UDP connections on non-standard ports, or high-volume outbound traffic inconsistent with normal device behavior; these are indicators of active botnet C2 communication.
3. Step 3, Assessment: Inventory all IoT and unmanaged network devices; cross-reference against known vulnerable device classes (web cameras, DVRs, consumer-grade routers). Identify devices running end-of-life firmware with no available update path.
4. Step 4, Hardening: Disable remote management interfaces on IoT devices where not operationally required; segment IoT devices onto isolated VLANs with egress filtering to block outbound connections to non-approved destinations. Enforce rate limiting and traffic shaping on IoT network segments.
5. Step 5, Long-term: Establish a formal IoT device lifecycle policy requiring credential hardening and firmware update verification before deployment. Review DDoS resilience posture, confirm upstream scrubbing capacity, validate DDoS runbooks, and confirm cloud mitigation service SLAs cover volumetric attacks at multi-Tbps scale.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to CTO/CISO and legal team immediately if any evidence of data exfiltration (DNS tunneling, encrypted outbound tunnels, unknown data volume) is found on compromised IoT devices, or if forensic analysis reveals C2 activity post-detection window — both indicate active compromise and potential secondary breach.
Recovery Notes	Post-eradication, conduct threat hunt on all network traffic for past 90 days using discovered botnet IOCs to identify any missed compromised devices or lateral movement attempts. Implement continuous EDR/EPP monitoring on systems adjacent to IoT segments and establish quarterly firmware audit process to prevent reinfection. Document lessons learned with timeline of detection, response actions, and root-cause (e.g., default credentials, outdated firmware) to inform future procurement decisions.
Forensic Artifacts	Firewall egress deny logs and NetFlow/sFlow records (shows C2 connection attempts and data volumes) | DNS query logs with source IoT device IPs (reveals DNS-based C2 beaconing or DGA behavior) | IoT device configuration backups and firmware version strings (establishes baseline and identifies compromise indicators) | Full packet captures from IoT network segment (enables payload analysis, malware signature identification, and C2 protocol reverse engineering) | System time/NTP synchronization logs on all logging sources (ensures forensic timeline accuracy for correlation across devices)

Per-Action IR Details

Step 1 — Immediate: Audit all internet-facing IoT devices (cameras, DVRs, routers) for default or weak credentials; force credential rotation on any device using factory defaults. Priority on perimeter and OT-adjacent devices.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 (Preparation phase); §4.2 (Initial access prevention)

Controls: NIST 800-53 AC-2 (Account Management), NIST 800-53 IA-4 (Identifier Management), CIS 5.2 (Account Changes and Monitoring)

Compensating: Use vendor-supplied CLI/web interface to enumerate devices; create a spreadsheet inventory (hostname, IP, current credential status, firmware version). For device types without API access, manually connect to each device's web UI and document credential status. Batch credential changes via SSH or Telnet scripts using expect(1) or Python paramiko library if vendor management portal unavailable. Test changes on a staging device first.

Evidence: Before credential rotation: (1) capture device configuration backups via vendor export tool or manual web UI screenshot of current settings; (2) log IP address and MAC address associations from DHCP server or ARP table (show ip arp on Cisco, arp -a on Windows); (3) document baseline device HTTP/HTTPS banners using nmap -sV for version fingerprinting; (4) export current SNMP community strings if enabled (snmpwalk -v2c -c public sysDescr). Store all backups with cryptographic hash (sha256sum) in offline evidence locker.

Step 2 — Detection: Review outbound traffic logs for IoT device endpoints showing anomalous DNS lookups, unexpected outbound TCP/UDP connections on non-standard ports, or high-volume outbound traffic inconsistent with normal device behavior — these are indicators of active botnet C2 communication.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2.1 (Detection and Analysis); §3.2.4 (Defining an incident)

Controls: NIST 800-53 SI-4 (Information System Monitoring), NIST 800-53 CA-7 (Continuous Monitoring), CIS 8.4 (Detect C2 traffic)

Compensating: Without SIEM: (1) Export DNS query logs from authoritative nameserver (dig +short @) or corporate DNS appliance (if available, tcpdump -i eth0 'udp port 53' -w dns.pcap; then use zeek or suricata to parse); (2) Extract netflow or sflow from core router/switch using nflow-export tool or manual syslog parsing; (3) For packet-level inspection, deploy tcpdump on IoT network segment (tcpdump -i eth0 -w iot.pcap 'src and (dst port 80,443,8080 or dst port >10000)') and analyze in Wireshark or tshark with Suricata/Zeek rules; (4) Correlate against known botnet C2 IOCs from CISA, Shadowserver, and URLhaus using grep and cut; (5) Baseline 'normal' device behavior first (expected DNS domains, typical ports, data volume) before flagging anomalies.

Evidence: Preserve (1) full packet captures (tcpdump -C 500 for rolling 500MB files) from IoT network segment for past 72 hours if available; (2) DNS query logs with timestamps and source/destination IPs (querylog from ISC BIND or equivalent); (3) Firewall/router egress deny logs showing blocked outbound connections (check firewall syslog, not just dropped packet counters); (4) NetFlow/sFlow exports covering IoT subnets for past 30 days (5-tuple: src IP, dst IP, src port, dst port, protocol); (5) System time synchronization status on all logging sources (chronyc tracking) to ensure timeline accuracy; (6) IOT device process list and network connection state at time of detection (netstat -anp or ss -anp on device if accessible).

Step 3 — Assessment: Inventory all IoT and unmanaged network devices; cross-reference against known vulnerable device classes (web cameras, DVRs, consumer-grade routers). Identify devices running end-of-life firmware with no available update path.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 (Preparation—asset inventory); NIST 800-53 CM-2 (Baseline Configuration)

Controls: NIST 800-53 CM-2 (Baseline Configuration), NIST 800-53 CM-8 (Information System Component Inventory), CIS 2.1 (Hardware Inventory)

Compensating: Without CMDB: (1) Active network scan using nmap (nmap -sV -sC -O -p- --script default -oX inventory.xml) to enumerate services and OS fingerprints; parse output with nmap-parse-output or custom parsing; (2) DHCP/DNS passive enumeration: export DHCP lease database (dhcp-lease-list on Linux, Get-DhcpServerv4Lease on Windows) and correlate with DNS PTR records; (3) ARP table snapshot: arp-scan --localnet --quiet for local segment

or arp -a from router; (4) Use Shodan, Censys, or FOFA queries for public-facing IoT devices using known device signatures; (5) Correlate discovered devices against NIST NVD, CVE Details, and ExploitDB for known vulnerabilities; (6) Contact device vendors directly via SNMP sysDescr or web UI banner to determine EOL status and available firmware versions.

Evidence: Before assessment: (1) preserve full nmap XML output with timestamp (nmap -sV -O --version-all -oX nmap_baseline_.xml); (2) export DHCP lease tables with last-seen timestamps; (3) capture ARP tables from all routers/switches; (4) screenshot device web UI banners and firmware version information; (5) document CVE-to-device mappings discovered during assessment with source URLs; (6) create signed hash manifest of inventory data (sha256sum inventory.csv > inventory.csv.sha256) for chain-of-custody.

Step 4 — Hardening: Disable remote management interfaces on IoT devices where not operationally required; segment IoT devices onto isolated VLANs with egress filtering to block outbound connections to non-approved destinations. Enforce rate limiting and traffic shaping on IoT network segments.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 (Containment); NIST 800-53 AC-4 (Information Flow Enforcement)

Controls: NIST 800-53 AC-4 (Information Flow Enforcement), NIST 800-53 SC-7 (Boundary Protection), CIS 3.3 (Address Unauthorized Access)

Compensating: Without enterprise firewall: (1) Disable remote management protocols at device level: for cameras/DVRs, disable SSH/Telnet/HTTP via web UI or console access (default: ports 22, 23, 80, 443); for routers, disable WAN-side access to admin portal via CLI configuration; (2) Implement VLAN segmentation using managed switch (configure VLAN trunk, assign IoT ports to isolated VLAN, set native VLAN); (3) For egress filtering without dedicated firewall, use Linux iptables on gateway appliance (iptables -A FORWARD -i iot_vlan -o WAN -j DROP for default-deny, then add allow rules; iptables -A FORWARD -i iot_vlan -p tcp --dport 80,443 -o WAN -j ACCEPT for allowed destinations); (4) Rate limit using tc (traffic control) on gateway: tc qdisc add dev eth0 root tbf rate 10Mbit burst 32kbit latency 400ms to shape IoT segment to 10 Mbps; (5) Test segmentation by attempting SSH from IoT device to external host (should fail), then verify permitted traffic still flows.

Evidence: Before implementing: (1) baseline all current device configurations via export/backup (screenshot device UI, use vendor CLI export command); (2) identify all operational dependencies: for each IoT device, document which destination IPs/ports it legitimately needs (test with traffic capture: tcpdump -i eth0 src and not dst -w dependencies.pcap); (3) capture current switch/router configuration (show running-config on Cisco, or config file export); (4) take baseline network performance metrics (iperf from IoT subnet to external host before rate limiting is applied); (5) document which management interfaces are actively in use (query device access logs if available, or query syslog for successful remote logins to device IPs).

Step 5 — Long-term: Establish a formal IoT device lifecycle policy requiring credential hardening and firmware update verification before deployment. Review DDoS resilience posture — confirm upstream scrubbing capacity, validate DDoS runbooks, and confirm cloud mitigation service SLAs cover volumetric attacks at multi-Tbps scale.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.4 (Post-Incident Activities); NIST 800-53 SI-12 (Information Handling and Retention)

Controls: NIST 800-53 CM-3 (Change Control), NIST 800-53 CM-5 (Access Restrictions), CIS 2.3 (Authorized Software Inventory)

Compensating: Without formal ITSM system: (1) Create IoT procurement checklist document (spreadsheet or markdown) requiring pre-deployment sign-off on: credential change from factory defaults (test procedure specified), firmware version and EOL date verified against vendor, device segmentation plan documented, and security scanning clearance (nmap vulnerability check passed); (2) Require change request ticket (use free tools: OpenProject, Taiga, or GitHub Issues) for any firmware update with rollback plan and downtime window; (3) For DDoS resilience without enterprise services: (a) contact ISP for upstream filtering/scrubbing SLA details and historical attack capacity; (b) validate on-premises DDoS runbook—specify action triggers (e.g., detect >1 Gbps outbound traffic spike), escalation contacts, and recovery procedures; (c) test cloud mitigation service failover quarterly (coordinate with provider for safe test window); (d) maintain IOC feeds from CISA, Shadowserver, and DDoS-mitigation vendors; implement auto-block

of known botnet C2 infrastructure at egress firewall.

Evidence: Post-recovery: (1) document all detected botnet command servers with IP/domain/port and IOC attribution (create threat report with source references); (2) preserve final state configurations of all hardened devices (config backups, VLAN assignments, firewall rules); (3) generate incident timeline report covering detection to eradication with evidence references; (4) capture before/after network diagrams showing segmentation changes; (5) retain all forensic evidence (packet captures, logs, memory dumps) in cryptographically sealed archive (tar + gpg) with chain-of-custody documentation for legal review.

Detection Guidance

Focus detection on IoT device behavior anomalies rather than signature-based indicators, as botnet C2 domains and IPs from this operation are not published in the available source data. Key behavioral signals: (1) IoT device initiating outbound connections to IP ranges outside expected geographic or operational scope; (2) sustained high-volume UDP or ICMP egress from IoT segments, particularly toward reflection amplification targets (DNS port 53, NTP port 123, SSDP port 1900, MEMCACHED port 11211); (3) repeated failed authentication attempts against IoT management interfaces from external IPs (CWE-306 exploitation pattern); (4) IoT devices polling the same external IP or domain at regular intervals (C2 beacon pattern, T1071.001). In SIEM, create alerts for: outbound traffic volume thresholds exceeded per IoT device over a 5-minute window; new outbound destination IPs from IoT VLAN segments not seen in prior 30 days; authentication failures on Telnet (port 23) or SSH (port 22) from external sources against IoT management interfaces. No confirmed IOCs (IPs, domains, hashes) are available from the source data at this time; monitor threat intelligence feeds (CISA, Akamai Security Intelligence) for indicator releases tied to this operation.

Indicators of Compromise

Type	Value	Context	Confidence
DOMAIN	`[not available — no IOCs published in source data]`	C2 infrastructure for Aisuru, KimWolf, JackSkid, and Mossad botnets was dismantled; specific indicators have not been released in available sources. Monitor CISA and Akamai threat intelligence for indicator releases.	LOW

Framework Mappings

MITRE-ATTACK

- **T1498.002** — Reflection Amplification
- **T1499** — Endpoint Denial of Service
- **T1190** — Exploit Public-Facing Application
- **T1584.005** — Botnet
- **T1583.005** — Botnet
- **T1498.001** — Direct Network Flood
- **T1665** — Hide Infrastructure

- **T1071.001** — Web Protocols
- **T1498** — Network Denial of Service
- **T1609** — Container Administration Command

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)
- **SR-2** — Supply Chain Risk Management Plan

OWASP-TOP10-2021

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

CIS-V8

- **6.3**
- **13.8**
- **15.1** — Establish and Maintain an Inventory of Service Providers

HIPAA-SECURITY

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

SOC2-TSC

- **CC6.1** — Logical access security software, infrastructure, and architectures
- **CC9.2** — Manages risks associated with vendors and business partners

NIST-CSF-2

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

ISO-27001-2022

- **A.5.21** — Managing information security in the ICT supply chain

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1498.002	Reflection Amplification	Impact
T1499	Endpoint Denial of Service	Impact
T1190	Exploit Public-Facing Application	Initial-Access

Technique ID	Technique Name	Tactic
T1584.005	Botnet	Resource-Development
T1583.005	Botnet	Resource-Development
T1498.001	Direct Network Flood	Impact
T1665	Hide Infrastructure	Command-And-Control
T1071.001	Web Protocols	Command-And-Control
T1498	Network Denial of Service	Impact
T1609	Container Administration Command	Execution

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
The U.S. DOJ recently disrupted several large and powerful DDoS ...	https://www.facebook.com/AkamaiTechnologies/videos/the-us-doj-recen...	T3
Akamai Research: Web Attacks Up 33%, APIs Emerge as Primary ...	https://www.ir.akamai.com/news-releases/news-release-details/akamai...	T3
FS-ISAC and Akamai Report: DDoS Attacks on APAC Financial ...	https://cybersecurityasia.net/fs-isac-and-akamai-report-ddos-attack...	T3

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