INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-17 14:04 UTC

# Operation PowerOFF Shifts to Deterrence Phase: 53 DDoS-for-Hire Domains Seized, 75,000 Users Warned

**THREAT CAMPAIGN** | **MEDIUM** | CVSS 5.0

| | |
|---|---|
| **SCC Item ID** | SCC-CAM-2026-0184 |
| **Type** | Threat Campaign |
| **Severity** | MEDIUM |
| **CVSS Base Score** | 5.0 |
| **Affected Products** | No specific products affected; global booter/stresser/DDoS-for-hire platform infrastructure and associated user base (~75,000 identified users) |
| **Published** | 2026-04-16T18:26:34 |
| **Discovery Source** | Rss |

## Executive Summary

Operation PowerOFF, a 21-country law enforcement effort coordinated by Europol, seized 53 DDoS-for-hire domains, arrested four individuals, and identified over 75,000 users of booter platforms now subject to active deterrence. Organizations that rely on public-facing services face reduced near-term DDoS-for-hire capacity, but the underlying threat is not eliminated; the booter ecosystem has repeatedly reconstituted after prior takedowns. Security teams should treat this as a window to strengthen DDoS defenses, not a signal to deprioritize them.

## Technical Analysis

Operation PowerOFF's latest phase targeted booter and stresser services that enable volumetric DDoS attacks by renting attack infrastructure on demand, mapping to CWE-400 (Uncontrolled Resource Consumption) and CWE-770 (Allocation of Resources Without Limits or Throttling). Relevant MITRE ATT&CK techniques include T1498 (Network Denial of Service), T1498.001 (Direct Network Flood), T1499 (Endpoint Denial of Service), T1583.005 (Acquire Infrastructure: Botnet), T1584 (Compromise Infrastructure), and T1586 (Compromise Accounts). No specific CVE applies; this is a service-ecosystem disruption, not a software vulnerability. Law enforcement seized 53 domains, executed 25 search warrants, and is pursuing deterrence via search engine advertising, search result delisting of booter services, and blockchain-linked warning notifications to identified users. The 75,000 identified users represent customers of these services, not victims. Historical pattern: prior PowerOFF phases (2018, 2022, 2023) resulted in temporary capacity reductions followed by ecosystem

reconstitution within weeks to months. No patch applies; organizational exposure depends on DDoS resilience posture.

## Action Checklist

1. Containment: Review current DDoS mitigation posture for all internet-facing services: confirm upstream scrubbing, rate limiting, and traffic baseline monitoring are active. This is not a patch event; there is no vendor advisory to apply.
2. Detection: Monitor network flow telemetry (NetFlow, sFlow, or equivalent) for volumetric anomalies consistent with direct network flood patterns (T1498.001). Establish or validate bandwidth and packet-per-second baselines for public-facing assets now, while threat capacity is reduced.
3. Eradication: No malware or vulnerability to remove. If your organization has been targeted by booter services previously, confirm those attack vectors are mitigated: null routing, anycast diffusion, or CDN-layer absorption should be verified as functional.
4. Recovery: Validate DDoS runbooks are current and incident response roles are assigned. Test alerting thresholds on flow monitoring tools. Confirm upstream provider DDoS mitigation SLAs are documented and contact escalation paths are known.
5. Post-Incident: Use this window to close control gaps: implement or validate rate limiting at the application and network layer (addresses CWE-770), review cloud provider DDoS protection tier subscriptions, and ensure playbooks distinguish between volumetric, protocol, and application-layer attack types.

## IR / Forensic Enrichment

| | |
|---|---|
| **Triage Priority** | STANDARD |
| **Escalation Criteria** | Escalate to urgent if active volumetric flood is observed against public-facing services (sustained PPS spike >3x baseline on border interfaces), if a specific deterrence warning letter from Operation PowerOFF law enforcement is received identifying your organization's infrastructure as a booter target, or if upstream ISP confirms a live RTBH null-route has been auto-triggered against your IP space without an internal incident declaration. |
| **Recovery Notes** | Since Operation PowerOFF seized 53 domains but did not eliminate the booter ecosystem — prior takedowns (PowerOFF 2018, 2022) were followed by platform reconstitution within weeks to months — maintain elevated flow monitoring for at least 90 days post-seizure. Verify that all runbook improvements and rate limiting changes made during this deterrence window are tested under simulated load before the booter ecosystem reconstitutes. Confirm ISP RTBH trigger procedures are re-validated quarterly, as NOC contacts and BGP community configurations change without customer notification. |

| | |
|---|---|
| **Forensic Artifacts** | NetFlow/sFlow/IPFIX records from border routers covering all public-facing IP prefixes: specifically look for high-PPS flows with small packet sizes (<64 bytes) indicating SYN floods, or large-volume flows sourced from UDP port 123 (NTP), 53 (DNS), 1900 (SSDP), or 389 (CLDAP) indicating amplification attacks — canonical booter/stresser attack vectors \| ISP/upstream provider DDoS mitigation event logs: most providers generate a mitigation event record with start/stop timestamps, peak Gbps/MPPS, and attack signature classification when scrubbing is triggered — request these logs via NOC ticket immediately after any suspected attack as they may be purged after 30 days \| Web server and load balancer access logs (Apache/nginx access.log or ALB access logs) filtered for HTTP 503/429 responses and connection timeout spikes, which indicate application-layer HTTP flood (T1499.002) distinct from volumetric floods — booter platforms increasingly offer Layer 7 attack options \| SNMP interface counter history (ifInOctets, ifOutOctets, ifInErrors, ifInDiscards) from border and distribution layer routers for the 72-hour window surrounding any suspected attack — these counters capture flood impact even when NetFlow export is not configured or gaps exist in flow collector coverage \| DNS authoritative server query logs filtered for sudden spikes in ANY, TXT, or MX record queries from diverse source IPs, which indicate DNS reflection/amplification attacks being proxied through your own DNS infrastructure if recursion is misconfigured — a secondary risk when booter platforms target DNS resolvers |

### Per-Action IR Details

**Containment — Review current DDoS mitigation posture for all internet-facing services: confirm upstream scrubbing, rate limiting, and traffic baseline monitoring are active. This is not a patch event; there is no vendor advisory to apply.**

**NIST Phase:** Containment

**Reference:** NIST 800-61r3 §3.3 — Containment Strategy: choose containment strategy based on potential damage, evidence preservation, service availability, and time/resources required

**Controls:** NIST IR-4 (Incident Handling) — implement handling capability including containment, eradication, and recovery, NIST SC-5 (Denial-of-Service Protection) — implement controls to protect against and limit effects of DoS/DDoS attacks, CIS 4.4 (Implement and Manage a Firewall on Servers) — enforce rate-limiting and ingress filtering rules at the server and network perimeter layer

**Compensating:** Without enterprise scrubbing infrastructure, use iptables/nftables rate limiting: 'iptables -A INPUT -p tcp --dport 80 -m limit --limit 100/sec --limit-burst 200 -j ACCEPT; iptables -A INPUT -p tcp --dport 80 -j DROP'. For UDP flood protection add '-p udp -m hashlimit --hashlimit-above 1000/sec --hashlimit-burst 2000 --hashlimit-mode srcip'. Cloudflare Free or OVH anti-DDoS (included in hosting) provide upstream scrubbing at no cost. Verify BGP null-route capability with your ISP by confirming the NOC contact exists and the procedure is documented before an attack occurs.

**Evidence:** Before making any configuration changes, capture: (1) current iptables/nftables ruleset — 'iptables-save > pre_change_rules_$(date +%F).txt'; (2) active NetFlow/sFlow export configuration and collector addresses to confirm telemetry is actually being received; (3) upstream provider scrubbing activation status via provider portal screenshot or API response — document whether auto-mitigation or manual-trigger mode is active; (4) current bandwidth utilization baselines from SNMP MIB-II ifInOctets/ifOutOctets counters on border interfaces, which will serve as the clean-state reference for T1498.001 (Network Direct Flood) anomaly detection.

**Detection — Monitor network flow telemetry (NetFlow, sFlow, or equivalent) for volumetric anomalies consistent with direct network flood patterns (T1498.001). Establish or validate bandwidth and packet-per-second baselines for public-facing assets now, while threat capacity is reduced.**

**NIST Phase:** Detection Analysis

**Reference:** NIST 800-61r3 §3.2 — Detection and Analysis: establish baselines of normal network behavior; use network flow monitoring to identify anomalies; validate that detection thresholds reflect current environment

**Controls:** NIST SI-4 (System Monitoring) — monitor system to detect attacks and indicators of potential attacks, NIST AU-2 (Event Logging) — identify event types the system is capable of logging in support of audit; network flow records are the primary audit source for DDoS detection, NIST AU-12 (Audit Record Generation) — generate audit records for defined events across system components including network devices, CIS 8.2 (Collect Audit Logs) — ensure logging has been enabled across enterprise assets; for DDoS this means NetFlow/sFlow export enabled on all border and edge routers

**Compensating:** Without a commercial SIEM, deploy ntopng Community Edition (free) or nfdump/nfcapd to collect and analyze NetFlow v5/v9/IPFIX exports from border routers. Establish PPS/BPS baselines using: 'nfdump -r /var/cache/nfdump/ -s srcip/bytes -n 20 -o long' to identify top talkers during clean traffic periods. For packet-level capture, run 'tcpdump -i eth0 -nn -c 100000 -w baseline_$(date +%F).pcap not port 22' during a known-clean window and use Wireshark IO Graphs to derive normal PPS rates. Set threshold alerts in ntopng at 3x baseline PPS for UDP and ICMP, which are the primary vectors used by booter/stresser platforms (UDP amplification, ICMP flood, SYN flood).

**Evidence:** Capture before tuning thresholds: (1) NetFlow/sFlow records for the prior 30 days from border routers covering all public-facing IP ranges — specifically look for historical spikes in UDP port 0/any, DNS (port 53), NTP (port 123), SSDP (port 1900), and CLDAP (port 389) traffic sourced from non-local ASNs, which are canonical booter amplification vectors; (2) router interface counters (SNMP) for the same 30-day window showing ifInErrors and ifInDiscards, which spike during flood events even without flow export; (3) existing IDS/IPS alert history filtered on 'flood', 'amplification', or 'reflection' signatures to determine if your organization has been targeted by booter services in the past without formal incident declaration.

**Eradication — No malware or vulnerability to remove. If your organization has been targeted by booter services previously, confirm those attack vectors are mitigated: null routing, anycast diffusion, or CDN-layer absorption should be verified as functional.**

**NIST Phase:** Eradication

**Reference:** NIST 800-61r3 §3.4 — Eradication and Recovery: after containment, eradicate components of the incident; for infrastructure-based threats with no host compromise, eradication means confirming mitigations that neutralize the attack surface are operational

**Controls:** NIST IR-4 (Incident Handling) — eradication activities include identifying and eliminating components that enabled the incident, even when those components are external threat infrastructure, NIST SC-5 (Denial-of-Service Protection) — verify that DoS protection mechanisms are correctly implemented and verified as functional, not merely configured, CIS 4.2 (Establish and Maintain a Secure Configuration Process for Network Infrastructure) — validate that network device configurations implementing null routing and rate limiting match documented secure baseline

**Compensating:** Verify null-route capability with a non-impacting test: coordinate with ISP NOC to confirm RTBH (Remotely Triggered Black Hole) BGP community tagging is configured for your ASN — request written confirmation of the trigger process and SLA. For anycast diffusion without a commercial CDN, verify Cloudflare or AWS CloudFront (both have free tiers) are configured to proxy all public-facing A/AAAA records so the origin IP is not exposed via DNS. Run 'dig +short yourdomain.com' and confirm the returned IPs are CDN ranges, not your origin — if the origin IP is exposed, the CDN layer is bypassable by booter platforms that enumerate origin IPs. Document verified functional status with timestamped screenshots.

**Evidence:** Before closing eradication: (1) pull historical DDoS incident tickets or NOC escalation logs to identify which attack vectors (UDP amplification, SYN flood, HTTP flood) were used in prior booter attacks against your organization — this determines which mitigations must be re-verified; (2) capture current BGP routing table from border router ('show ip bgp summary' or 'show route') to confirm no null routes are currently in effect from a prior unresolved attack; (3) document CDN/proxy configuration export showing all public-facing hostnames and whether origin IPs are masked — this is the primary residual attack surface for booter services that bypass CDN layers.

**Recovery — Validate DDoS runbooks are current and incident response roles are assigned. Test alerting thresholds on flow monitoring tools. Confirm upstream provider DDoS mitigation SLAs are documented and contact escalation paths are known.**

**NIST Phase:** Recovery

**Reference:** NIST 800-61r3 §3.5 — Recovery: restore systems to normal operation; verify systems are functioning normally; implement additional monitoring to watch for recurrence; execute recovery plan and verify integrity

**Controls:** NIST IR-8 (Incident Response Plan) — IR plan must include restoration procedures, criteria for declaring recovery complete, and post-incident monitoring requirements, NIST IR-7 (Incident Response Assistance) — identify and document IR support resources including upstream provider NOC contacts and escalation paths as part of the IR capability, NIST CP-2 (Contingency Plan) — contingency plan must include recovery objectives and escalation procedures; DDoS SLA documentation maps to this control, CIS 7.2 (Establish and Maintain a Remediation Process) — remediation process must include documented roles, responsibilities, and timelines; runbook validation satisfies this requirement

**Compensating:** For a 2-person team without a GRC platform, maintain runbooks as version-controlled Markdown in a private Git repo (GitHub/GitLab free tier) so changes are auditable. Test flow monitoring alert thresholds using a controlled traffic generator: 'hping3 -S --flood -V -p 80 ' in an isolated lab or staging environment — do NOT test against production. Confirm the alert fires in ntopng or your flow collector before the test concludes. For SLA documentation, create a single reference card with ISP NOC phone number, account ID, RTBH trigger process, and estimated mitigation activation time — store it in the runbook repo and verify it is accessible offline (printed or local copy) since a live DDoS may impair cloud-hosted documentation access.

**Evidence:** Before validating recovery readiness: (1) retrieve the most recent tabletop exercise or runbook walk-through record — if none exists within the past 12 months, document the gap as a finding; (2) pull current upstream provider contract or service agreement to verify the DDoS mitigation SLA clause exists and specifies activation time, mitigation capacity (Gbps), and escalation contact — many SMB contracts have no SLA for DDoS; (3) collect flow monitoring tool alert history to confirm thresholds have fired at least once on a real or simulated event, establishing that the alerting pipeline from sensor to notification is verified end-to-end.

**Post-Incident — Use this window to close control gaps: implement or validate rate limiting at the application and network layer (addresses CWE-770), review cloud provider DDoS protection tier subscriptions, and ensure playbooks distinguish between volumetric, protocol, and application-layer attack types.**

**NIST Phase:** Post Incident

**Reference:** NIST 800-61r3 §4 — Post-Incident Activity: lessons learned meetings; update IR plan and procedures based on findings; improve detection and prevention capabilities; share threat intelligence

**Controls:** NIST SI-2 (Flaw Remediation) — although no CVE applies, CWE-770 (Allocation of Resources Without Limits or Throttling) represents a systemic architectural flaw requiring remediation through rate limiting controls, NIST IR-4 (Incident Handling) — post-incident review must identify improvements to preparation, detection, containment, and recovery capabilities, NIST AU-6 (Audit Record Review, Analysis, and Reporting) — post-incident analysis of flow telemetry and alert history informs threshold tuning for future booter activity, CIS 7.1 (Establish and Maintain a Vulnerability Management Process) — use this deterrence window as a scheduled review trigger to assess DDoS mitigation posture as a control gap, not a patching event, CIS 7.2 (Establish and Maintain a Remediation Process) — document the three DDoS attack type distinctions (volumetric T1498.001, protocol, application-layer T1499) in the remediation process so response actions are mapped to attack type before an incident occurs

**Compensating:** Implement application-layer rate limiting for free using nginx 'limit_req_zone' and 'limit_conn_zone' directives — e.g., 'limit_req_zone $binary_remote_addr zone=api:10m rate=100r/s; limit_req zone=api burst=200 nodelay;' protects against HTTP flood (T1499.002) without a WAF. For cloud tier review without a CSPM tool, manually audit AWS Shield (Standard vs Advanced), Cloudflare Free vs Pro DDoS rules, or Azure DDoS Protection Basic vs Network Plan — document current tier, cost, and the specific attack capacity threshold each tier defends against. Publish the three-category DDoS playbook distinction (volumetric/protocol/application) as a one-page decision tree in the runbook repo referencing MITRE ATT&CK T1498 (Network DoS) and T1499 (Endpoint DoS) so responders can classify attack type within the first 5 minutes.

**Evidence:** For the post-incident lessons learned record: (1) aggregate all NetFlow anomaly records, alert firing events, and ISP NOC communications from the review period into a timeline — this becomes the evidence base for the lessons learned report required by NIST 800-61r3 §4; (2) document current cloud provider DDoS protection tier with a portal screenshot dated today, establishing a baseline against which future subscription changes can be measured; (3) capture rate limiting configuration state (nginx, iptables, or WAF rules) in a versioned config export so the pre-improvement baseline is preserved for comparison after CWE-770 remediations are applied.

## Detection Guidance

No IOCs are publicly attributed to specific active booter campaigns at this time. Detection focus should be behavioral. Monitor NetFlow or sFlow data for sudden spikes in inbound UDP, ICMP, or TCP SYN traffic from distributed source IPs, characteristic of volumetric floods (T1498.001). Key indicators: packet-per-second ratios disproportionate to session counts; geographic clustering inconsistent with normal traffic patterns; traffic targeting a single destination IP or port. For application-layer signals, watch for HTTP request floods with minimal payload variation (T1499). SIEM queries should alert on: inbound traffic volume exceeding 2x the 30-day baseline for any public-facing interface; BGP route changes or upstream provider null-route notifications; repeated connection resets from single source CIDRs. No specific file hashes, domains, or IPs are available for blocklisting from this operation as of this advisory.

## Framework Mappings

### MITRE-ATTACK

- **T1586** — Compromise Accounts
- **T1499** — Endpoint Denial of Service
- **T1584** — Compromise Infrastructure
- **T1498.001** — Direct Network Flood
- **T1498** — Network Denial of Service
- **T1583.005** — Botnet

### NIST-800-53R5

- **SC-5** — Denial-of-Service Protection

### CIS-V8

- **13.8** — Deploy a Network Intrusion Prevention Solution

## MITRE ATT&CK Mapping

| Technique ID | Technique Name | Tactic |
|---|---|---|
| T1586 | Compromise Accounts | Resource-Development |
| T1499 | Endpoint Denial of Service | Impact |
| T1584 | Compromise Infrastructure | Resource-Development |
| T1498.001 | Direct Network Flood | Impact |
| T1498 | Network Denial of Service | Impact |
| T1583.005 | Botnet | Resource-Development |

## Sources

| Source | URL | Tier |
|---|---|---|
| **Security News** | https://www.bleepingcomputer.com/news/security/operation-poweroff-i... | T3 |
| **Officials seize 53 DDoS-for-hire domains in ongoing crackdown** | https://cyberscoop.com/ddos-for-hire-takedowns-operation-poweroff/ | T3 |
| **Law Enforcement Seizes 9 DDoS-for-Hire Webpages as Part of ...** | https://www.justice.gov/usao-cdca/pr/law-enforcement-seizes-9-ddos-... | T1 |
| **2024 DDoS-for-Hire Landscape Part 5 - Netscout** | https://www.netscout.com/blog/asert/2024-ddos-hire-landscape-part-5 | T3 |
| **Understanding Botnet for Hire Services: DDoS Booter, Stressers ...** | https://datadome.co/learning-center/what-is-ddos-booter-botnet-booter/ | T3 |



Generated 2026-04-17 14:04 UTC by TJS Security Command Center