INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-01 07:12 UTC

Brazilian DDoS Protection Firm Allegedly Enabling Botnet Activity

SECURITY ANALYSIS | HIGH

SCC Item ID	SCC-STY-2026-0100
Type	Security Analysis
Severity	HIGH
Affected Products	Networks protected by unnamed Brazilian DDoS mitigation firm (specific products/versions unconfirmed)
Published	5 hours ago
Discovery Source	Serper

Executive Summary

A Brazilian DDoS mitigation firm has been reported by Krebs on Security as allegedly operating botnet infrastructure rather than defending against it. If confirmed through law enforcement or regulatory findings, this would represent a supply-chain trust failure: organizations paying for DDoS protection could unknowingly be using a service that facilitates attacks against others. This case signals a documented threat pattern: malicious actors embedding within legitimate security service providers to abuse network access and credibility.

Technical Analysis

The primary Krebs on Security article was not accessible for verification in this analysis. The following describes the general pattern this class of threat follows, based on MITRE technique mappings and historical precedent, NOT specific confirmed details from the reported case. Security teams must access the primary Krebs article directly to verify the specific firm identity, technical mechanisms, and scope.

General threat pattern: The core allegation class is that a purported DDoS mitigation firm operates botnet infrastructure rather than neutralizing it. The MITRE ATT&CK techniques associated with this activity are T1583.005 (Acquire Infrastructure: Botnet) and T1498 (Network Denial of Service), describing a threat actor acquiring or operating distributed attack infrastructure and deploying it for volumetric denial-of-service campaigns.

The structural vulnerability is one of misrepresentation at the service layer. A DDoS mitigation provider occupies a privileged position in customer network architecture: traffic is scrubbed through the provider's infrastructure before reaching the customer. A firm operating in bad faith in that role can observe traffic patterns, maintain

persistent network positioning, and potentially redirect or weaponize the very infrastructure customers believe is protecting them.

This pattern has precedent. The 2018 exposure of bulletproof hosting operations embedded within legitimate-appearing ISPs, documented extensively by security researchers and covered by Krebs, established a playbook: acquire or register a legitimate-looking service company, use the business cover to obtain IP address space and upstream transit, then operate offensive infrastructure through that cover. The Brazilian context is notable given the region's documented growth in cybercrime-as-a-service markets and botnet-for-hire ecosystems.

Confidence in specific technical details about this incident is LOW. All analysis above is either MITRE framework mapping or historical pattern reference. For incident-specific details, access the primary Krebs reporting directly.

Action Checklist

1. Step 1: Access primary source, retrieve the full Krebs on Security article to identify the specific Brazilian firm, products, and technical indicators; use that article as the basis for all subsequent steps
2. Step 2: Assess exposure, determine whether your organization uses any Brazilian-registered or Brazil-operated DDoS mitigation, traffic scrubbing, or CDN service; cross-reference the firm identified in Step 1 against your vendor inventory immediately
3. Step 3: Review controls, audit traffic flows through any third-party scrubbing or mitigation provider: confirm what data and traffic those services can observe, log, or redirect; verify contractual and technical controls governing that access
4. Step 4: Update threat model, add 'malicious or compromised DDoS mitigation provider' as an explicit supply-chain threat scenario; map to T1583.005 and T1498 in your threat register and evaluate existing detective controls against botnet participation or infrastructure misuse
5. Step 5: Communicate findings, brief leadership on the specific third-party risk angle: this is not a vulnerability in your own systems but a potential trust failure in a contracted security service; frame the risk in terms of vendor due diligence and contractual obligations
6. Step 6: Monitor developments, track Krebs on Security directly for the full published article and any follow-up disclosures; watch for Brazilian CERT (CERT.br) advisories, law enforcement actions, or regulatory responses naming the firm

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate to immediate priority and engage legal counsel if vendor inventory confirms active use of the identified Brazilian DDoS mitigation firm, if NetFlow or BGP analysis reveals non-attack-period traffic being routed through the provider (indicating potential passive interception beyond the scrubbing function), or if any data subject to breach notification obligations (PII, PHI, PCI) transited the scrubbing path.

Recovery Notes	If the provider is suspended or terminated, verify that BGP diversion routes to the provider's IP ranges are fully withdrawn and that all GRE tunnel configurations are removed from border routers before restoring normal traffic paths — validate using 'show ip bgp' and 'show interfaces tunnel' outputs. Identify and contract an alternative DDoS scrubbing provider with verified legal entity registration outside the implicated jurisdiction and contractual audit rights. Monitor outbound traffic for 30 days post-transition using NetFlow or Zeek conn.log for any anomalous connections to IP ranges previously associated with the terminated provider, which could indicate residual routing or misconfiguration.
Forensic Artifacts	BGP routing table snapshots and change history from border routers showing when traffic diversion to the Brazilian provider's anycast or GRE endpoints was active, including any non-attack-period diversion that would indicate passive traffic interception beyond the stated scrubbing function | NetFlow/IPFIX records (90-day retention recommended) from all ingress and egress points showing traffic volume, protocol distribution, and destination IP ranges routed to the scrubbing provider — specifically capturing baseline (non-DDoS) periods to identify unauthorized traffic observation | DNS query logs from internal resolvers showing resolution history for the scrubbing provider's mitigation endpoints, including any subdomains used for health checks or GRE tunnel keepalives that could map provider infrastructure | Firewall and router configuration archives capturing GRE tunnel definitions, BGP peer configurations, and static routes associated with the provider's IP ranges — these establish the technical access boundary the provider had to organizational traffic | Vendor contract, onboarding documents, and any SOC 2 or penetration test reports provided by the DDoS mitigation firm — these establish what security assurances were represented and are essential for any contractual dispute or regulatory inquiry arising from the supply-chain trust failure

Per-Action IR Details

Step 1: Assess exposure — determine whether your organization uses any Brazilian-registered or Brazil-operated DDoS mitigation, traffic scrubbing, or CDN service; if vendor identity is confirmed in the Krebs article, cross-reference against your vendor inventory immediately

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: identifying scope of potential impact from the adverse event

Controls: NIST IR-4 (Incident Handling), NIST IR-5 (Incident Monitoring), NIST RA-3 (Risk Assessment) — assess likelihood and impact of using a potentially adversarial scrubbing provider, CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory) — extend to third-party service inventory, CIS 7.1 (Establish and Maintain a Vulnerability Management Process) — vendor exposure qualifies as a risk to be assessed

Compensating: Pull your vendor inventory from accounts payable or procurement records — filter for any vendor with Brazilian CNPJ registration, .com.br domains, or AS numbers registered under ANATEL. Cross-reference BGP routing data using free tools: run 'whois -h whois.radb.net ' and 'curl https://stat.ripe.net/data/whois/data.json?resource=' to confirm country of registration and ASN ownership. Document all third-party IPs your traffic is currently routed through using 'traceroute' or 'mtr' to upstream scrubbing nodes.

Evidence: Before acting, capture: (1) current BGP routing table snapshots showing any anycast or scrubbing provider next-hops — run 'show ip bgp summary' on border routers and save output; (2) DNS resolution history for your scrubbing provider's mitigation endpoints, pulled from internal DNS resolver query logs; (3) NetFlow/IPFIX records showing traffic volumes routed to the scrubbing provider's IP ranges over the past 90 days; (4) vendor contract documents and onboarding records identifying the legal entity, registration country, and ASN ranges assigned to the provider.

Step 2: Review controls — audit traffic flows through any third-party scrubbing or mitigation provider: confirm what data and traffic those services can observe, log, or redirect; verify contractual and technical

controls governing that access

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: understanding adversary access and visibility into organizational data and communications

Controls: NIST IR-4 (Incident Handling), NIST AU-6 (Audit Record Review, Analysis, and Reporting) — review logs of traffic redirected through scrubbing provider, NIST AU-9 (Protection of Audit Information) — assess whether the scrubbing provider has access to or can tamper with your traffic logs, NIST SC-5 (Denial of Service Protection) — evaluate whether the contracted control is itself a threat vector, NIST SA-9 (External System Services) — review obligations and controls governing third-party service provider access, CIS 3.3 (Configure Data Access Control Lists) — determine what data classes traverse the scrubbing provider, CIS 4.2 (Establish and Maintain a Secure Configuration Process for Network Infrastructure)

Compensating: Without a SIEM, use NetFlow data (ntopng free tier or pmacct) to quantify traffic volume and protocol mix routed to the scrubbing provider's IP ranges. Pull firewall and router ACL configs manually and identify any GRE tunnels, BGP sessions, or static routes terminating at provider-controlled IPs. Review your BGP community strings to confirm you are not advertising more-specific routes than intended to the provider. Use Wireshark on a network tap or SPAN port to capture a 15-minute sample of traffic transiting the scrubbing path and verify no unexpected protocol encapsulation (e.g., unexplained GRE or IPIP headers) is present.

Evidence: Preserve before auditing: (1) router and firewall configuration backups showing BGP peer relationships and GRE tunnel endpoints associated with the DDoS scrubbing provider; (2) NetFlow/sFlow records from the past 30–90 days showing all traffic egressing toward scrubbing provider IP ranges, including non-attack-period baseline traffic — this establishes what was observable to the provider during normal operations; (3) any existing SLA or SOC reports from the provider that characterize their logging and data retention practices, which may evidence what they captured; (4) SSL/TLS inspection configuration records showing whether decrypted traffic was forwarded through the scrubbing path.

Step 3: Update threat model — add 'malicious or compromised DDoS mitigation provider' as an explicit supply-chain threat scenario; map to T1583.005 and T1498 in your threat register and evaluate existing detective controls against botnet participation or infrastructure misuse

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: lessons learned and threat model updates to prevent recurrence of supply-chain trust failures

Controls: NIST IR-8 (Incident Response Plan) — update IR plan to include malicious security vendor as a threat scenario, NIST RA-3 (Risk Assessment) — incorporate adversarial DDoS provider as an explicit supply-chain risk, NIST SA-9 (External System Services) — revise third-party risk requirements to include provider behavioral monitoring, NIST SI-4 (System Monitoring) — evaluate whether existing monitoring detects outbound botnet C2 traffic that a scrubbing provider could be facilitating or masking, CIS 7.1 (Establish and Maintain a Vulnerability Management Process) — extend process to include third-party service provider threat scenarios, CIS 4.2 (Establish and Maintain a Secure Configuration Process for Network Infrastructure)

Compensating: Map MITRE ATT&CK T1583.005 (Botnet infrastructure acquisition) and T1498 (Network Denial of Service) into your threat register using the ATT&CK Navigator (free, browser-based). For detective control gap analysis without a SIEM, deploy Zeek (free) on a network tap to generate conn.log and dns.log data; write a simple AWK or Python script to flag outbound connections from your network to IP ranges associated with known botnet C2 infrastructure using threat intel feeds from Spamhaus DROP list or Feodo Tracker (both free). This tests whether your current visibility would catch traffic manipulation or C2 relay activity a rogue scrubbing provider might facilitate.

Evidence: Before updating the threat model, preserve the current state: (1) existing threat model documentation and risk register entries for DDoS and third-party risk — these establish the pre-event baseline for lessons-learned; (2) current network topology diagrams showing the scrubbing provider's position in the traffic path — specifically whether the provider sits inline (all traffic passes through) or on-demand (BGP diversion only during attack); (3) Zeek or NetFlow conn.log samples showing any anomalous outbound connection patterns from internal hosts that could indicate the scrubbing provider was relaying traffic or acting as a C2 intermediary.

Step 4: Communicate findings — brief leadership on the specific third-party risk angle: this is not a vulnerability in your own systems but a potential trust failure in a contracted security service; frame the risk in terms of vendor due diligence and contractual obligations

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment: communicating incident status and risk to leadership to enable containment decisions including vendor relationship actions

Controls: NIST IR-4 (Incident Handling) — incident handling includes leadership notification and coordination, NIST IR-6 (Incident Reporting) — report suspected third-party compromise to appropriate organizational leadership, NIST IR-8 (Incident Response Plan) — execute communication procedures defined in the IR plan, NIST SA-9 (External System Services) — leadership must be informed to authorize contractual or service termination actions, CIS 7.2 (Establish and Maintain a Remediation Process) — leadership briefing enables risk-based remediation authorization

Compensating: Prepare a one-page executive brief using the following structure: (1) what the Krebs on Security report alleges about the specific Brazilian firm, (2) whether your vendor inventory confirms or rules out use of this provider, (3) what traffic and data the provider can observe based on Step 2 findings, (4) recommended action — suspend, monitor, or terminate — with contractual basis cited. Attach the vendor contract SLA clauses governing data handling and termination rights. This brief should be delivered before any unilateral technical action to ensure leadership authorization per NIST 800-61r3 escalation procedures.

Evidence: Before briefing leadership, compile: (1) written confirmation from Step 1 of whether your organization uses the identified firm or any Brazil-registered DDoS scrubbing service, with supporting vendor records; (2) the Krebs on Security article URL and publication date as the triggering intelligence source — do not rely on paraphrased summaries; (3) a traffic exposure summary from Step 2 quantifying what categories of traffic (volumetric DDoS diversion only vs. all traffic inline) were observable to the provider, which directly informs the data exposure risk framing for leadership.

Step 5: Monitor developments — track Krebs on Security directly for the full published article and any follow-up disclosures; watch for Brazilian CERT (CERT.br) advisories, law enforcement actions, or regulatory responses naming the firm

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: maintaining situational awareness and integrating external threat intelligence to inform ongoing risk decisions

Controls: NIST IR-5 (Incident Monitoring) — track incident status and external developments, NIST SI-5 (Security Alerts, Advisories, and Directives) — receive and act on advisories from external organizations including CERT.br and law enforcement, NIST AU-6 (Audit Record Review, Analysis, and Reporting) — maintain ongoing review of internal traffic logs against newly disclosed IOCs as they emerge, CIS 7.1 (Establish and Maintain a Vulnerability Management Process) — incorporate emerging intelligence about this threat into your vulnerability and risk process

Compensating: Set up free RSS monitoring for Krebs on Security (krebsonsecurity.com/feed) and CERT.br (cert.br) using an RSS reader or a simple cron job with curl and grep alerting on the firm's name or related keywords. Monitor CERT.br's published incident statistics and advisories at cert.br/en/published for any formal disclosure. Subscribe to CISA's free alert mailing list for any US-side law enforcement or regulatory action. If the firm's name or associated ASNs become publicly confirmed, immediately query those ASNs against Spamhaus, AbuseIPDB, and Shodan (free tiers) to identify any overlap with infrastructure your organization communicates with.

Evidence: Establish a monitoring evidence baseline before this step concludes: (1) a dated snapshot of the Krebs on Security article and any follow-up posts, preserved as PDF with timestamp — this is your threat intelligence source record for audit purposes; (2) CERT.br advisory archive snapshot (cert.br/en/published) at the date of initial assessment, so any new entries can be diff'd against the baseline; (3) current Spamhaus DROP and EDROP list exports filtered for Brazilian ASNs, saved with date — provides a baseline to detect future listings of the alleged firm's infrastructure; (4) internal ticket or case record documenting this monitoring activity as an open action item per NIST IR-5 (Incident Monitoring) tracking requirements.

Detection Guidance

Because the specific firm and technical details from the Krebs article are not accessible for verification in this analysis, firm-specific IOCs cannot be confirmed. The following describes detection strategies for this threat class. For firm-specific indicators, access the primary Krebs article directly or monitor CERT.br advisories.

Network telemetry: Review outbound traffic flows to DDoS mitigation provider infrastructure. Look for unexpected traffic volumes, unusual protocol usage, or connections to IP ranges beyond what your provider's documentation describes as scrubbing infrastructure. Legitimate scrubbing services have well-defined BGP announcements and traffic paths.

BGP and routing anomalies: If your organization uses BGP-based mitigation (anycast or on-demand rerouting), audit route advertisements. Unexpected prefix announcements or route leaks from your mitigation provider's ASN warrant investigation.

DNS and infrastructure mapping: Map all domains and IP ranges operated by your DDoS mitigation vendors. Cross-reference against threat intelligence feeds for any overlap with known botnet C2 infrastructure or bulletproof hosting ASNs.

Log sources to prioritize: Netflow/IPFIX records showing traffic volumes to and from scrubbing provider infrastructure, BGP route change logs, firewall logs for provider management plane connections, and DNS query logs for provider-managed domains.

Vendor due diligence audit: Review the provider's ASN registration history, corporate registration details, and upstream transit providers. Tools such as BGPView, RIPE NCC (for LACNIC-registered resources), and Hurricane Electric BGP Toolkit can surface anomalies in provider infrastructure that warrant escalation.

Indicators of Compromise

Type	Value	Context	Confidence
URL	`Pending — refer to Krebs on Security (krebsonsecurity.com) for published indicators`	The Krebs on Security article is the primary source for firm identity, associated IP ranges, ASN details, and any infrastructure indicators published in connection with this investigation. The full article was not accessible for this analysis.	LOW

Framework Mappings

MITRE-ATTACK

- **T1583.005** — Botnet
- **T1498** — Network Denial of Service

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1583.005	Botnet	Resource-Development
T1498	Network Denial of Service	Impact

Sources

Source	URL	Tier
	https://krebsonsecurity.com/	T3
Brian Krebs - Wikipedia	https://en.wikipedia.org/wiki/Brian_Krebs	T3
Brian Krebs - SecureWorld News	https://www.secureworld.io/industry-news/author/brian-krebs	T3
'Next generation' of tech advancement comes with growing threats ...	https://www.youtube.com/watch?v=wUOOAUW5KAY	T3
Krebs on Security - Internet Salmagundi	https://internet-salmagundi.com/2019/12/krebs-on-security/	T3

Generated 2026-05-01 07:12 UTC by TJS Security Command Center