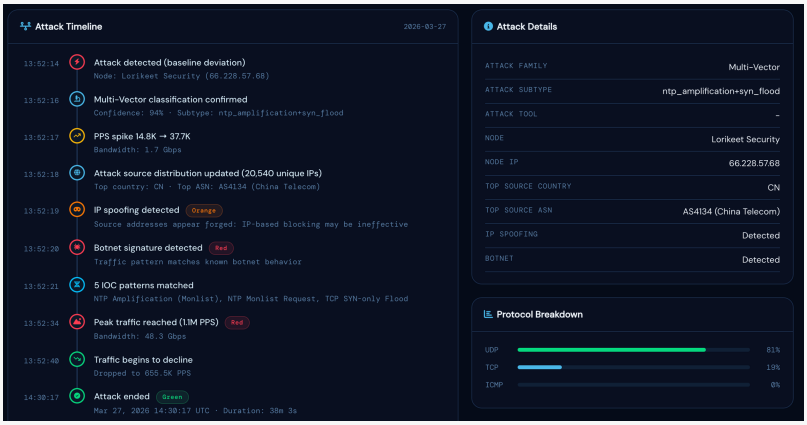
Flowtriq Detects 48.3 Gbps Multi-Vector DDoS Attack in Under One Second

Canadian cybersecurity startup stops multi-vector attack during live training event with zero service disruption



Flowtriq attack timeline · Detection 13:52:14 UTC peak traffic 48.3 Gbps resolved 14:30:17 UTC · IP spoofing and botnet confirmed

TORONTO, ONTARIO, CANADA, April 27, 2026 /EINPresswire.com/ -- Flowtriq, a real-time DDoS detection and mitigation platform headquartered in Toronto, Ontario, today announced the results of its deployment across Lorikeet Security's live cyber range infrastructure. During a March 27, 2026 public cybersecurity training event attended by 240 participants, Flowtriq detected a multi-vector DDoS attack within 0.9 seconds of the first malicious packet, automatically applied on-node mitigation rules, and pushed BGP FlowSpec drop rules to Lorikeet's upstream transit provider within 11 seconds. The training session continued uninterrupted throughout the 38-minute attack. Zero participants were disconnected.

> We had 240 people in a live cybersecurity event and took close to 50 gigabits of attack traffic mid-session. Full mitigation stack in under 15 seconds from detection. Not one participant noticed."
>
> *Ryan Wilke, CEO & Founder, Lorikeet Security*

The attack was a coordinated multi-vector campaign combining NTP amplification, peaking at 39 Gbps and 1.06 million packets per second from approximately 2,140 open NTP reflectors, with a spoofed SYN flood generating 890,000 SYN packets per second across 18,400 source IPs. Both vectors targeted the training platform and CTF challenge server simultaneously. Flowtriq identified both vectors as a single multi-vector incident within the initial 0.9-second detection cycle, enabling targeted FlowSpec rules for each vector rather than a broad blackhole response.

The incident highlights a structural gap in DDoS response. NETSCOUT's 1H2024 DDoS Threat Intelligence Report found that 70 percent of DDoS attacks last fewer than 15 minutes, while

manual response workflows typically require 15 to 30 minutes under best-case conditions. Most attacks cause their maximum damage or resolve entirely before a manual response can take effect. Flowtriq completed the full detection-to-upstream-mitigation cycle in under 12 seconds. DDoS attack volume has escalated sharply. According to Cloudflare's Q4 2025 DDoS Threat Report, the total number of DDoS attacks reached 47.1 million in 2025, a 236 percent increase over 2023. Multi-vector attacks, which combine volumetric and protocol-level components to evade single-dimension detection, are increasingly common. The Lorikeet incident is a documented example of automated multi-vector classification and mitigation operating under real-world conditions against a live production workload.

Flowtriq was founded by Jacob Masse, a cybersecurity researcher who discovered CVE-2024-45163, a CVSS 9.1 critical kill switch vulnerability in the command-and-control infrastructure of the Mirai botnet. Masse previously founded and exited AttackEngine, an anti-DDoS platform acquired within one year of launch. Flowtriq was built to address the detection speed and automation gap he observed across years of working with infrastructure operators who lacked the tooling or staffing to respond to attacks in real time.

Lorikeet Security is an Orlando, Florida-based cybersecurity firm offering offensive security services including penetration testing, red teaming, cloud and Active Directory assessments, API and mobile application testing, and attack surface management. The company also provides defensive security operations including SOC as a Service, managed detection and response, incident response, digital forensics, and threat hunting, as well as managed services such as vCISO advisory, compliance consulting, security awareness training, and code review. Founded by Ryan Wilke, Lorikeet delivers live hands-on cybersecurity training events with instructor-led adversarial exercises for enterprise security teams, government contractors, and university programs. Following the March 27 incident, Lorikeet standardized Flowtriq across all event infrastructure as a required pre-flight component.

Flowtriq is available now at flowtriq.com. Plans start at $9.99 per node per month with a 7-day free trial and no credit card required. A full technical case study is available.

Jacob Masse
Flowtriq
jacob@flowtriq.com
Visit us on social media:
LinkedIn
X
Other