

The 2026 Lumen Defender Threatscape Report: CISO Update

Stop the attack before the alert

The 2026 threatscape has changed. Established cyber threats are becoming faster, broader, and more persistent with AI.



Faster

Attackers are compressing the path from vulnerability discovery to exploitation.

<24 hours

Black Lotus Labs observed dedicated exploit servers targeting Ivanti Connect Secure services **within 24 hours** of CVE disclosure.



Broader

Automated scanning keeps constant pressure on internet-facing infrastructure.

4K

Black Lotus Labs detected **4,000 daily brute-force attacks** and exploit scanners per day in H1 2026.



More persistent

Malicious infrastructure can regenerate even after major disruption.

+112%

The IPIDEA botnet **reconstituted nearly 112%** of its ecosystem less than 6 months after large-scale disruption.

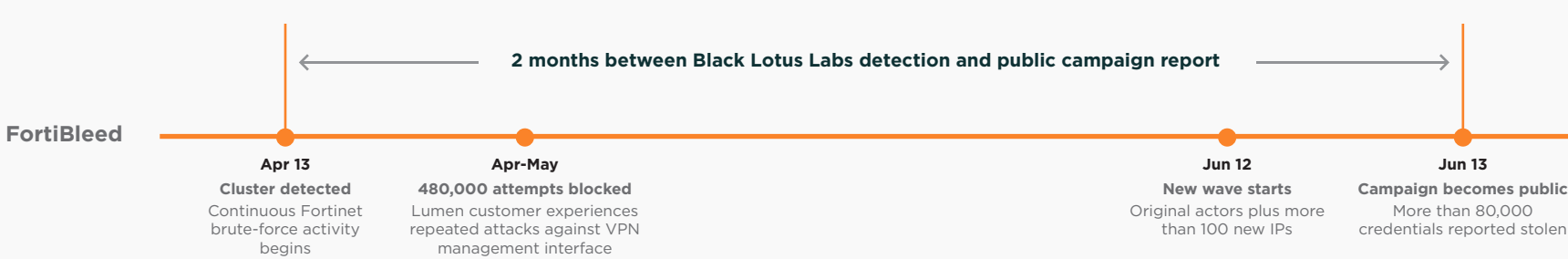
CISO takeaway: Traditional detection and response starts when malicious activity reaches the enterprise. Network-level intelligence can reveal campaigns while attacker infrastructure is still forming.

As AI accelerates established threats, CISOs can shift the advantage upstream by combining stronger posture management, proactive network-level threat intelligence, and automation to stop more attacks before they reach the SOC.

Campaign spotlights

Faster

FortiBleed: AI-accelerated attacks against exposed infrastructure

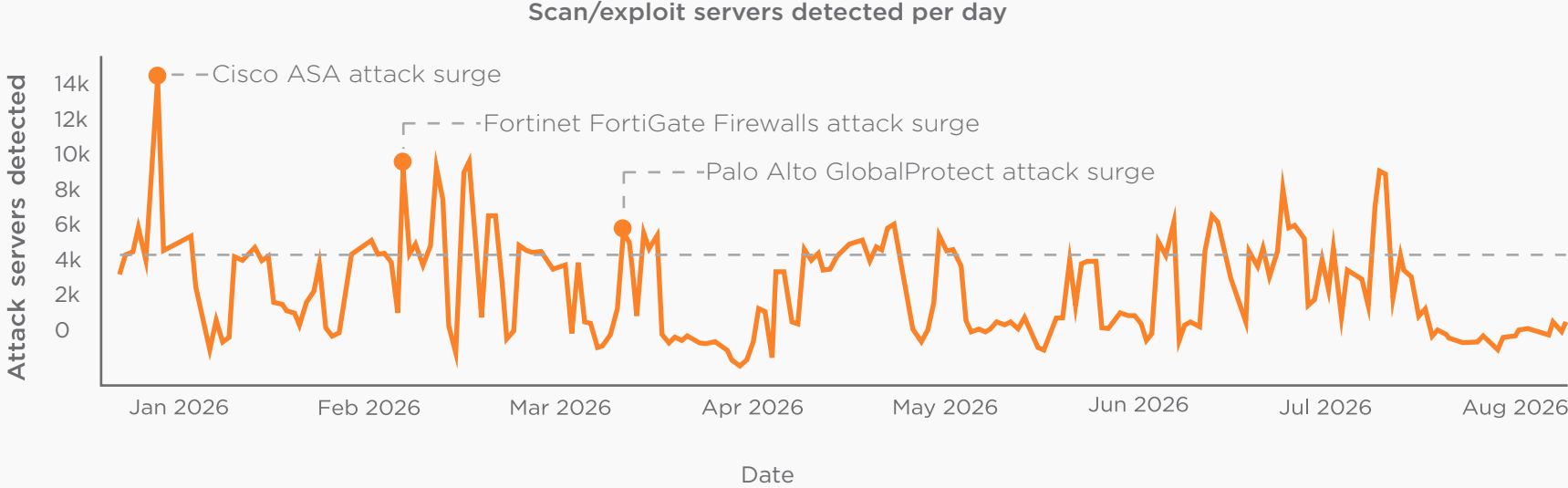


FortiBleed shows how AI can accelerate familiar attack techniques at scale, with more than 480,000 login attempts blocked against one customer and attacker infrastructure later rotating through 100+ new IPs.

For CISOs, network-level visibility can help identify those coordinated shifts early and block malicious activity upstream before it becomes a full-blown breach.

Broader

Brute force & exploit scanners: Constant pressure meets opportunistic bursts

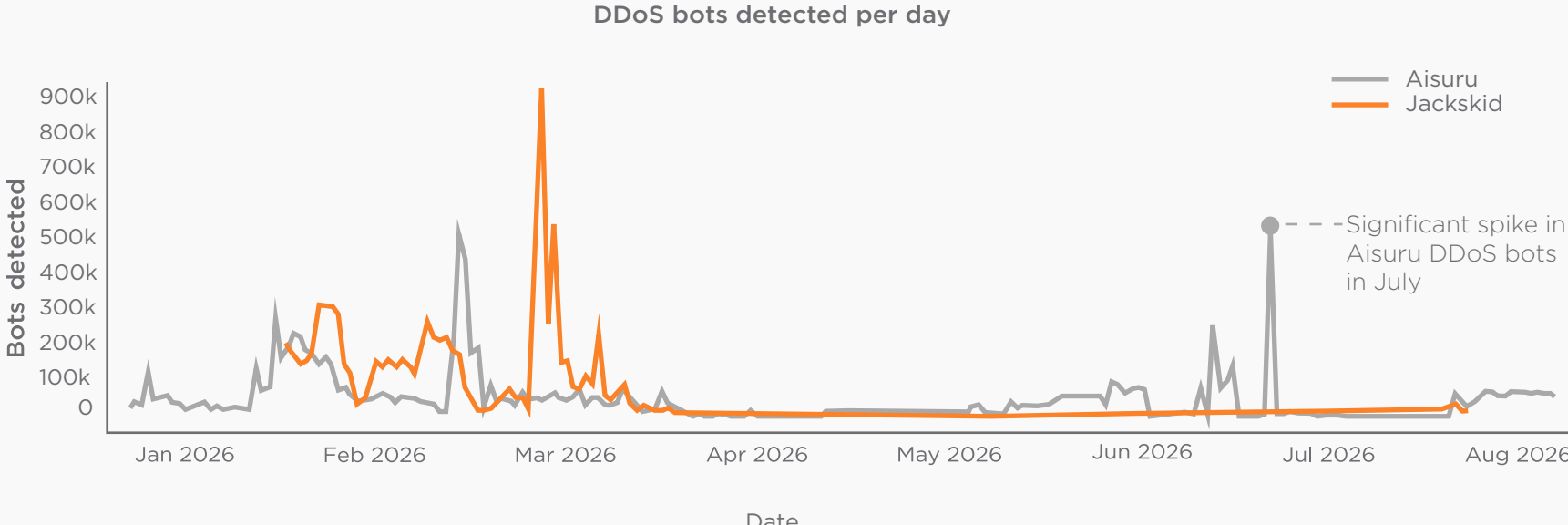


Adversaries are applying continuous pressure to internet-facing infrastructure, averaging nearly 4,000 brute-force attacks and exploit scanners per day, then surging around newly disclosed vulnerabilities and zero-days—as demonstrated by these endpoint-specific spikes.

For CISOs, that means exposure management and defensive action must be continuous enough to withstand both automated, large-scale scanning and sudden bursts of exploitation.

More persistent

Aisuru & Jackskid: DDoS regeneration at scale



Aisuru/Kimwolf and Jackskid show how DDoS botnets can rapidly rebuild as operators vary C2 techniques and recruit new devices. Black Lotus Labs partnered with law enforcement and private-sector partners to disrupt the botnets in March, including Lumen null-routing nearly 1,000 C2 servers. Yet less than 4 months later, Aisuru activity spiked again.

For CISOs, resilience means assuming capacity will re-form and continuously validating upstream mitigation, escalation paths, and service-availability plans.

Shift left with internet backbone visibility

Global internet backbone

Traffic moves across large, high-capacity networks



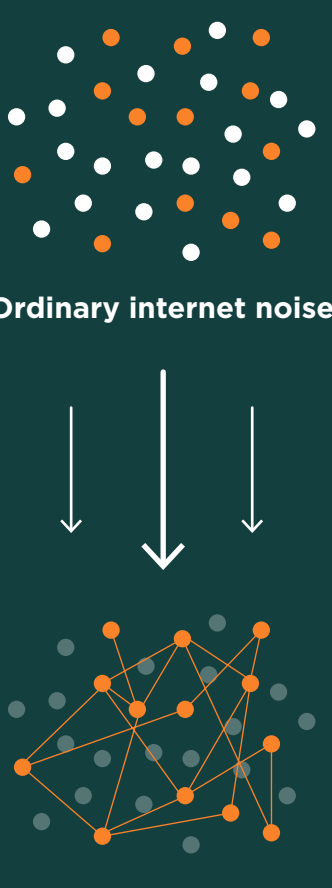
Network telemetry

Network telemetry captures signals



Analytics

Threat analysts use telemetry to identify malicious behavior



Black Lotus Labs

Detect malicious infrastructure as it forms

Block suspicious traffic upstream

- Threat intelligence research
- Automation
- Machine learning



Strengthen your defense posture for H2 2026

As AI-enabled threats become faster, broader, and more persistent, security teams must move defensive action upstream. These priorities help CISOs strengthen posture, reduce exposure, and combine network infrastructure intelligence with existing controls to stop attacks earlier.

- Lock down administrative access:** Require MFA, restrict edge management interfaces, and enforce least privilege.
- Reduce exploitable exposure:** Patch critical internet-facing vulnerabilities quickly, retire unsupported edge devices, and remove unnecessary services.
- Continuously monitor network activity:** Centralize key logs and review traffic flows for distributed, low-and-slow, or coordinated activity.
 - Lumen customers:** Use Lumen Defender Threat Feed to correlate Black Lotus Labs-profiled IPs against enterprise traffic.
- Correlate intelligence across control layers:** Connect endpoint, identity, cloud, exposure management, and network intelligence to speed investigation and blocking.
 - Lumen customers:** Review Lumen Defender-blocked IPs and extend validated blocking across other edge controls.
- Plan for regenerated DDoS capacity:** Test upstream mitigation, escalation paths, rate limits, and communications before an event.
 - Lumen customers:** Review DDoS countermeasures and alert thresholds with the Lumen SOC team.
- Prepare for extortion and supply chain compromise:** Plan for third-party compromise, data theft, supplier outages, and reputational pressure—not just restoration.
 - Lumen customers:** Use Lumen Defender AMDR to review exposure gaps and align on extortion response plans.

Download the 2026 Lumen Defender Threatscape Report: CISO Update

Download now

