NEWS RELEASE

Lumen Unveils 2026 Defender Threatscape Report: Upstream Network Visibility is the New Front Line of Cyber Defense

2026-04-07

Black Lotus Labs reveals why upstream network visibility is essential to detecting and disrupting disguised proxies, edge exposure, and AI-driven attacks

DENVER--(BUSINESS WIRE)-- As threat actors traverse the network in new and innovative ways, Lumen Technologies (NYSE: **LUMN**) today released its **2026 Lumen Defender Threatscape Report**, identifying a major shift in the digital battlefield: the most critical signals no longer live on the endpoint, but upstream in the network itself.

2026 Lumen Defender Threatscape Report

This new report, authored by Lumen's threat research and operations arm Black Lotus Labs, leverages Lumen's position as one of the world's largest internet backbone operators to track how cyber criminals have evolved into "heist crews" with industrialized operations. Most notably, it reveals critical insights into how threat actors use disguised proxies, compromised edge devices, and generative AI to pre-stage attacks.

Key Findings

The 2026 Threatscape Report identifies critical shifts in how attackers operate:

- **Generative AI as an Operational Engine**: Threat actors are using AI to iterate and regenerate malicious infrastructure at machine speed. This automation helps sustain malicious campaigns, compressing the window between exposure and impact.
- **Targeting the "Vault Door" at the Edge**: As endpoint detection and response (EDR) has matured, attackers have pivoted to internet-exposed edge devices — routers, VPN gateways and firewalls. These assets offer

privileged access, limited forensic capabilities, and typically operate outside traditional endpoint security visibility.

- **The Rise of Residentially Disguised Proxies:** Criminal and nation-state crews are industrializing proxy networks using compromised small office/home office (SOHO) devices. By hijacking these "rentable identities," attackers blend into legitimate residential traffic to bypass Zero Trust and geolocation controls.
- **Blurred Lines of Attribution:** Elite espionage campaigns are increasingly built on "stolen staging," where nation-state actors hijack criminal infrastructure to hide their fingerprints behind noisy, common criminal activity.

"As attackers shift toward internet-exposed edge infrastructure, defenders are losing visibility at a critical stage of an attack," said Nat Habtesion, SVP and chief security officer at Lumen. "By seeing attacker infrastructure as it forms at the network layer, Lumen and our Black Lotus Labs team can identify threat actors' activities early, disrupt campaigns in motion, and reduce the operational burden on security teams before damage is done."

The Professionalization of Cybercrime

The report identifies a new standard for cyber operations: the "heist crew" model. Rather than deploying standalone malware, these actors operate with the precision of a logistics firm. They use generative AI to rotate IP addresses and domain names faster than manual defenders can track, and they utilize "rentable identities" through compromised home routers to blend into everyday residential traffic. This highly professionalized setup allows attackers to remain invisible in the "staging grounds" of the network, ensuring that by the time they interact with a target, the path of least resistance has already been cleared.

The Shift to Upstream Intelligence

Traditional defense models often rely on post-infection signals from inside the network. However, the 2026 report demonstrates that by the time an alert triggers on an endpoint, the attacker's preparation — scanning, infrastructure rotation and proxy formation — is already complete.

With visibility into 99% of public IPv4 addresses and while monitoring more than 200 billion NetFlow sessions and 46,000 C2s daily, Lumen’s vantage allows Black Lotus Labs to identify coordinated infrastructure behavior as it emerges. In 2025, Lumen participated in eight multi-partner takedowns and disrupted 5,000 IPs to degrade adversary capabilities.

The report deconstructs several high-profile operations that define this new era:

- **Kimwolf:** A massive, distributed denial-of-service (DDoS) botnet that scaled to hundreds of thousands of bots

in weeks by exploiting residential proxy ecosystems. Lumen observed Kimwolf triple its bot count in just one week and launch attacks reaching 30 terabits per second (Tbps).

- **Rhadamanthys:** The largest malware-as-a-service platform by volume at the time of takedown that operates like a professional startup, complete with subscription tiers and customer support for more than 12,000 victims.
- **Raptor Train:** A nation-state botnet that utilized an enterprise-grade control center to manage over 200,000 compromised Internet of Things (IoT) devices.

"Threat intelligence is needed to find the adversary as early as possible and as close to the point of origination as possible," said Chris Kissel, IDC vice-president, Security & Trust. "Lumen's massive infrastructure and the quality of Black Lotus Labs provides optimal visibility of the IP backbone greatly reducing the odds of successful cyber-attack campaigns."

Strategic Guidance for 2026: Neutralizing the Staging Ground

Lumen recommends that organizations shift from reactive indicators to infrastructure awareness. Habtesion concluded, “Effective defense requires neutralizing the ‘staging grounds’, those upstream environments where attackers build their routes, rather than just hardening the final point of intrusion.”

The full **2026 Lumen Defender Threatscape Report** is now available for download.

About Lumen Technologies

Lumen is unleashing the world’s digital potential. We ignite business growth by connecting people, data, and applications — quickly, securely, and effortlessly. As the trusted network for AI, Lumen uses the scale of our network to help companies realize AI’s full potential. From metro connectivity to long-haul data transport to our edge cloud, security, managed service, and digital platform capabilities, we meet our customers’ needs today and as they build for tomorrow. For news and insights visit **news.lumen.com**, LinkedIn: **/lumentechnologies**, X: **@lumentechco**, Facebook: **/lumentechnologies**, Instagram: **@lumentechnologies**, and YouTube: **/lumentechnologies**.

Forward-Looking Statement

This press release includes certain forward-looking statements about future events. These forward-looking statements are not guarantees of future results, are based on our current expectations only and are subject to various uncertainties. Actual results may differ materially from those anticipated by us in these statements due to several factors, including those referenced in our filings with the U.S. Securities and Exchange Commission.

Media Contact:
Danielle Spears
Danielle.Spears@Lumen.com
321-256-3854

Source: Lumen Technologies