LUMEN

BLACK LOTUS LABS by Lumen

The 2026 Lumen Defender Threatscape Report

Why visibility at breach misses the plot

Backed by intelligence from our threat research and operations arm, Black Lotus Labs®, and our own vantage point inside a global internet backbone, Lumen has identified a major shift for 2026: **modern cyberattacks are increasingly driven by exposure, with threat actors optimizing their targeting for vulnerable edge devices and services.**

Inside Lumen's internet backbone

Lumen manages and operates one of the largest, most connected, and most deeply peered networks in the world.[1] Black Lotus Labs provides

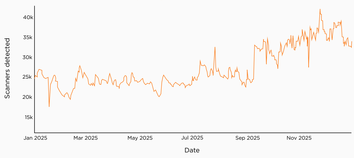
- Visibility into 99% of public IPv4 addresses
- Daily monitoring of 200B+ NetFlow sessions and DNS queries and 46,000 C2s
- Daily tracking of 2.3M unique threats
- 5000+ C2s disrupted in 2025

Top 2025 trends

1 Generative AI changed the tempo, unleashing attacks at machine speed

Threat actors embraced automated tasking, scanning, infrastructure rotation, and C2 management, in addition to adopting new generative AI-enabled attack vectors.

Total malicious scanners detected per day (2025)



Botnet operators, initial access brokers, and advanced actors use continuous malicious scanning to preemptively inventory internet-facing devices and services.

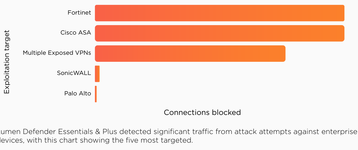
2 Attackers are moving deeper into the network itself—hiding in the infrastructure

Adversaries targeted vulnerable edge devices to "live in the middle," stealing credentials to access protected information while hiding their activity inside the connective tissue of the internet.

3 Malware-backed proxy networks became full-fledged economies of disguise

Compromised home routers, IoT devices, and high-volume VPS hosts were used to disguise attackers as trusted remote employees, bypassing geofencing, ASN-based blocking, IP reputation checks, and many Zero Trust location signals.

Top enterprise edge devices brute forcing events tracked by Black Lotus Labs (October–December 2025)



Lumen Defender Essentials & Plus detected significant traffic from attack attempts against enterprise devices, with this chart showing the five most targeted.

Continuous malicious scanning represents 33% of all malicious traffic blocked by Lumen Defender Essentials & Plus

4 Criminal ecosystems professionalized, adopting the polish of legitimate SaaS

Adversaries assembled polished platforms—complete with customer support and subscription tiers—to scale access, automate abuse, and lower the barrier to entry for cybercrime.

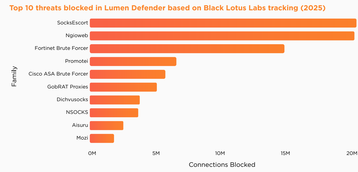
5 Nation-state & criminal crews blurred together on shared infrastructure

Nation-states piggybacked off criminal infrastructure and cybercriminals reused tooling forged by intelligence services, making criminal intent a stronger attribution signal than ownership.

6 The global backbone transformed from a conduit into an early-warning system

As adversaries weaponized routers, appliances, and management planes, the global internet backbone evolved from an invisible highway for threat actor transport into a critical detection and disruption layer.

Top 10 threats blocked in Lumen Defender based on Black Lotus Labs tracking (2025)



Note that this chart excludes blocks due to malicious scanners.

2026 threat predictions

Setup gets faster as adoption of generative AI and agents goes mainstream

We expect a sharp acceleration in AI-enabled chained exploit paths targeting edge devices and internet-exposed management interfaces, including the use of AI agents to

- Evaluate privilege levels
- Identify adjacent trust relationships
- Select the optimal exploit paths
- Adapt tactics mid-operation

Targeting will focus on opportunity at the edge

Attackers will continuously and indiscriminately scan for exposed edge devices and services. When a reachable device is found—especially one with weak authentication or missing patches—adversaries will move quickly, using whatever technique or CVE that is most effective to gain and maintain access.

The real signals lie in the network

In 2026, the earliest signals will come from collective infrastructure behavior, not device telemetry.

- Rapid C2 rotation
- Sudden proxy layer emergence
- Orchestration traffic patterns
- Coordination across geographies

The best disguises will be legitimate infrastructure

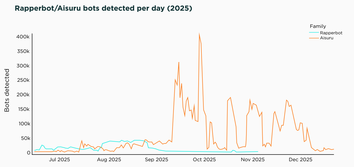
Adversaries will rely even more heavily on malware-backed proxy networks, SOHO-based botnets, hijacked VPS infrastructure, and "clean-looking" residential IP spaces to

- Obscure attribution
- Enable shared infrastructure across multiple campaigns
- Rent, trade, or reuse capabilities at scale

Campaign spotlight: Kimwolf/Aisuru

Kimwolf emerged in late 2025 as a breakaway operation from Aisuru, which, at the time, was the most powerful distributed-denial-of-service (DDoS) botnet on the internet. Kimwolf relied on a multi-layered architecture of bots, rapidly rotating domains and IPs, and malware distribution nodes.

Rapperbot/Aisuru bots detected per day (2025)



Following a law enforcement disruption of another prominent botnet, Rapperbot, in August 2025, Aisuru leveraged local-area network exploitation capabilities against large malware-backed proxy networks to rapidly expand operations. Kimwolf emerged in late September, leveraging the broader reach of devices within the Aisuru botnet to scale.

The peaks and valleys shown in the Aisuru and Kimwolf bot detection image above demonstrate the cycle of continuous discovery, null-routing, and regrowth that characterizes modern DDoS botnets.

Key takeaway: Kimwolf illustrates how botnets are shifting to prioritize regeneration speed as a primary survival trait, not just stealth. The earliest warning signs to identify Kimwolf were infrastructure choreography like proxy service probing, sudden traffic convergence, and mass malware redeployment rather than attack payloads. These signals are invisible without upstream visibility.

Bottom line?

Modern cyber threats are built long before they are launched. Adversaries are rapidly assembling infrastructure ecosystems powered by:

- Generative AI
- Resilient proxy networks
- Compromised edge devices
- Shared criminal-state platforms

Organizations that combine strong cybersecurity fundamentals with upstream visibility and infrastructure intelligence will be best positioned to shrink attacker dwell time, block malicious systems early, and stop adversarial operations before they ever reach the vault.

Discover how Lumen global internet traffic visibility unlocks early detection.

Download report

LUMEN

BLACK LOTUS LABS by Lumen

Footnotes

1. The Center for Applied Internet Data Analysis (CAIDA), AS Rank, January 2025.