PUBLIC PREVIEW — FULL BRIEF AVAILABLE TO CUSTOMERS

# AT THE EDGE

Weekly Intelligence Brief

## From Reconnaissance to Execution. Adversaries Operationalize at Scale.

This week's intelligence highlights a shift from opportunistic scanning to coordinated, targeted exploitation of enterprise perimeter devices and IoT infrastructure, with adversaries operationalizing prior reconnaissance at scale.

| 6,180,111 | 1,652,443 | +76.9% | 13x |
|---|---|---|---|
| SESSIONS FROM VISIONHEIGHT SCANNING CLUSTER | COMBINED FORTINET EXPLOITATION SESSIONS | MIRAI ACTIVITY INCREASE WEEK-OVER-WEEK | OLLAMA AI SCANNING GROWTH OVER THREE WEEKS |

### WHAT'S INSIDE

1

#### VisionHeight Cluster Targets Enterprise Perimeters

Six AWS-hosted nodes sharing a single JA3 fingerprint systematically probed Fortinet, Palo Alto, Sophos, Ivanti, Citrix, ConnectWise, and F5 appliances — covering the full enterprise perimeter stack in one coordinated operation active since January. Fortinet FortiClient EMS API Auth Bypass Check

2

#### Fortinet Multi-Vector Exploitation Intensifies

FortiClient EMS authentication bypass (CVE-2026-35616, CVSS 9.1, CISA KEV) generated 1,535,690 sessions while SSL VPN brute-forcing trended upward — creating a dual-vector attack posture against the most targeted perimeter vendor. Fortinet SSL VPN Bruteforcer

3

#### IoT Botnet Recruitment Expands Against Volume Decline

Mirai activity increased 76.9% while overall volume fell 28.3%. The VPSVAULT cluster weaponized 16+ CVEs across cameras, routers, DVRs, and NAS devices with 2,732,814 combined sessions. Mirai

4

#### AI Infrastructure Under Systematic Reconnaissance

Ollama API endpoint scanning grew 93.6% for the second consecutive week — a thirteenfold increase over three weeks — as threat actors build inventories of exposed AI inference infrastructure. Ollama API Endpoint Crawler

### Want the full brief?

GreyNoise customers get complete IOCs, infrastructure attribution, and role-based recommendations every week.

greynoise.io/contact