WEEKLY INTELLIGENCE BRIEF

AT THE EDGE

GreyNoise Research — Week of March 9, 2026

The Scanning Landscape Is Reorganizing

A single Hong Kong cloud provider surged nearly sevenfold to become the dominant source of internet scanning. RDP operators rotate faster than blocklists. Edge device exploitation enters its fourth month — and it's re-accelerating.

301.8M	439K	+578%	+90.5%
SESSIONS OBSERVED	UNIQUE SOURCE IPS	UCLOUD SURGE	SOPHOS WK 4

WHAT'S INSIDE

UCLOUD Surges 578% to #1 Scanning Source
1

A single Hong Kong cloud provider surged nearly sevenfold, deploying a new tunneled fingerprint at 29.3M sessions. Western providers declined simultaneously.

Edge Device Siege: Month 4, Re-Accelerating
2

Sophos CVE-2022-1040 nearly doubled for the 4th consecutive week. SonicWall VPN doubled. Dell NetExtender appeared for the first time. Two Cisco CVSS 10.0 CVEs on CISA KEV. State-aligned and financially motivated actors converging on the same attack surface.

RDP Operators Rotate Faster Than Blocklists
3

MEVSPACE collapsed. Its replacement disappeared. RDP scanning surged 157%. The criminal ecosystem treats infrastructure as disposable.

React2Shell Reverses Decline
4

After weeks of contraction, CVE-2025-55182 surged 56.2%. New proxy infrastructure linked to known operators suggests campaign refresh.

Get the full At The Edge brief.

Complete IOCs, infrastructure attribution, and role-based recommendations inside.

greynoise.io/contact