GREYNOISE INTELLIGENCE

March 16 – March 23, 2026

TLP:CLEAR

PUBLIC PREVIEW — FULL BRIEF AVAILABLE TO CUSTOMERS

AT THE EDGE

Weekly Intelligence Brief

Criminal Scanning Infrastructure Regenerates on Demand.

The MEVSPACE RDP operator returned from a 99.8% collapse, reconstituting scanning capacity on demand. Two new coordinated campaigns emerged simultaneously — IoT botnet recruitment and evasion-optimized scanning — revealing an industrialized attack supply chain.

200.9M	TOTAL SESSIONS OBSERVED
21+	CVES WEAPONIZED IN IOT WORM
5,854	MAX UNIQUE JA3 FINGERPRINTS PER NODE
9 Weeks	CONSECUTIVE VPN CREDENTIAL PRESSURE

WHAT'S INSIDE

MEVSPACE RDP Operator Returns After Collapse

A single IP generated 7,975,241 sessions — the highest of any source — across 10,000+ ports before going dark. Tracked since January 2026, the operator shows a repeating surge-withdraw-reconstitute cycle, reinforcing that well-resourced operators can reconstitute capacity within days. Deploy RDP Bruteforce Attempt blocklists.

VPSVAULT.HOST IoT Botnet Recruitment

Two IPs weaponized 21+ CVEs against routers, cameras, and embedded devices from 12+ manufacturers — 2,042,092 sessions linked to the RondoDox threat operator. TP-Link CVE-2023-1389 carries 13 botnet associations. Track IoT Default Password Attempt tags.

Omegatech TLS Fingerprint Randomization

Five nodes generated up to 5,854 unique JA3 fingerprints each to evade detection while conducting path traversal reconnaissance across 4,106,542 sessions. Organizations relying on fingerprint-based correlation should add behavioral heuristics. Review Path Traversal Attempt detections.

Sophos Firewall Exploitation — Fifth Consecutive Week

CVE-2022-1040 exploitation reached 638,654 sessions with an additional 402,098 User Portal scanning sessions — over 1 million combined. After four weeks of acceleration, activity is stabilizing at an elevated baseline. Patch immediately and restrict management interfaces. Deploy Sophos CVE-2022-1040 RCE blocklists.

Want the full brief?

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

greynoise.io/contact