PUBLIC PREVIEW — FULL BRIEF AVAILABLE TO CUSTOMERS

AT THE EDGE

Weekly Intelligence Brief

The Pressure Was on Remote Access.

This week's highest-intent activity targeted the login surfaces of remote access — RDP, enterprise SSL VPN, and router management — not any new vulnerability. A single host produced more than a quarter of all RDP-crawling traffic GreyNoise observed: 4.18 million sessions in a 48-hour burst, then silence. Enterprise SSL VPN portals from every major vendor drew six-figure credential pressure, and a MikroTik RouterOS brute-force campaign ran for a third straight week. The actionable intelligence is the specific IPs, ASNs, and behavioral tags to hunt — not another hardening checklist.

>25%	6	1.5M	317M
OF ALL RDP-CRAWLING TRAFFIC THIS WEEK CAME FROM ONE HOST (4.18M SESSIONS)	ENTERPRISE SSL VPN SURFACES UNDER SIX-FIGURE CREDENTIAL & SCANNING PRESSURE	MIKROTIK ROUTEROS BRUTE-FORCE SESSIONS FROM TWO IPS — THIRD WEEK RUNNING	TOTAL SESSIONS ACROSS 1.55M SOURCE IPS — WITHIN THE NORMAL WEEKLY RANGE

WHAT'S INSIDE

1 One Host, a Quarter of All RDP Crawling

94.102.49.82 (AS202425, Netherlands, malicious) generated 4,180,759 sessions — RDP Crawler 3.13M plus RDP Bruteforce 280K — more than a quarter of all RDP-crawling traffic GreyNoise recorded this week, across a wide port range, concentrated in a 48-hour burst then silent.

2 Enterprise SSL VPN Portals Under Credential Pressure

Fortinet (686K) and Cisco (401K) drew six-figure SSL VPN brute-forcing; SonicWall (325K login / 331K API), Cisco ASA (264K), and Palo Alto (255K) drew six-figure login and API scanning of the same portals. Apply GreyNoise dynamic blocklists for the Fortinet, Cisco, SonicWall, and Palo Alto login-scanner tags — the distributed source pattern makes tag-based blocking the primary lever.

3 MikroTik RouterOS Brute-Force — Third Week

Two hosts (45.198.224.18 NL, 45.205.1.5 BR) on TCP/8728 accounted for nearly all of the dataset's RouterOS brute-force sessions this week.

4 Rented Hosting Out-Rotates Reputation Feeds

Eight of the ten busiest sources are classified malicious and a ninth suspicious; all sit on rented hosting, mostly in the Netherlands. Apply GreyNoise dynamic blocklists for the relevant tags — the IPs rotate, the tag-based coverage does not.

Want the full brief?

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

greynoise.io/contact