PUBLIC PREVIEW — FULL BRIEF AVAILABLE TO CUSTOMERS

AT THE EDGE

Weekly Intelligence Brief

Rented Recon Is Cataloging the Edge.

Rented, disposable infrastructure spent the week methodically inventorying the edge — routers, VPN gateways, and container control planes — to build the target lists that precede intrusion. That reconnaissance was the week's standout development. The window before operators return to use those lists is the most cost effective time to act.

+85%
ROUTEROS BRUTE-FORCE, REVERSING ITS DECLINE

–59%
VISIONHEIGHT RECON CONTRACTED TO TWO NODES

5 vendors
VPN/FIREWALL FAMILIES UNDER SUSTAINED RECON

Container planes
KUBERNETES/DOCKER RECON NOW FROM A HIJACKED CONSUMER LINE

WHAT'S INSIDE

1 MikroTik RouterOS Brute-Force Reverses Its Decline

The long-running VPSVAULT operation (AS215925) added a second RouterOS Bruteforcer node this week, pushing the tag to 1,938,001 sessions from 1,049,230 in the prior brief — reversing a multi-week decline. Both nodes hit the management API on TCP/8728 and nothing else (the 8th-busiest port, 4,830,676 sessions). The pattern fits building router-based proxy infrastructure for follow-on operations, not chasing one victim.

2 Enterprise VPN and Firewall Reconnaissance Persists

A fingerprinted Netherlands cluster methodically cataloged Fortinet, Ivanti, Pulse Secure, Sophos, and F5 appliances — running authentication-bypass checks and version scans, including Palo Alto PAN-OS GlobalProtect (CVE-2020-2034). The Fortinet SSL VPN Bruteforcer tag logged 875,138 sessions ecosystem-wide. This is the initial-access gear whose exploitation repeatedly precedes ransomware.

3 Telnet Leads Volume; a Tracked telnetd Flaw Persists

Telnet stayed the loudest surface — the Telnet Protocol tag logged 19,612,395 sessions and TCP/23 was the second-busiest port. Low-level probing continued for the previously flagged GNU inetutils telnetd out-of-bounds write (CVE-2026-32746, CVSS 9.8), minimal in volume today but high-impact if weaponized.

4 Container-Plane Recon Spreads to Hijacked Broadband

Dedicated Kubernetes Crawler and Docker API reconnaissance ran from a likely-compromised consumer broadband host — the only consumer-ISP address among the 20 busiest sources, and a residential origin that blends into normal traffic and is harder to filter than rented hosting.

Want the full brief?

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

greynoise.io/contact