PUBLIC PREVIEW — FULL BRIEF AVAILABLE TO CUSTOMERS

Weekly Intelligence Brief

One Fingerprint. Four Attack Categories.

A single JA4T signature linked React, Fortinet, Palo Alto, and ENV campaigns across 3.3 million sessions. Combined with a 20M-session VNC reconnaissance surge and two-week RouterOS persistence, this week confirms coordinated operations targeting enterprise infrastructure at scale.

20M	3.3M	2.2×	14 Days
VNC RECON SESSIONS	CROSS-CAMPAIGN FINGERPRINT	TRAFFIC SPIKE	ROUTEROS PERSISTENCE

WHAT'S INSIDE

1 20 million VNC reconnaissance sessions from one ASN

Netherlands-based infrastructure systematically enumerated VNC ports 5900-5920 with uniform distribution across ~100 IPs. Reconnaissance at this scale typically precedes credential attacks.

2 Same infrastructure, two weeks running

MikroTik RouterOS brute force IPs from last week's brief continued without pause. 1.1 million authentication attempts. One IP dropped; new one emerged. Deliberate infrastructure management.

3 React exploitation declined 38% but persists

1 million CVE-2025-55182 attempts from the same top IPs. Three scanners rotate through 11 identical user agents spanning 6 platforms — a pattern consistent with LLM-generated evasion lists.

4 Enterprise VPNs under sustained pressure

585,000 combined sessions targeting Palo Alto GlobalProtect and Fortinet SSL VPN. Same IP ranges observed last week — persistent scanning infrastructure.

Want the full brief?

GreyNoise customers get complete IOCs, infrastructure attribution, JA4T fingerprints, and role-based recommendations every week.

greynoise.io/contact