PUBLIC PREVIEW — FULL BRIEF AVAILABLE TO CUSTOMERS

AT THE EDGE

Weekly Intelligence Brief

Three Campaigns. One Fingerprint.

React exploitation, VPN brute forcing, and router scanning all traced back to the same network signature. What looked like separate campaigns was coordinated infrastructure.

1.7M	506K	1.8M	3
REACT ATTACKS	VPN TARGETS	ROUTER ATTEMPTS	IPS BEHIND 99%

WHAT'S INSIDE

PREVIEW

1 — 1.7 million React exploitation attempts

CVE-2025-55182 with CVSS 10.0. 179,000 sessions included actual command injection. Metasploit module available. One hosting provider generated 57% of traffic.

2 — Enterprise VPNs under sustained pressure

Fortinet SSL VPN and Palo Alto GlobalProtect both targeted. 506,000 combined sessions. Fortinet attacks up 25% from baseline. VPN credentials remain ransomware's front door.

3 — Three IPs generated 1.8 million router attacks

MikroTik RouterOS brute force campaign with a 64,000:1 session-to-IP ratio. Compromised routers become pivot points for lateral movement and botnet recruitment.

4 — Same fingerprint across all three campaigns

JA4T signature linked React RCE, VPN brute force, and ENV crawling to shared infrastructure. Organized operations, not opportunistic scanning.

Want the full brief?

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

greynoise.io/contact