PUBLIC PREVIEW — FULL BRIEF AVAILABLE TO CUSTOMERS

AT THE EDGE

Weekly Intelligence Brief

One Netherlands /24 Outweighed the Next Four Emitters Combined. Concentration, Not Novelty.

A paired-IP set in 85.11.167.0/24 (Netherlands, AS209630, hosting) produced roughly 3% of the entire weekly corpus while Fortinet SSL VPN bruteforcing led the enterprise edge by 4.7x over Cisco and 8.5x over Palo Alto. WannaCry-family SMB probing held steady at 2.6M sessions nine years after the original outbreak, and an eight-IP GCP subset spread across eight regional prefixes added another ~3.4M sessions. The infrastructure is rented and disposable; the targets are stable and well understood.

3.0%	4.7x	8.5x	2.6M
OF WEEKLY CORPUS FROM ONE /24 PAIR	FORTINET VS CISCO SSL VPN BRUTEFORCE	FORTINET VS PALO ALTO LOGIN SCANNER	WANNACRY-FAMILY SMB PROBES — 9 YRS ON

WHAT'S INSIDE

1 Netherlands /24 pair tops the week at 7.2M sessions — paired coverage across two target categories

Two IPs in 85.11.167.0/24 (.7 + .11; AS209630, Netherlands hosting per GreyNoise) generated 7,190,652 combined sessions — 4.1x the next-largest single emitter and ~3.0% of the 243M-session week. GreyNoise classifies .7 malicious (16 tags, web-exploitation + embedded/IoT focus including CGI Script Scanner, ${IFS} RCE, Telnet Bruteforcer, Shenzhen TVT, Hytec CVE-2022-36553) and .11 suspicious (7 tags, enterprise focus including Redis, PAN-OS CVE-2020-2034, SQL injection, TLS/SSL Crawler). Shared /24, shared ASN, complementary primary scans. .11 has been tracked since the 26 April brief; .7 first seen by GreyNoise 9 May.

2 Fortinet SSL VPN bruteforce leads enterprise edge pressure

The Fortinet SSL VPN Bruteforcer tag drew 832,516 sessions — 4.7x Cisco SSL VPN Bruteforcer and 8.5x Palo Alto Networks Login Scanner volume. Vendor-narrowed credential pressure on the largest enterprise install base; verify MFA on every internet-facing FortiGate this week.

3 WannaCry-family SMB probing sustains 2.6M sessions

The WannaCry Variant SMB Connection Attempt tag drew 2,612,131 sessions and sits inside 13.1M sessions of SMBv1 Crawler activity. Operators don't run MS17-010 targeting at this volume unless internet-exposed SMBv1 endpoints are still being found at density.

4 Eight GCP IPs across eight regional prefixes — single-tenant pattern

Eight Google Cloud IPs across the 34.32 / .35 / .87 / .97 / .116 / .142 / .151 / .176 regional ranges produced ~3.4M combined sessions — consistent with one tenant pre-positioning across cloud regions to survive single-region blocks.

Want the full brief?

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

greynoise.io/contact