PUBLIC PREVIEW — FULL BRIEF AVAILABLE TO CUSTOMERS

AT THE EDGE

Weekly Intelligence Brief

Credential Discovery, VNC Exposure, and a New Multi-Cloud Scanning Framework.

A ~6.2M-session credential and configuration discovery campaign ran across hundreds of IPs. Port 5900 (VNC) ranked third-most-targeted on the internet at 17.4M sessions. A new four-IP multi-cloud scanning framework activated this week, sharing identical JA4T/JA4H/JA3 across Poland and Singapore. IoT worm operators weaponized a new critical RCE.

6,228,817
CREDENTIAL / CONFIG DISCOVERY SESSIONS (ENV, .GIT, AWS, PATH TRAVERSAL)

17,375,937
PORT 5900 (VNC) SESSIONS — 3RD MOST-TARGETED

8,678,148
MULTI-CLOUD SCANNER SESSIONS — 4 IPS, SHARED JA4T/JA4H/JA3

CVE-2025-54322
NEW XSPEEDER SXZOS RCE (CVSS 10.0) WEAPONIZED IN VPSVAULT IOT WORM

WHAT'S INSIDE

1 Broad Credential and Configuration Discovery Campaign

Parallel scanning across ENV files, .git/config, AWS metadata, path traversal, and generic sensitive file access ran at approximately 6.2 million combined sessions — distributed across hundreds of source IPs rather than concentrated in a single cluster. The biggest real story of the week. Audit internet-facing web paths for exposed configuration files and rotate any credentials suspected of exposure.

2 VNC Endpoint Discovery at Top-Three Port Rank

Port 5900 recorded 17,375,937 sessions this period, ranking third-most-targeted on the internet behind only SSH and SMB. RFB Protocol tag generated 4,305,556 sessions (scanners negotiating the VNC protocol), while VNC-specific authentication tags remained nearly empty — exposure-surface mapping, not password guessing. Not documented in prior briefs. Block ports 5900–5908 at the perimeter.

3 New Multi-Cloud Scanning Framework Activated

A four-IP cluster sharing identical JA4T `1025_2_1460_0`, JA4H `ge10nn020000_db6abae5e99a`, and JA3 `9812cdc989e02988bd1f0734fb6ed1a5` generated 8.7 million combined sessions across Poland (87.251.64.159, new April 7) and DigitalOcean Singapore (167.172.65.202, 128.199.240.7, 152.42.238.0). Raw-SYN kernel-bypass toolkit, structurally similar to Masscan. Shared tooling confirms common software, not necessarily a common operator.

4 VPSVAULT IoT Exploitation Platform Continues

Three IPs in the 45.205.1.0/24 range on VPSVAULT.HOST LTD (AS215925, Brazil) generated 3,352,578 combined sessions deploying 18+ CVE exploits against routers, cameras, NAS devices, and embedded systems. Newly weaponized: CVE-2025-54322 (Xspeeder SXZOS RCE, CVSS 10.0). Also in payload: trending CVE-2026-24061 (GNU telnetd, CISA KEV). Confirmed Mirai node 36.25.240.114 added 851,713 sessions of Telnet default-credential stuffing this period.

Want the full brief?

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

greynoise.io/contact