PUBLIC PREVIEW — FULL BRIEF AVAILABLE TO CUSTOMERS

AT THE EDGE

Weekly Intelligence Brief

Attackers Found the AI Stack. Everything Else Got Worse.

AI infrastructure joined the attack surface this week as threat actors systematically mapped Ollama model servers, coding assistant credentials, and notebook environments — while ICS scanning hit three-week highs and legacy protocol worms surged 52.8 million sessions.

279.5M	+374%	828K	52.8M
SESSIONS OBSERVED	OLLAMA MODEL ENUM SURGE	ICS/SCADA SESSIONS	MULTI-PROTOCOL SURGE SESSIONS

WHAT'S INSIDE

1 Threat actors are systematically harvesting AI infrastructure

Ollama model server scanning reached 51,801 sessions (+37.9%), with the /api/tags model enumeration endpoint surging +374%. For the first time, GreyNoise observed scanning for AI coding assistant configuration files — Cline, Aider, and Cursor — targeting API keys, conversation histories, and cloud credentials. Specialized scanning tooling (ollama-audit/1.0) confirmed purpose-built AI reconnaissance.

2 ICS/SCADA scanning volumes surged — but mostly benign

Combined ICS sessions hit 828,696 (+513%), but the dominant DigitalOcean/Linode cluster (89–99.8% of Cisco Smart Install, Veeder-Root ATG, and iSCSI traffic) is consistent with benign internet scanning platforms. The genuinely malicious development: Chimay Red MikroTik exploitation exploded +1,103% as two command IPs directed 6,046 compromised routers.

3 Multi-protocol worm activity produced 52.8 million sessions

SMBv1 (+197%), DCERPC (+199%), RFB/VNC (+250%), and Telnet (+207%) surged simultaneously. Thirty-nine of the top 50 source IPs are shared between SMBv1 and DCERPC — self-propagating Windows worm activity from residential ISPs in Vietnam, India, Russia, and Egypt.

4 Sophos exploitation and VPN credential pressure continue escalating

Sophos CVE-2022-1040 RCE sessions reached 357,762 (+71.2%), marking three consecutive weeks of escalation. Enterprise VPN credential pressure hit 1,527,864 sessions (+28.5%) across five vendors. MEVSPACE — the dominant RDP brute-force operator — collapsed 99.8%.

Want the full brief?

GreyNoise customers receive the complete At The Edge brief every week: full IOCs, infrastructure attribution, JA4 fingerprint analysis, and role-based recommendations for every team from CISO to SOC to threat hunters.

greynoise.io/contact

© 2026 GreyNoise, Inc.