GREYNOISE INTELLIGENCE

February 2–9, 2026

TLP:CLEAR

PUBLIC PREVIEW — FULL BRIEF AVAILABLE TO CUSTOMERS

Weekly Intelligence Brief

Three Campaigns. One Has Cobalt Strike Ready.

Ivanti Connect Secure exploitation from three independent operators—Netherlands malware delivery, Russian OAST testing with 352 callback domains, and US infrastructure co-located with active Cobalt Strike C2. Combined with a 113% RDP surge and coordinated n8n exploitation, attackers are building target lists across enterprise infrastructure.

29.9M	113%	83K	352
RDP ATTEMPTS	WEEK-OVER-WEEK SURGE	N8N EXPLOITS	OAST CALLBACK DOMAINS

WHAT'S INSIDE

1 RDP attacks more than doubled in one week

29.9 million password-guessing attempts against Remote Desktop—up 113% from 14 million last week. One IP generated 6.75 million sessions alone. Exposed RDP remains the #1 ransomware entry point.

2 Ivanti 'Three-Headed Hydra' with C2 linkage

Three independent campaigns targeting CVE-2026-1281: Netherlands malware delivery, Russian blind testing (352 OAST domains), and US scanning co-located with active Cobalt Strike on port 34473.

3 n8n exploitation from coordinated infrastructure

83,334 attempts against CVE-2026-21858 from a single /24 block (AS211590). Workflow automation platforms hold API keys and credentials to everything. 33 days from disclosure to mass exploitation.

4 Rondodox botnet joins React2Shell

44,763 sessions from the Rondodox botnet using the same JA4T fingerprint as December's IAB campaign. When botnets adopt a CVE, exploitation scales. 1.88M total React sessions.

Want the full brief?

GreyNoise customers get complete IOCs, infrastructure attribution, the Three-Headed Hydra breakdown, and role-based recommendations every week.

greynoise.io/contact