PUBLIC PREVIEW — FULL BRIEF AVAILABLE TO CUSTOMERS

AT THE EDGE

Weekly Intelligence Brief

One Fingerprint Links a 64-Host Secret-Harvesting Fleet

GreyNoise has tracked this credential-harvesting fleet since early July; this week one TLS client fingerprint and an identical toolkit link 64 rented hosts running as a single operation. Separately, one coordinated cluster of 300 hosts probed Citrix and Palo Alto gateways together, and two WordPress Core flaws that chain toward remote code execution stayed under probing after their CISA KEV listing.

64	300	10.0	3
HARVESTING HOSTS LINKED BY ONE TLS FINGERPRINT AND TOOLKIT	HOSTS PROBING CITRIX AND PALO ALTO GATEWAYS AT THE SAME TIME	CVSS OF THE WEBLOGIC FLAW THE FLEET KEEPS PROBING	KEV-LISTED FLAWS UNDER PROBING THIS WEEK

WHAT'S INSIDE

1 A 64-host fleet under one fingerprint

One TLS fingerprint and an identical toolkit link 64 hosts running as a single credential-harvesting operation on rented infrastructure across several providers (Bucklog SARL, the 3xK Tech range). It crawls for exposed secret files at volume, driving about 6% of everything GreyNoise observed. Hunt the shared fingerprint across providers.

2 One cluster, two vendor gateways

A separate cluster of 300 rented hosts probed Citrix NetScaler and Palo Alto Networks GlobalProtect at once, every host carrying both a CitrixBleed 2 (CVE-2025-5777, CISA KEV) exploit attempt signature and a GlobalProtect login scanner signature, from United States and Nordic hosting.

3 WordPress Core KEV flaws still probed inside the KEV clock

Two WordPress Core flaws added to CISA's Known Exploited Vulnerabilities (KEV) catalog on 20 July kept drawing probing this week: CVE-2026-60137 (SQL injection), roughly 95 non-research sources, and CVE-2026-63030 (CVSS 9.8), which chains with it toward remote code execution. WordPress Core runs a very large share of public websites.

4 Hunt the fingerprint and tags as the IPs rotate

Each operation is defined by a durable behavior, a shared fingerprint or a co-occurring signature set, that persists as source addresses rotate. Last week's highest-volume brute force source, a United States ISP host, is still active but down about 73%.

Want the full brief?

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

greynoise.io/contact