PUBLIC PREVIEW | FULL BRIEF AVAILABLE TO CUSTOMERS

AT THE EDGE

Weekly Intelligence Brief

Adversaries Asked for the Keys. No Flaw Required.

Credential collection was the highest-volume malicious activity this period, and almost none of it required a vulnerability. Environment files, cloud configuration and repository configuration hold credentials for other systems, and a correctly functioning web server returns them to anyone who asks for the right path. A patch queue never sees any of this.

64 in 1 day
KEV BYPASS SOURCES, 0 TO 1 EVERY OTHER DAY

2 in 3
OF FORGED GOOGLEBOT TRAFFIC, FROM 9 HOSTS

24%
OF ALL GIT CONFIG HARVESTING, ONE HOST

2 of 4
FINDINGS THAT NEEDED NO VULNERABILITY

WHAT'S INSIDE

1 A KEV-listed GlobalProtect bypass arrived as a one-day cohort

Adversaries attempted CVE-2026-0257 in Palo Alto Networks PAN-OS from 64 sources on 02 September. The flaw is rated CVSS 9.1, has been in CISA KEV since May 2026, and CISA records known ransomware use. One source or none arrived on every other day of the window, and all 65 sources GreyNoise observed classified malicious.

2 Nine rented hosts forged Googlebot to harvest secrets

Rented hosts on one network presented themselves as Googlebot while requesting environment files and cloud configuration. Those nine hosts produced roughly two thirds of all forged search engine crawler traffic GreyNoise observed, and the forged identity covered 63% of everything they sent. Relax rate limiting or logging by user agent, and this traffic gets the same treatment.

3 One cloud host ran four unrelated sweeps at one volume

A single cloud-hosted source paired Oracle WebLogic remote code execution attempts with enumeration of an unauthenticated Cisco switch provisioning service. It supplied 36% of all attempts GreyNoise observed against CVE-2018-2628 and 35% of all switch provisioning enumeration. Four unrelated target classes sat within 337 connection attempts of one another, consistent with one scheduled pass.

4 A short-lived host took a quarter of all repository harvesting

A source that appeared on 01 September requested repository configuration files from web roots across a seven-day span. It contributed 24% of all such activity in the corpus before going quiet. This class of collection, alongside environment file crawling, is the largest malicious-intent volume of the period and maps to no CISA KEV entry.

Want the full brief?

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

greynoise.io/contact