PUBLIC PREVIEW — FULL BRIEF AVAILABLE TO CUSTOMERS

AT THE EDGE

Weekly Intelligence Brief

Twin Crawlers Probe for Credentials and Keys at the Edge.

A matched pair of web crawlers sharing one client fingerprint probed NGINX UI and LiteSpeed Cache for two critical unauthenticated flaws that leak administrative credentials, private keys, or session material, running the same toolkit from two different hosting providers. In parallel, an RDP brute force cohort spread across three networks under one transport fingerprint, a fresh host masked command injection probes as Googlebot traffic, and a secret harvesting pair was linked by a shared fingerprint. Every primary source ran on short-lived rented hosting.

9.8	1 → 3 networks	1-day	Behavioral
CVSS OF BOTH TWIN-CRAWLER WEB FLAWS	RDP BRUTE FORCE COHORT SPREAD IN A WEEK	LIFESPAN OF THE GOOGLEBOT-MASKING HOST	THE DURABLE SIGNAL, NOT IP ADDRESSES

WHAT'S INSIDE

1 A Twin Crawler Pair Probes NGINX UI and LiteSpeed for Credentials

Two crawlers, 159.89.117.80 (DigitalOcean) and 161.97.74.198 (Contabo), ran an identical toolkit against NGINX UI (CVE-2026-27944) and LiteSpeed Cache (CVE-2024-44000), both CVSS 9.8 flaws that disclose credentials, keys, or session material. They share one JA4H fingerprint, and the credential exposure risk sat in this mid-volume pair, not the week's highest-volume sources.

2 An RDP brute force cohort spread across three networks

The remote desktop cohort reported last week on a single hosting block spread across AS215929, AS35042, and AS49434 while keeping one shared transport fingerprint. Each host runs 95% or more RDP crawling with a small brute force fraction. A per-ASN block lags the next provider hop; a detection on the shared JA4T plus RDP crawling behavior is the control that survives it.

3 A fresh host masked command injection probes as Googlebot

A BytePlus host, 101.47.13.192, appeared one day before the window closed and wrapped command injection and configuration file collection inside traffic impersonating Googlebot. The single day lifespan and search engine cover are the tradecraft; organizations that allowlist Googlebot by user-agent should verify inbound claims against Google's published crawler ranges.

4 A German hosted secret harvesting pair linked across a second host

The source 213.209.159.175, tracked across prior briefs, was linked this week to a second host on AS208137, 213.209.159.154, by a shared client fingerprint. Both share the same JA4H and sweep exposed web apps for .env files, Git and SVN configuration, and framework debug interfaces. The newly linked second node is the development, not a new discovery.