PUBLIC PREVIEW — FULL BRIEF AVAILABLE TO CUSTOMERS

Weekly Intelligence Brief

IoT, Edge, Credentials. All Surging at Once.

Three attack surfaces accelerated simultaneously: IoT botnet recruitment surged up to 91%, Fortinet VPN brute-forcing nearly doubled, and credential harvesting more than doubled to 8.28 million sessions. Meanwhile, a coordinated Iranian scanner cluster deployed custom tooling unknown to any public database, and an 84-day C2 operation was uncovered hiding behind cryptocurrency exchange API traffic.

91%	98%	8.28M	84
IOT DEFAULT PASSWORD SURGE	FORTINET VPN BRUTE-FORCE INCREASE	CREDENTIAL HARVESTING SESSIONS	DAYS OF CRYPTO C2 BEACONING

WHAT'S INSIDE

1 IoT botnet recruitment accelerating for second straight week

Five IoT-related tag categories surged 53–91% WoW — Telnet Protocol, IoT Default Password, and ADB Check all rose in lockstep, consistent with centralized botnet orchestration.

2 Enterprise edge under multi-vendor credential storm

Fortinet SSL VPN brute-forcing nearly doubled. A brand-new SonicWall scanning campaign emerged from zero to 199,743 sessions. Cisco and Palo Alto pressure steady.

3 Credential harvesting more than doubled across every category

ENV Crawler surged 112% to 4.29 million sessions. WordPress Enumeration up 273%. AWS credentials, Git repos, and Spring Boot actuators all targeted.

4 84-day crypto exchange C2 operation uncovered

A Japanese-hosted server impersonated BitMart, KuCoin, and Bitget APIs across four parallel channels — sending identical static trading payloads to disguise C2 callbacks as legitimate financial API traffic.

Want the full brief?

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

greynoise.io/contact