PUBLIC PREVIEW, FULL BRIEF AVAILABLE TO CUSTOMERS

AT THE EDGE

Weekly Intelligence Brief

Operators Are Targeting the Products Exposed at the Network Edge.

The signal this week was targeting, not volume. One host quietly inventoried the full perimeter stack, a two-node pair shared tooling against an internet-facing camera RCE, and credential pressure on enterprise VPN logins held steady. The infrastructure is rented and rotates fast, so the durable defense is patching the targeted products and detecting on behavior.

1 host
SWEPT THE FULL ENTERPRISE-EDGE PRODUCT STACK IN A SINGLE WEEK

CISA KEV
HIKVISION CAMERA RCE BACK AT SCALE FROM A SHARED-TOOLING PAIR

Multi-week
SUSTAINED CREDENTIAL PRESSURE ON ENTERPRISE VPN LOGINS

WHAT'S INSIDE

1 One Host Mapped the Enterprise Edge

A single host probed the full perimeter stack, VPN gateways, application delivery controllers, file-transfer appliances, and webmail, in a tight one-week sweep. Per-product volume was low; the breadth is the tell of a target list being built.

2 Hikvision Camera RCE Back at Scale

Two hosts on separate Netherlands networks ran the same Hikvision camera exploit (CVE-2021-36260, CISA KEV) with shared tooling. Despite restrictions by the U.S. and allied governments, Hikvision cameras remain widely deployed across commercial and critical infrastructure networks.

3 Enterprise VPN Logins Under Sustained Pressure

Credential attacks on Palo Alto, Cisco, and SonicWall remote-access portals held steady across multiple briefs. The edge portal stays the most consistently targeted entry point GreyNoise observes.

Read the full brief

GreyNoise At The Edge is our weekly intelligence brief. Get the complete findings, IOCs, infrastructure attribution, and role-based actions.

greynoise.io