PUBLIC PREVIEW — FULL BRIEF AVAILABLE TO CUSTOMERS

Weekly Intelligence Brief

The Scanning Landscape Collapsed. Enterprise Campaigns Intensified.

Global scanning volume cratered 37% in a single day as major operations went dark. But Sophos exploitation surged 435%, RDP scanning hit 9.1 million sessions, and VPN credential campaigns entered their sixth consecutive week — confirming dedicated infrastructure independent of the broader scanning ecosystem.

268M	435%	9.1M	Week 6
SESSIONS OBSERVED	SOPHOS SURGE	RDP SESSIONS	VPN SIEGE

WHAT'S INSIDE

Sophos firewall exploitation intensified for the second consecutive week

1

Combined CVE-2022-1040 exploitation and user portal probing reached 276,358 sessions — a fivefold increase targeting enterprise perimeter infrastructure that provides direct access to internal networks.

One RDP operation from two IPs generated 9.1 million sessions

2

A dedicated MEVSPACE scanning operation dominated sensor traffic for the second straight week, pushing port 3389 from the 13th to the 3rd most-targeted destination port. Exposed RDP remains the primary ransomware entry vector.

VPN credential siege rotates to new vendors

3

Scanning pressure against Cisco and Palo Alto portals climbed while SonicWall activity declined 86% following GreyNoise's published analysis. Sophos emerged as a significant new rotation target.

Global scanning infrastructure reshuffled overnight

4

A custom SYN scanner collapsed 86%, UCLOUD declined 63%, and ColoCrossing nearly disappeared — yet enterprise-targeted campaigns intensified against the declining backdrop, revealing which operations run on dedicated infrastructure.

Want the full brief?

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

greynoise.io/contact