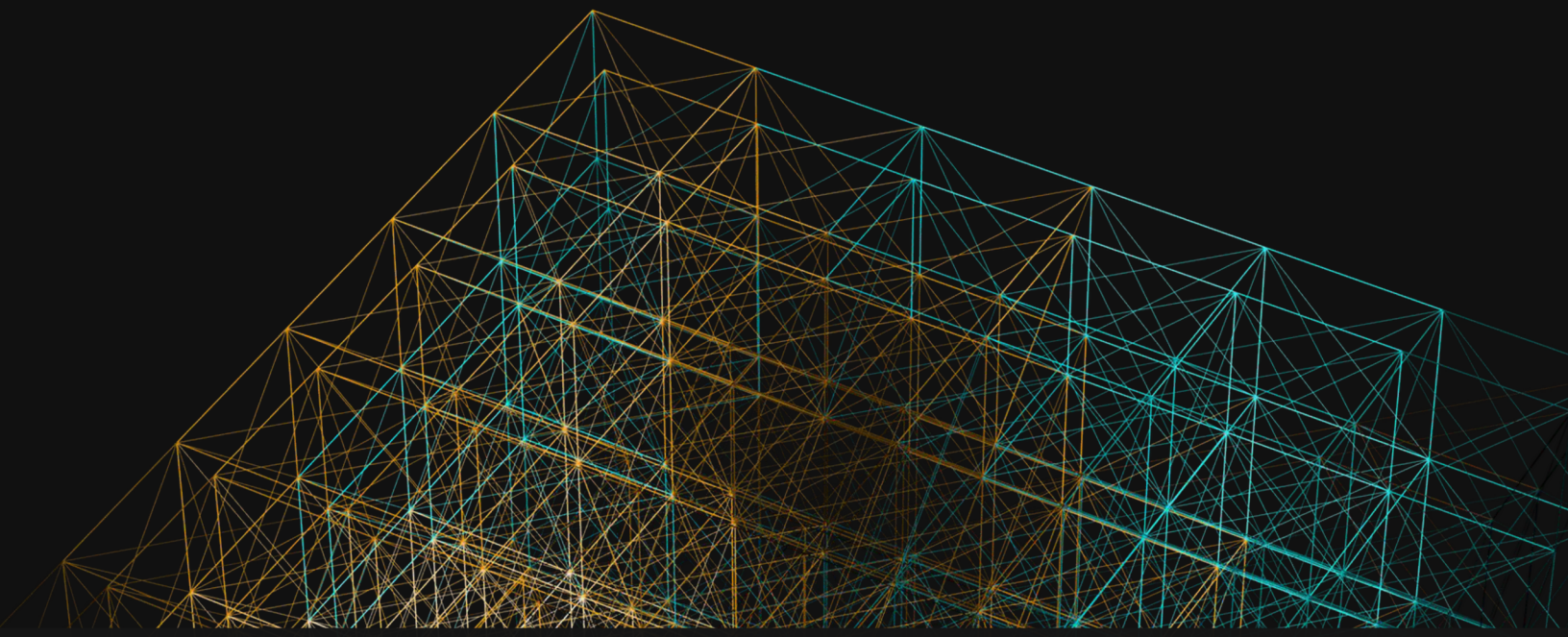

GREYNOISE

AT THE EDGE

Weekly Intelligence Brief

Report Date: 20 April 2026

Analysis Period: 13 April – 20 April 2026

Bottom Line Up Front

During this reporting period, GreyNoise observed sustained reconnaissance against enterprise-exposed remote access services and management infrastructure. There is no evidence of widespread exploitation at this time, but multiple indicators show active pre-exploitation targeting at scale. The highest near-term risk is concentrated in organizations with internet-accessible VNC, VPN, firewall, or management interfaces, particularly where authentication or segmentation is weak. Adversaries, and commercial scanning entities, are systematically identifying vulnerable assets, enabling rapid transition to exploitation when conditions permit.

Coordinated Scanning of Enterprise Attack Surface. A four-IP cluster conducted broad, multi-protocol reconnaissance (8.7 million sessions) using a shared scanning toolkit, confirmed by identical TCP, HTTP, and TLS fingerprints. Activity is consistent with scanning across all major services. Shared tooling confirms common software; it does not, on its own, confirm a common operator.

Remote Access Exposure Driving Risk. VNC (port 5900) activity reached 17.4 million sessions, ranking as the third-most-targeted service globally. Traffic is primarily reconnaissance rather than credential attacks; however, any exposed or unauthenticated VNC service presents immediate compromise risk. In parallel, RDP brute-force activity increased 116% week over week, indicating expanding attacker focus across remote access pathways, not substitution between them.

The current threat environment reflects a steady-state reconnaissance posture, not a discrete campaign. Adversaries are maintaining persistent visibility into enterprise attack surfaces, prioritizing assets that provide direct access (remote desktop) or scale (IoT/proxy infrastructure). Risk is driven primarily by exposure rather than targeting. Organizations with externally accessible remote access services should assume they have been identified and assessed.

Priority Actions. Organizations should focus on reducing immediate exposure across the most targeted services. Begin by blocking the four identified scanner IPs, ensuring they are not part of an approved ASM allowlist. Remove any external access to VNC services (ports 5900–5908), as these present direct compromise risk if exposed.

Recommended Actions by Role

For CISO / Security Leadership

Strategic decisions and resource allocation for this week.

- **Review inbound VNC exposure. Port 5900 ranked third-most-targeted on the internet this period; any unauthenticated VNC server is an interactive-desktop compromise with no credential required**
- **Move detection beyond IP reputation. As GreyNoise's Invisible Army report documents, cloud-hosted and residential-proxy-rotated scanners defeat IP-only blocking; add behavioral and fingerprint-based detection (JA4T, JA4H, user-agent anomalies)**

For SOC Teams

Detection and monitoring priorities for the analysis period.

- **Alert on inbound VNC/RFB connection attempts to port 5900 and surrounding ports (5901–5908) from untrusted sources — the relevant GreyNoise tags are RFB Protocol, VNC Login Attempt, and VNC Bruteforcer; tag pages carry per-tag IP lists and context**
- **Flag inbound connections matching the four-node scanning fingerprint set — JA4T `1025_2_1460_0`, JA4H `ge10nn020000_db6abae5e99a_000000000000_000000000000`, JA3 `9812cdc989e02988bd1f0734fb6ed1a5`. Lead with JA4T (survives TLS 1.3 / GREASE randomization, computed at the TCP SYN stage), retain JA3 for stack compatibility. Validate against your external attack surface management allowlist before auto-blocking**
- **Continue to alert on HTTP requests targeting `.env`, `.git/config`, `.aws/credentials`, and cloud metadata paths — active at reduced volume (see Persistent Activity Update) and consistent with both credential-discovery campaigns and routine search-engine crawling, so pair the detection with a response threshold rather than an automatic block**
- **Tag pages are the primary source for per-tag IP context, sample payloads, and intention classification: RFB Protocol, Palo Alto Networks PAN-OS CVE-2020-2034 Crawler, ENV Crawler**

For Vulnerability Management Teams

Patch prioritization based on probing and exploitation-pattern activity observed on the GreyNoise Global Observation Grid (GOG).

- **Patch on accelerated cadence (within 7 days):**
- **CVE-2026-21962 — Oracle WebLogic Proxy Plug-in access control bypass — observed on active exploit delivery infrastructure**
- **CVE-2026-24061 — GNU Inetutils telnetd authentication bypass — currently trending on GreyNoise**
- **Patch on standard cadence:**
- **CVE-2020-2034 — Palo Alto Networks PAN-OS GlobalProtect command injection — 187,509 sessions observed via the corresponding scanner tag**

- **CVE-2024-9474 — PAN-OS management interface privilege escalation (CISA KEV) — currently trending on GreyNoise (30 malicious IPs in the last 30 days)**
- **Compensating Controls:**
- **Block external access to port 5900 (VNC) and PAN-OS GlobalProtect management portals**
- **Remove `.env`, `.git/`, and cloud credential files from any internet-accessible web root; add web application firewall rules that block direct access to these paths, scoped to permit legitimate search-engine crawlers**
- **Disable Telnet on all network devices where Secure Shell (SSH) is available (mitigates CVE-2026-24061)**

For Network Security / Infrastructure Teams

Perimeter and segmentation actions.

- **Block external access to ports 5900–5908 (VNC/RFB) — port 5900 ranked third this period at 17,375,937 sessions**
- **Deploy access control list rules blocking the four scanning-cluster IPs — 87.251.64.159, 167.172.65.202, 128.199.240.7, 152.42.238.0 — after validating against your external attack surface management allowlist**
- **Add web application firewall rules blocking requests containing `.env`, `.git/config`, `.aws/`, or `%2e%2e/` (URL-encoded traversal) patterns against internet-facing applications — with an exception pathway for known-legitimate indexing traffic (major search engines also crawl environment files on routes they discover)**
- **Tag pages are the per-tag primary source for IP lists and behavioral context**

For Threat Hunters

Hunting leads for the analysis period.

- **Hunt for any successful inbound authentication from 87.251.64.159, 167.172.65.202, 128.199.240.7, or 152.42.238.0 against SSH (22), RDP (3389), or MySQL (3306) — these four IPs conducted full-spectrum scanning this period and any successful auth warrants an access audit**
- **Identify successful RFB/VNC connections from untrusted sources to internal endpoints over the last 14 days — any successful VNC session from an internet source is a high-severity finding (interactive-desktop compromise, no additional credential required)**
- **Review web-server logs for HTTP 200 responses to requests for `.env`, `.git/config`, `.aws/credentials`, or `/metadata` over the last 30 days — any successful response warrants credential rotation and a downstream access audit**
- **For IoT/embedded-device (routers, cameras, DVRs) fleets: search for outbound connections to untrusted destinations within 24 hours of inbound exploitation on ports 23, 2323, 8728, or 80; cross-reference source IPs against Mirai, Mirai Variant, and Androxgh0st observed on your perimeter**

For Identity & Access Management Teams

Authentication and access control priorities.

- **Review and rotate any credentials potentially exposed through `.env` files, `.git/config`, or path traversal — Generic Sensitive File Access Attempt and Generic Path Traversal Attempt remain active at reduced volume**
- **Audit MikroTik RouterOS device credentials — 1,181,580 brute-force sessions targeting RouterOS API port 8728**
- **Enforce multi-factor authentication on all remote access surfaces (VPN portals, RDP, appliance management consoles)**
- **Enforce account lockout policies on all internet-facing authentication surfaces**

Findings at a Glance

- **Four IPs, one toolkit, two continents.** A Poland IP (first seen 07 April) and three DigitalOcean Singapore hosts (active since late October 2025) share identical JA4T, JA4H, and JA3 fingerprints; combined volume reached 8.7 million sessions. The toolkit is a raw-SYN kernel-bypass scanner — structurally similar to, but not identical to, Masscan's published reference. Shared tooling confirms common software, not a common operator.
- **VNC at top-three port rank.** Port 5900 (VNC remote-desktop) recorded 17.4 million sessions, third-most-targeted on the internet this period — no comparable volume in prior briefs. VNC-specific authentication tags (VNC Login Attempt at 28 IPs, VNC Bruteforcer at zero) are nearly empty, so the volume is scanners cataloging which VNC servers respond — not password-guessing.

Key Judgments & Evidence

JUDGMENT 1

> **Four IPs sharing identical TCP, HTTP, and TLS fingerprints operated against the GOG this period. The fingerprint cluster is consistent with a raw-SYN kernel-bypass scanner class (high confidence on fingerprint alignment; low-to-medium confidence on shared operator — shared tooling is necessary but not sufficient for same-operator attribution).**

Evidence:

- IP 87.251.64.159 (ISAEV Igor, AS200730, Poland) first seen 07 April 2026 and generated 5,322,494 sessions during the current analysis period
- All four IPs share JA4T `1025_2_1460_0` (1025 window, single MSS option, no SACK / timestamp / window-scale — a raw-SYN kernel-bypass scanner class, structurally similar to but not identical to the Masscan reference `1024_00_00_00` in the JA4+ database); JA4H `ge10nn020000_db6abae5e99a_000000000000_000000000000` (HTTP/1.0 GET, two-header primitive client); and JA3 `9812cdc989e02988bd1f0734fb6ed1a5`
- All four IPs carry the Masscan Client tag
- Same fingerprint set observed on 167.172.65.202, 128.199.240.7, and 152.42.238.0 — three DigitalOcean Singapore hosts active since late October 2025
- All four IPs conduct full-spectrum scanning across 10,000 ports and target every major internet protocol (SSH, Telnet, RDP, SMB, LDAP, Kerberos, SQL, Redis, FTP, SMTP, DNS, HTTP/HTTPS/TLS)
- Behavioral commonality beyond fingerprints is weak — the four IPs do not share a common source ASN (one is AS200730/ISAEV Igor, three are AS14061/DigitalOcean), do not share reverse DNS, and we have no passive DNS or WHOIS pivot linking them to a single registrant
- The shared three-layer fingerprint set is consistent with a single operator, with multiple operators using the same off-the-shelf scanner, or with external attack surface management vendors doing legitimate scanning — the signal is a toolkit class, not an identity

JUDGMENT 2

> **VNC endpoint activity ran at anomalous volume relative to prior weeks this period — dominated by protocol probing rather than authentication attempts (medium confidence pending week-over-week trend confirmation).**

Evidence:

- Port 5900 recorded 17,375,937 sessions, ranking third behind only SSH (port 22) and Server Message Block (port 445)
- RFB Protocol tag generated 4,305,556 sessions (scanners negotiating VNC protocol version) with surrounding ports (5901–5908) also elevated
- VNC Login Attempt observed 28 suspicious IPs over the same window and VNC Bruteforcer observed zero — the 17.4M sessions are exposure-surface mapping (cataloging which VNC servers respond), not bruteforce pressure
- RDP Bruteforce Attempt rebounded 116.1% week-over-week in the same period, so VNC is running alongside RDP pressure rather than displacing it

• No comparable VNC volume was documented in the 06 April or 13 April briefs; medium confidence reflects a single-week observation

Details of Our Findings

1 Coordinated Multi-Cloud Scanning Via Shared JA4T/JA4H/JA3

During the analysis period, GreyNoise observed four IPs — one in Poland and three in DigitalOcean Singapore — sharing three converging fingerprint dimensions.

• **JA4T** `1025_2_1460_0` (TCP layer): 1025 window, single MSS option, no SACK, no timestamp, no window-scale. The fingerprint is in the class of raw-SYN kernel-bypass scanners. The JA4+ database lists Masscan's canonical JA4T as `1024_00_00_00` (1024 window, zero options); this cluster's signature differs in both the window (1025 vs 1024) and the MSS option count. Similar does not mean identical, and attribution to a specific tool from JA4T alone is not conclusive — see FoxIO on JA4T and JA4TSCAN documentation for how similar-looking signatures map to distinct implementations.

• **JA4H** `ge10nn020000_db6abae5e99a_000000000000_000000000000` (HTTP layer): HTTP/1.0 GET with only two headers, no cookies, no referer — a primitive HTTP client.

• **JA3** `9812cdc989e02988bd1f0734fb6ed1a5` (TLS layer): retained here for detection-stack compatibility; JA3 is less durable than JA4T against Transport Layer Security 1.3 / GREASE randomization.

All four IPs carry the Masscan Client tag and scan across 10,000 ports and every major application protocol.

In plain terms, the same off-the-shelf scanning toolkit is running on infrastructure in different countries and hosting providers. The fingerprint alignment is the observation. We cannot, from fingerprints alone, confirm that the operator is the same, and we cannot, from JA4T alone, prove the tool is Masscan rather than a structurally similar kernel-bypass scanner.

Session Volume by IP:

Source IP	Sessions	Org	Country	First Seen
87.251.64.159	5,322,494	ISAEV Igor (AS200730)	Poland	07 April 2026
167.172.65.202	1,139,924	DigitalOcean (AS14061)	Singapore	29 October 2025
128.199.240.7	1,128,922	DigitalOcean (AS14061)	Singapore	01 November 2025
152.42.238.0	1,086,808	DigitalOcean (AS14061)	Singapore	30 October 2025
Combined	8,678,148			

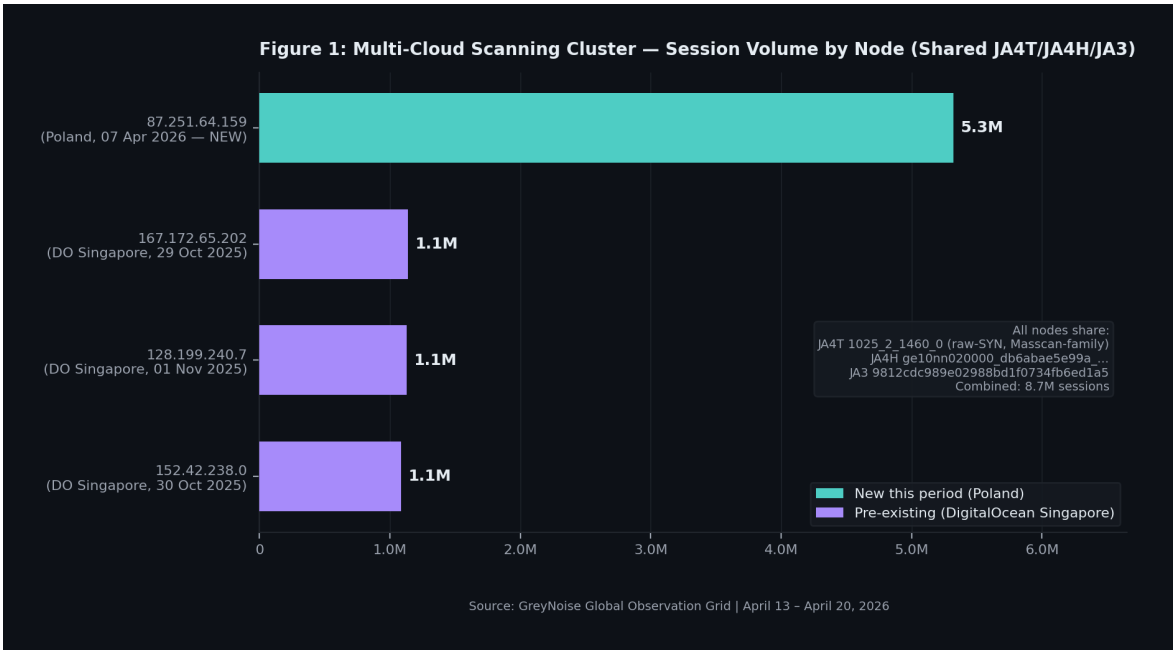

Figure 1: Multi-Cloud Scanning — Session Volume by IP Since Activation

What these four IPs share beyond the fingerprints. The behavioral commonality is bounded: shared JA4T/JA4H/JA3, shared full-spectrum 10,000-port target profile, and a temporal overlap on the current period. The four IPs do **not** share a source ASN (87.251.64.159 is on ISAEV Igor/AS200730, the other three are on DigitalOcean/AS14061), do not share reverse DNS, and we have no passive DNS or WHOIS pivot linking them to a single registrant. None of the four resolves to, or is hosted on infrastructure operated by, a known external attack surface management vendor (SecurityScorecard, Shodan, Censys, Qualys, BitSight, Rapid7, or similar). Reading the four as a single operator is consistent with the data but not established by it; reading them as two independent operators running the same off-the-shelf scanner against the same broad target surface is equally consistent.

Why JA4T leads here. JA4T is computed from the initial TCP SYN — it operates pre-TLS and survives the TLS 1.3 / GREASE randomization that degrades JA3. In detection stacks that support both, JA4T should lead; JA3 is kept in this brief for compatibility with telemetry that hasn't migrated. JA4H (HTTP-layer fingerprint) is a separate, independent dimension — a TCP-level match and an HTTP-level match and a TLS-level match on four distinct IPs is a stronger toolkit signal than any one in isolation.

Target Assessment. Breadth (every major protocol) and volume (8.7 million combined sessions) indicate bulk reconnaissance rather than targeted exploitation. Output of bulk kernel-bypass scanning typically feeds downstream campaigns — credential brute-forcing, vulnerability exploitation, or proxy/relay recruitment — rather than generating direct compromise. Defenders should block the four listed IPs at the perimeter after validating against any external attack surface management allowlists (several ASM vendors emit structurally similar scanner traffic), alert on JA4T `1025_2_1460_0` in TCP telemetry (the most durable fingerprint against IP rotation), alert on the JA4H and JA3 fingerprints in HTTP and TLS logs respectively, and audit any successful authentication from the listed source IPs over the last 30 days.

Details of Our Findings

2 VNC/RFB Endpoint Activity Reaches Top-Three Port Rank

Port 5900 — the Virtual Network Computing (VNC) Remote Framebuffer (RFB) protocol default — ranked as the third-most-targeted port on GreyNoise sensors this period at 17,375,937 sessions, trailing only Secure Shell (port 22, 28.2 million sessions) and Server Message Block (port 445, 19.0 million sessions). The volume did not appear prominently in the 06 April or 13 April briefs and represents a single-week observation; trend confirmation requires continued monitoring.

In plain terms, scanners are cataloging which VNC servers respond to protocol probes — not yet trying passwords in bulk. RFB is the wire protocol spoken by VNC servers; the 4.3 million RFB Protocol tag sessions mean scanners completed enough of the handshake to negotiate a VNC protocol version, not merely TCP SYN-probing the port.

Port-and-Tag Summary:

Metric	Value
Port 5900 total sessions	17,375,937
Port 5900 GOG rank	#3
RFB Protocol tag sessions	4,305,556
VNC Login Attempt tag IPs (10d)	28 suspicious
VNC Bruteforcer tag IPs (10d)	0
Ports 5901–5908 additional scanning	Elevated

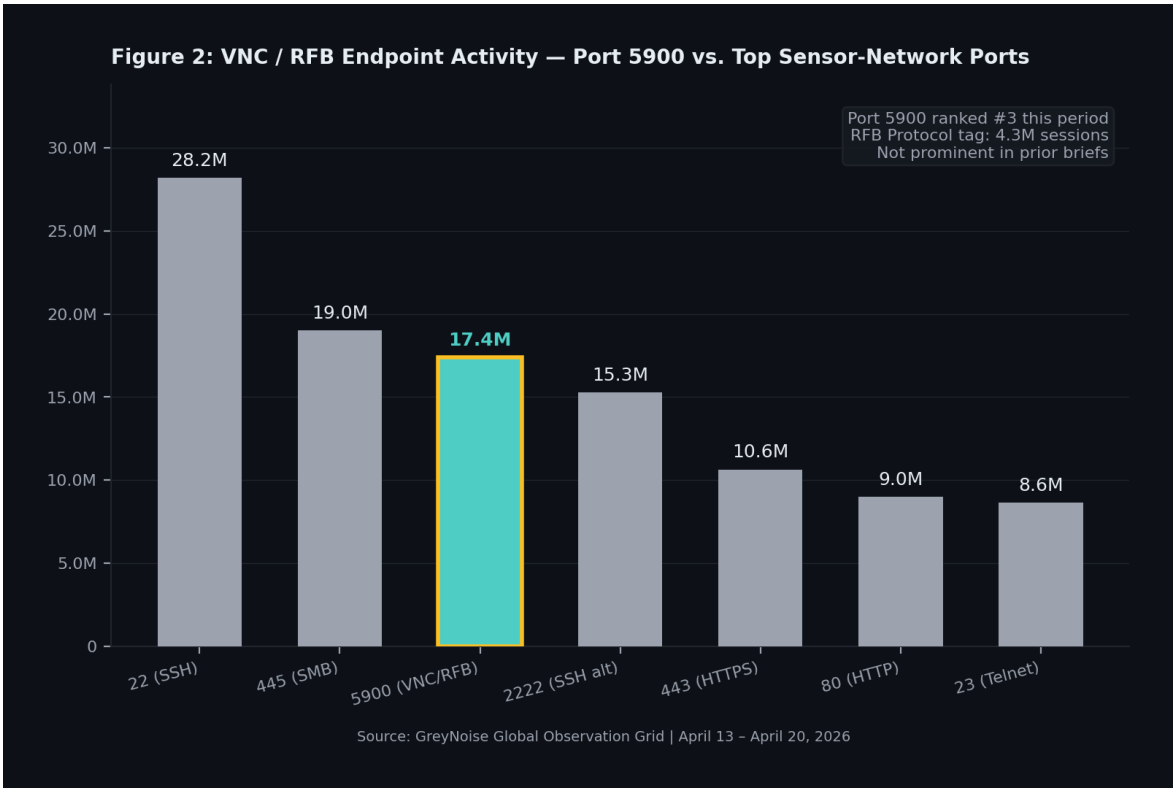

Figure 2: VNC / RFB Endpoint Activity — Port 5900 Weekly Trend

What the tags tell us the traffic is doing. Three VNC-specific tags establish the intent of the traffic. RFB Protocol (protocol-category, 4.3M sessions) fires when the sender successfully negotiates VNC protocol version — a probe-and-catalog operation, not an authentication attempt. VNC Login Attempt (suspicious — 28 IPs) fires on attempted authentication. VNC Bruteforcer (malicious — 0 IPs) fires on repeated authentication attempts consistent with a password-guessing campaign. The gap (4.3M RFB probes versus 28 auth attempts and 0 bruteforcers) is the evidence that port 5900 is being indexed, not attacked at scale — yet. ThinVNC Authentication Bypass Attempt and ThinVNC Directory Traversal CVE-2019-17662 LFI Attempt showed no anomalous spike this period, so the surface mapping is not currently paired with a specific VNC-software CVE push.

Correlation with RDP. RDP Bruteforce Attempt rebounded 116.1% week-over-week in the same period (see Persistent Activity Update). VNC-surface mapping is running alongside RDP bruteforce pressure rather than in place of it — remote-access-surface reconnaissance is broader this period, not displaced.

Why the RFB-high / VNC-login-low gap is anomalous. The normal steady-state for port 5900 on the GOG is a modest baseline of protocol-version probes alongside a small, persistent volume of VNC Login Attempt and VNC Bruteforcer activity. What changed this period is the protocol-probe channel: 4.3 million RFB Protocol sessions landing at top-three port rank while the auth-attempt channel stayed nearly empty — 28 suspicious VNC Login Attempt IPs over 10 days and zero VNC Bruteforcer IPs. Three explanations are consistent with this shape, each with different defensive implications:

- **Pre-campaign enumeration.** A downstream operator is building an inventory of reachable VNC servers (which versions answer, which require no authentication) before running a targeted follow-on auth campaign. If this is the shape, expect VNC Login Attempt and VNC Bruteforcer session volumes to rise in the next 1–3 briefs. This is the historical pattern for new remote-access campaigns.
- **Proxy-discovery probing.** Some scanners survey VNC surfaces as part of broader open-proxy discovery — misconfigured VNC servers can be used as relay endpoints rather than compromise targets. If this is the shape, expect the RFB volume to stay flat or drift, without VNC-specific auth follow-on.

• **Research / ASM scanning.** Academic scanners, threat intelligence vendors, and ASM providers routinely survey VNC. If this is the shape, the RFB volume will persist at the same band and will carry clean attribution to known-benign infrastructure.

What to track next week. The informative signals are the VNC-specific authentication tags and the VNC-software CVE tags. Watch VNC Login Attempt (the earliest indicator of a transition to auth pressure), VNC Bruteforcer (scaled password-guessing), ThinVNC Authentication Bypass Attempt, and ThinVNC Directory Traversal CVE-2019-17662 LFI Attempt. No anomalous spike on the two ThinVNC-specific tags this period means the surface mapping is not currently paired with a specific VNC-software CVE push — but the catalog-then-attack pattern is common enough that defenders should harden VNC exposure now rather than waiting for the auth tags to fire.

Target Assessment. Any organization operating VNC servers exposed to the public internet — commonly deployed for remote IT support, virtual machine console access, or legacy remote access to industrial control systems — is a target. Defenders should block port 5900 and surrounding ports (5901–5908) at the network perimeter, require VNC access through a VPN only, and audit for VNC servers configured without authentication or with weak shared secrets. Given the catalog-then-attack pattern typical of bulk scanning, expect the VNC Login Attempt and Bruteforcer tag volumes to rise in the coming weeks if this mapping activity is preparation for follow-on authentication campaigns.

Persistent Activity Update

The following activity continues from prior analysis periods. These items are not among this week's primary findings but represent persistent infrastructure that defenders should continue monitoring and blocking.

Credential and Configuration Discovery Campaign — Declining:

The 06 April brief documented a broad credential and configuration discovery campaign at peak levels. Combined thematic volume this period reached 6,228,817 sessions — still high in absolute terms, but with the highest-volume components declining week-over-week.

Tag	Sessions	Change vs. 06 Apr
Generic Sensitive File Access Attempt	2,787,682	-40.0%
ENV Crawler	1,607,562	-4.8%
Generic Path Traversal Attempt	1,230,670	-62.2%
Git Config Crawler	549,384	+7.4%
AWS Configuration Scanner	53,519	—
Combined thematic volume	6,228,817	—

One IP of note is 185.177.72.61 (Bucklog SARL, AS211590, France), which generated 1,397,597 sessions focused specifically on sensitive file discovery and also carries the l9tcpid internet scanning tag. `l9tcpid` is LeakIX's open-source TCP-identification tool — it uses unusual TCP options to fingerprint socket protocols and capabilities during scanning, and is a distinct toolchain from ProjectDiscovery's Naabu/Nuclei stack. The tag set points to an actor running protocol-reachability probing (LeakIX tooling) rather than a single off-the-shelf nuclei-template campaign.

Defenders should maintain web application firewall rules blocking requests containing `.env`, `.git/config`, `.aws/`, or `%2e%2e/` patterns on internet-facing applications, scoped to permit legitimate search-engine and security-scanner traffic (see ENV Crawler — major search engines also crawl environment files on routes they discover, so context-aware rules beat outright blocking).

• Status: Declining

Remote Desktop Protocol (RDP) Brute-Force — Rebounded This Week:

The April 06 brief documented a 340.7% RDP surge. The April 13 brief showed the surge had receded. This period, RDP Bruteforce Attempt more than doubled versus the prior week to 1,319,328 sessions (+116.1% vs 13 April) and RDP Crawler rose to 16,175,005 sessions (+90.1% vs 13 April). A new source at 91.202.233.121 (PROSPERO OOO, Russia) appeared 03 April and scaled to 958,443 sessions, joining the SS-Net (Romania) and FOP Dmytro Nedilskyi (Netherlands, IP 185.156.73.157 — the highest-volume source observed this period at 7,699,077 sessions, active since June 2022) clusters from the April 06 brief.

Caveat on the week-over-week delta: a rebound of this magnitude can be driven by real attacker activity, by a shift in GreyNoise sensor placement (new sensors being added, old sensors being retired, profiles being rotated), or by both. The RDP Bruteforce Attempt source-IP set is consistent with the 06 April brief (three named clusters, one net-new source), which points toward real attacker activity rather than a pure coverage artifact — but sensor/profile changes cannot be ruled out without a Deception Engineering / Beholder confirmation. Defenders should maintain RDP on VPN-only access, enforce account lockout, and use the RDP Bruteforce Attempt tag for blocking.

- RDP Bruteforce Attempt: 1,319,328 (+116.1% vs 13 April)
- RDP Crawler: 16,175,005 (+90.1% vs 13 April)
- Status: Rebounded after prior-week recession (pending sensor-change confirmation)

IoT Botnet Recruitment — Continuing:

IoT and embedded-device botnet recruitment continued through two complementary mechanisms: CVE-based exploitation from three IPs hosted on VPSVAULT.HOST LTD infrastructure (AS215925, Brazil) and high-volume default-credential stuffing by a confirmed Mirai node. The three VPSVAULT-hosted IPs in the 45.205.1.x range — documented in the 13 April brief as a continuing operation — generated 3,352,578 combined sessions this period; IP 45.205.1.5 individually carries 18+ CVE exploits spanning routers, cameras, DVRs, NAS devices, and embedded systems. Generic IoT Default Password Attempt reached 3,056,131 sessions. The confirmed Mirai node 36.25.240.114 (CT-HangZhou-IDC, AS58461, China) generated 851,713 sessions exclusively against Telnet; this IP carries 65.5 million total sensor hits across its history and tags as Mirai.

The two mechanisms are complementary at the recruitment layer. CVE-driven exploitation from the VPSVAULT-hosted IPs targets devices that have been patched against factory credentials but not against the specific product CVEs. Default-credential stuffing — the combination of Mirai, Mirai Variant, Mirai Bruteforcer Attempt, and Androxgh0st — recruits the long tail of unpatched devices still accepting factory credentials. Telnet Login Attempt at 4,277,863 sessions this period is the umbrella volume metric under which Mirai-family and Androxgh0st credential stuffing show up; MikroTik RouterOS Bruteforcer at 1,181,580 sessions captures the RouterOS API brute-force lane specifically.

- VPSVAULT-hosted IPs combined sessions: 3,352,578
- MikroTik RouterOS Bruteforcer: 1,181,580
- Generic IoT Default Password Attempt: 3,056,131
- Telnet Login Attempt: 4,277,863
- Status: Continuing

SOCKS5 and Open-Proxy Scanning — Continuing:

IP 185.91.127.85 (Ferdinand Zink trading as Tube-Hosting, AS49581, Germany) generated 4,095,453 sessions this period operating as a dedicated open-proxy and SOCKS5 Proxy Scanner targeting hundreds of proxy-related ports. This activity identifies exploitable open proxies for downstream use in anonymization or relay-abuse campaigns.

- Sessions this period: 4,095,453
- Status: Active

Operational Technology (OT) / Industrial Control System (ICS) Reconnaissance — Mixed:

ICS scanning, which intensified for three consecutive weeks through the April 06 brief, showed mixed signals this period versus that peak. Siemens S7Comm Protocol Scanner declined 39.4% to 47,285 sessions (vs 06 April) and OPC UA Scanner (Open Platform Communications Unified Architecture) declined 36.0% to 396,040 (vs 06 April), while Tridium Niagara AX Fox ICS Scanner increased 13.9% to 65,866 (vs 06 April).

One IP of note is 104.131.63.228 (DigitalOcean, Clifton NJ), a multi-protocol scanner carrying 70+ protocol tags and 29.7 million total sensor hits across its history. Its ICS coverage this period spanned Siemens S7Comm, OPC UA, IEC 60870-5-104, Omron FINS, and Veeder-Root Automatic Tank Gauge protocols — manufacturing automation and energy-sector infrastructure both. The IP also carries the BPFDoor Malware Traffic tag among its 70+ tags, which means GreyNoise has observed packets from this IP matching the BPFDoor class signature — one signal among many on a high-coverage scanner, **not** a direct indication the host itself is BPFDoor-infected. Treat the combination as "broad ICS scanner that also emitted traffic matching one malware-class pattern," not as "BPFDoor C2."

- Siemens S7Comm: 47,285 (-39.4% vs 06 April)
- OPC UA: 396,040 (-36.0% vs 06 April)
- Tridium Niagara AX Fox: 65,866 (+13.9% vs 06 April)
- Status: Mixed vs 06 April peak

React Server Components CVE-2025-55182 RCE — Fourth Month, Declining:

React Server Components exploitation-attempt activity continued to decline. The 724,172 sessions observed represent a 33.5% decrease from 1,088,288 sessions in the April 06 brief. The associated tag is on CISA KEV.

- Sessions this period: 724,172
- Change from 06 April brief: -33.5%
- Status: Declining

AS135377 (UCloud HK) — Stable at Peak:

AS135377, registered to UCloud Information Technology (HK) Limited (APNIC WHOIS: UCLOUD-HK-AS-AP, Hong Kong), maintained its position as the dominant source ASN at 38,450,170 sessions this period — the largest single-ASN volume on the GOG. The ASN is fully attributed via APNIC WHOIS; session volume at this scale reflects the overall traffic routed through UCloud HK customer infrastructure, not a single coordinated scanner.

- Sessions this period: 38,450,170
- Status: Stable

New Tags of Note:

- GNU Inetutils Telnetd Authentication Bypass CVE-2026-24061 Attempt — authentication bypass, currently trending on GreyNoise
- Oracle WebLogic Server Proxy Plug-In Access Control Bypass CVE-2026-21962 Attempt — observed on the 85.11.167.11 multi-CVE platform
- Ollama API Endpoint Crawler — 154,505 sessions this period, up from 65,880 in the 13 April brief (+134.5% week-over-week) and from 34,021 two weeks prior (+354% since 06 April). Continued AI/LLM infrastructure reconnaissance; no confirmed exploitation attempts observed

Campaigns Ending:

- GeoServer GeoTools CVE-2024-36401 RCE Attempt — no longer in top 100 observed tags
- Symfony Profiler Debug Mode RCE Attempt — no longer observed at measurable volume
- Feroxbuster — not present in current top 100 tags

Analyst Comment

Two findings this period are material to defenders.

Finding 1 — four IPs sharing identical TCP, HTTP, and TLS fingerprints across two continents. Fingerprint alignment is high-confidence; attribution to a specific tool and to a single operator is not established. New material this period.

Finding 2 — VNC/RFB endpoint activity reaching top-three port rank, predominantly protocol probing rather than interactive login pressure. Not documented in prior briefs. New material this period.

The credential and configuration discovery campaign (at peak in the 06 April brief) is declining in its highest-volume components (Generic Sensitive File Access Attempt -40.0%, Generic Path Traversal -62.2% vs 06 April) and has been moved to the Persistent Activity Update section; it remains at 6.2 million combined sessions. IoT botnet recruitment is similarly continuing from prior briefs — Mirai-family default-credential stuffing plus CVE-based exploitation from VPSVAULT-hosted infrastructure — and is tracked in Persistent Activity Update.

Action items are narrow: block the four scanning-cluster IPs in Finding 1 at the perimeter (validate against external attack surface management allowlists first), and block external access to VNC (port 5900 and 5901–5908).