Research Report — Week 1

Topic: GlobalProtect VPN portals: 2.3 Million Scan Sessions & Defensive Analysis
Author: Nirmiti (The Cyber Ledger — Intern)
Date: November 2025

Executive Summary

Between **14–19 November 2025**, threat intelligence observed an unprecedented surge of **~2.3 million sessions** targeting Palo Alto Networks' GlobalProtect login endpoint (/global-protect/login.esp). The activity intensified rapidly (a **40× surge within 24 hours**) and reached a 90-day high, prompting concern that attackers are either probing for vulnerable PAN-OS instances or preparing brute-force/exploitation campaigns. The activity is concentrated in a small number of ASNs and appears coordinated, with primary traffic originating from AS200373 and additional clusters routed via AS208885. This report explains the technical behavior, attack implications, safe PoC demonstrations, detection indicators, and a prioritized defensive playbook. BleepingComputer+1

What is GlobalProtect and Why VPN Portals Matter :

- **GlobalProtect** is Palo Alto Networks' remote access VPN (portal and gateway) used to provide secure access for corporate users. The portal typically exposes a login page (/global-protect/login.esp) where users authenticate and establish secure tunnels to internal networks.
- VPN portals are high-value targets because they provide entry to the corporate "trusted" network. If an attacker can brute-force credentials, exploit a login vulnerability, or perform session fixation, they can gain authenticated access and pivot to sensitive resources. Past CVEs and authentication design issues have made GlobalProtect an attractive target for mass scanning and follow-on attacks. Palo Alto Networks Security+1

Timeline & Key Facts (What Happened)

1. **Activity Start:** GreyNoise and other intelligence sources detected rising probe activity beginning **14 November 2025**. greynoise.io
2. **Surge Magnitude:** Within ~24 hours the scanning activity spiked **40×**, culminating in **~2.3 million sessions** against the /global-protect/login.esp endpoint during the 14–19 Nov window. BleepingComputer+1
3. **Infrastructure Concentration:** Intelligence attributes **~62%** of sessions to ASN **AS200373 (3xK Tech GmbH)** with additional traffic routed through Canadian clusters of the same ASN and secondary traffic via **AS208885**. Attack traffic focused on the United States, Mexico, and Pakistan. BleepingComputer+1
4. **Campaign Traits:** Researchers note recurring TCP and JA4t fingerprints across waves, reuse of ASNs, and synchronized spikes — suggesting a coordinated operation likely iterating on prior campaigns. BleepingComputer+1

These facts are drawn from live threat feeds and reporting (GreyNoise / BleepingComputer / others) and represent observed scan sessions — **not** successful compromises. BleepingComputer+1

Deep Technical Analysis — What "Scan Sessions" & Login Probes Mean

Scan sessions: automated, repeated HTTP(S) requests made to a specific endpoint to detect the existence and behavior of that endpoint. For GlobalProtect:

- The **/global-protect/login.esp** endpoint is the web page used to begin user authentication. Attackers probe it to see if it exists, to fingerprint PAN-OS versions via error messages, and to test for specific vulnerable behaviors (e.g., login flow anomalies, SAML/session fixation weaknesses). BleepingComputer+1

Why attackers probe at scale

- **Identify targets**: find internet-facing devices that expose GlobalProtect.
- **Fingerprinting**: retrieve headers, error pages, TLS certs to infer PAN-OS versions that might be vulnerable to specific CVEs.
- **Prepare for brute-forces**: high-volume probes often precede credential stuffing or brute-force attempts if lists of credentials are available.
- **Exploit novel 0-days**: coordinated scans may indicate actors searching for a new zero-day; a scan wave can preface targeted exploitation. Palo Alto Networks Security+1

Common attack vectors against VPN portals

- Brute-force / credential stuffing (automated login attempts).
- Authentication bypass (session fixation, SAML issues).
- Exploiting known PAN-OS CVEs (RCE, XSS, DoS).
- Misconfiguration exploitation (management interfaces exposed, default settings, weak rate-limiting). Palo Alto Networks Security+1

Indicators & Signatures (What to Look For in Your Environment)

Top indicators to monitor immediately:

- Repeated requests to /global-protect/login.esp from the same source ASNs or IP clusters. (Look for concentrated bursts from AS200373 / AS208885.) BleepingComputer+1
- **Unusual User-Agent / TCP fingerprints** (GreyNoise observed repeated TCP and JA4t fingerprints tied to this campaign). Monitor for JA4t fingerprints such as those reported by analysts (examples seen in reporting). Rewterz - Revolutionizing Cybersecurity+1
- High rate of failed authentication attempts against GlobalProtect portals (from multiple sources or a single orchestrated IP set).
- Sudden surge in connections to management or portal ports (443/8443) followed by abnormal session creation.
- Abnormal authentication flows: session tokens created with unexpected parameters, cookies with unusual lifetimes or multiple session creations from the same client footprint. Palo Alto Networks Security

PoC goals

- Demonstrate how an attacker would **discover** GlobalProtect portals (OSINT).
- Show how to **fingerprint** an endpoint without exploitation.
- Provide sample (non-functional) request formats to explain attack logic.

Detection & Response Playbook (Step-by-Step)

Immediate (within hours) :

Identify and inventory all internet-facing GlobalProtect portals and PAN-OS management interfaces. Use asset inventory + external port scanner only against your own IP ranges.

1. **Enforce MFA** for all VPN logins today (if not already in place). MFA mitigates credential stuffing. BleepingComputer
2. **Apply rate limiting & account lockout**: block IPs that exceed threshold login failures in short period; consider CAPTCHAs or secondary verification.
3. **Patch/validate PAN-OS** — compare installed PAN-OS versions against Palo Alto advisories and CVEs (apply vendor patches). Palo Alto Networks Security+1

Hunt & Investigate (24–72 hrs):

4. **Search logs** for repeated requests to /global-protect/login.esp and for JA4t/TCP fingerprints observed by GreyNoise. Correlate with ASNs (AS200373 / AS208885) and IP clusters. BleepingComputer+1
5. **Block / rate-limit** known malicious clusters at network perimeter (in-line) and add to WAF / firewall deny lists.
6. **Rotate credentials** for any account with suspicious access attempts; require password resets for affected users.

Containment & Recovery (if compromise suspected):

7. **Isolate affected systems** and revoke VPN sessions if suspicious session creation is observed.
8. **Reset credentials and reissue tokens/cookies** for any accounts that show successful authentication from suspicious sources.
9. **Conduct forensic investigation** and check for indicators of lateral movement (AD logs, EDR alerts).
10. **Inform stakeholders** and, if data access occurred, follow incident response & disclosure processes.

Longer term:

11. **Reduce attack surface** — private VPN access via IP allow-lists, client certificates, or on-demand VPN.
12. **Adopt zero-trust** principles — do not automatically grant broad network access simply via VPN.
13. **Threat intel integration** — subscribe to GreyNoise, vendor advisories, and community feeds to receive updates. greynoise.io+1

Risk & Impact Scenarios (Three realistic cases)

Scenario A — Credential Stuffing (most likely, medium impact)

- Attack: Lists of leaked passwords used to brute force VPN authentication.
- Impact: Unauthorized access to user-level resources; potential data exfiltration.
- Mitigation: MFA, account lockouts, monitoring.

Scenario B — Exploit of PAN-OS vulnerability (if present, high impact)

- Attack: If a targeted PAN-OS instance is vulnerable to a remote code execution or session fixation CVE, the actor could bypass auth and execute code.
- Impact: Full device compromise, network lateral movement, ransomware.
- Mitigation: Patch promptly, isolate compromised devices.

Scenario C — Supply-chain or chained exploitation (low frequency, critical impact)

- Attack: Scans lead to identification of devices that are then attacked with chained 0-day or misconfiguration exploits.
- Impact: Massive network compromise and long-term persistence.
- Mitigation: Harden edge controls, continuous monitoring, and segmentation.

Appendix

PoC — Discovery (OSINT, safe)
Use Shodan/GreyNoise dashboards to show the existence of internet-facing GlobalProtect portals.

PoC — Fingerprinting (lab)
Demonstrate header and TLS certificate retrieval against a lab host (show the curl -I and openssl s_client outputs).

References (Key sources used)

- Bill Toulas, “GlobalProtect VPN portals probed with 2.3 million scan sessions,” *BleepingComputer*, Nov 20, 2025. BleepingComputer
- GreyNoise Intelligence bulletin — surge in GlobalProtect login traffic (Nov 2025). greynoise.io
- Palo Alto Networks — Security Advisories and PAN-OS CVE information (PAN-OS/GlobalProtect advisories). Palo Alto Networks Security+1
- The Register — coverage summarizing the surge and defensive context. The Register
- Rewterz / Threat advisory summaries highlighting ASNs and fingerprints used in campaign analysis. Rewterz - Revolutionizing Cybersecurity