# Executive Situation Report | Surge in Scanning Against Palo Alto Login Portals

## Key Judgments & Evidence

1. **Threat actors are escalating attempts to log into Palo Alto Networks GlobalProtect login portals.**
   - On 3 October, GreyNoise observed ~1,300 unique IPs attempting to log into Palo login portals.
   - This activity escalated on 5 October; peaking today at over 2,200 daily unique IPs.
   - The unique count of ASNs has risen significantly since 3 October.
2. **Ongoing login attempts may be related to broader remote access targeting.**
   - In the past month, GreyNoise has observed spikes in activity against other remote access products including Ivanti Connect Secure, Pulse Secure, SonicWall SonicOS, and others.
   - There is partial signature overlap between recent scanning against Cisco ASA and the login attempts against Palo Alto.
3. **Observed Palo scanning is mostly targeted in nature.**
   - The overwhelming majority of traffic is targeting GreyNoise's emulated PAN-OS and GlobalProtect profiles.
4. **Similar surges have preceded new Palo vulnerabilities.**
   - Similar spikes in activity against Palo products have been followed by new vulnerabilities within six weeks; however, we have not observed a specific correlation between surges in Palo login scanning and subsequent disclosures.
5. **Activity may be driven by a threat actor(s) iterating through a large dataset of credentials.**
   - The pace of login attempts in the past week follows a roughly linear path.

| | |
|---|---|
| Top 3 Source Countries: | UNITED STATES (85%)<br>UNITED KINGDOM (2%)<br>CANADA (2%) |
| Top 3 Target Countries: | UNITED STATES (78%)<br>CANADA (38%)<br>UNITED KINGDOM (36%) |

**Source and target information based on observations from the past 90 days*
**Percentages can exceed 100% as threat actor IPs may target multiple countries*

## Strategic Threat Context

| STATE-SPONSORSHIP: | RANSOMWARE: | GLOBAL EXPLOITATION: |
|---|---|---|
| Volexity linked exploitation of Palo Alto Networks PAN-OS (CVE-2024-3400) to a threat actor it tracks as UTA0218 and assessed the actor is state-backed. | Ransomware groups, including LockBit affiliates, have exploited edge appliances and VPNs for initial access — most notably using the CitrixBleed (CVE-2023-4966) vulnerability. | Unit 42 observed post-exploit intrusion activity against GlobalProtect devices following CVE-2024-3400 exploitation. |

## Recommended Actions

> Block suspicious IPs observed during this period of elevated activity.

> Review GlobalProtect and PAN-OS portals for signs of unauthorized access or probing.

> Consider hardening defenses in the event a Palo CVE is disclosed in the coming weeks.

## Implications

> **Surges in activity:** GreyNoise's July research found spikes in some Palo Alto attack and reconnaissance activity correlated with later vulnerability disclosures, but scanning of Palo Alto login portals has not.

> **Shared tooling suggests overlap:** Partial signature overlap across Palo Alto and Cisco ASA scanning indicates common tooling or shared infrastructure.

> **U.S. endpoints most targeted:** Most observed probes were directed at U.S.-hosted assets, suggesting focus on U.S. networks.

## Threat Actor Activity (Past 90 Days)

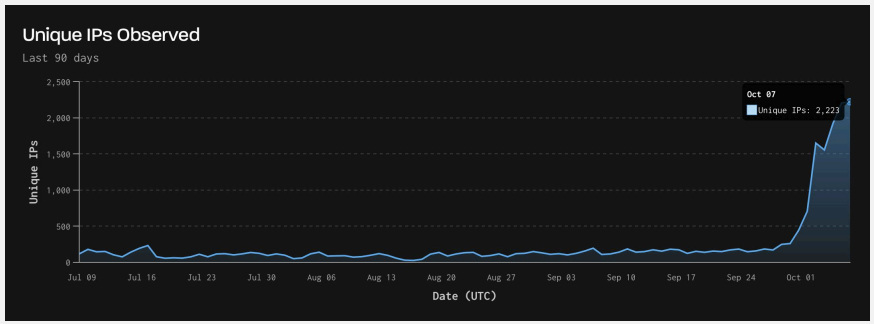


*Figure 1. Palo Alto Networks Login Scanner (Source: GreyNoise Global Observation Grid (GOG))*

**Peak Activity:**
2,200+ unique IPs (7 October 2025)

**Baseline:** ~200 IPs daily

**Percentage Increase:** ~1,000%

Significant spike in login attempts against Palo login portals



*Data from: GreyNoise "Palo Alto Networks Login Scanner" tag*

*Timeframe:* 3 October 2025 – 7 October 2025
*Source:* GreyNoise Intelligence

*Original GreyNoise Analysis*