IMPORTANT CYBERSECURITY NEWS: SURGE IN PALO ALTO NETWORKS SCANNER ACTIVITY SIGNALS POTENTIAL CYBER THREATS

Vairav Cyber Security News Report

Date: April 02, 2025

Vairav Cyber Threat Intelligence Team

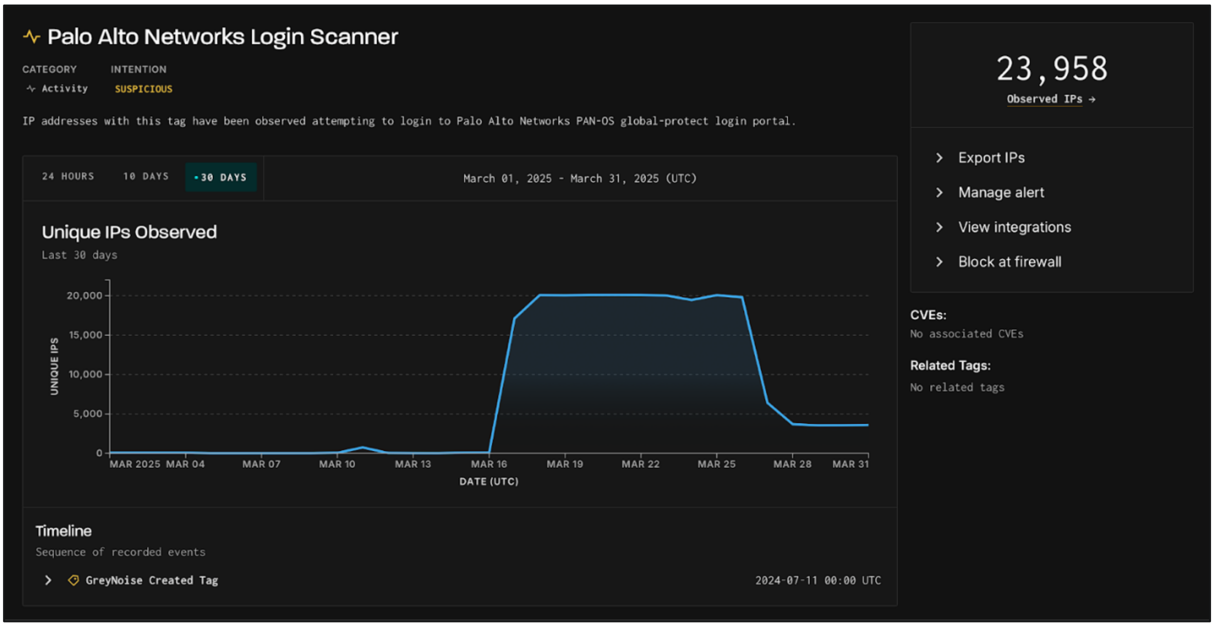
Vairav Technology Security Pvt. Ltd.

Thirbam Sadak 148
Baluwatar, Kathmandu

Phone: +977 4541540
Mobile: +977-9820105900
Email: sales@vairavtech.com

EXECUTIVE SUMMARY

GreyNoise has detected a significant surge in login scanning activity targeting Palo Alto Networks PAN-OS GlobalProtect portals, with nearly 24,000 unique IPs probing these portals over the past 30 days. The coordinated nature of this activity suggests an effort to identify exposed systems, potentially paving the way for future exploitation. Security experts warn that such reconnaissance spikes often signal the emergence of new vulnerabilities within 2 to 4 weeks, underscoring the need for proactive security measures.



Palo Alto Networks Login Scanner

CATEGORY: Activity
INTENTION: SUSPICIOUS

IP addresses with this tag have been observed attempting to login to Palo Alto Networks PAN-OS global-protect login portal.

March 01, 2025 - March 31, 2025 (UTC)

Unique IPs Observed
Last 30 days

23,958
Observed IPs →

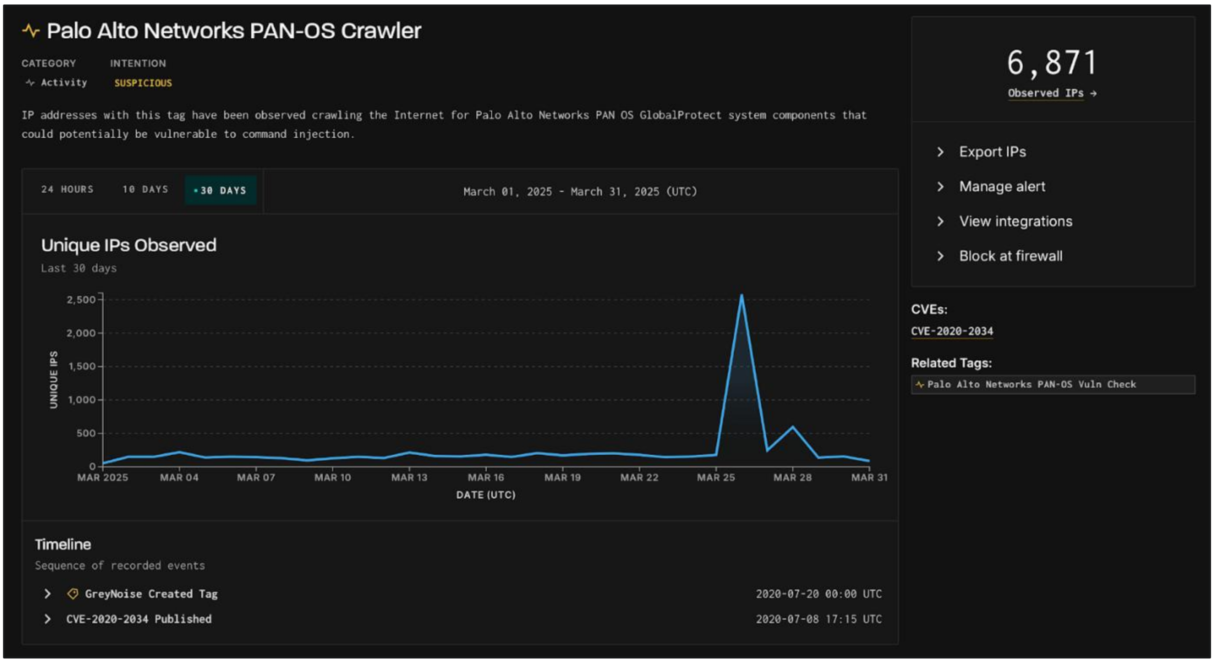
CVEs:
No associated CVEs

Related Tags:
No related tags

Timeline
Sequence of recorded events

GreyNoise Created Tag 2024-07-11 00:00 UTC

Figure 1: Palo Alto Networks Login Scanner



Palo Alto Networks PAN-OS Crawler

CATEGORY: Activity
INTENTION: SUSPICIOUS

IP addresses with this tag have been observed crawling the Internet for Palo Alto Networks PAN OS GlobalProtect system components that could potentially be vulnerable to command injection.

March 01, 2025 - March 31, 2025 (UTC)

Unique IPs Observed
Last 30 days

6,871
Observed IPs →

CVEs:
CVE-2020-2034

Related Tags:
Palo Alto Networks PAN-OS Vuln Check

Timeline
Sequence of recorded events

GreyNoise Created Tag 2020-07-20 00:00 UTC
CVE-2020-2034 Published 2020-07-08 17:15 UTC

Figure 2: Palo Alto Networks PAN-OS Crawler

KEY FINDINGS

1. The spike in scanning activity began on March 17, 2025, peaking at nearly 20,000 IPs per day before tapering off on March 26, 2025.
2. **Suspicious activity:** 23,800 IPs were flagged as suspicious; 154 were classified as malicious.
3. **Attack Infrastructure:**
   - 3xK Tech GmbH (ASN200373) accounted for 20,010 IPs.
   - Other contributors include PureVoltage Hosting Inc., Fast Servers Pty Ltd., and Oy Crea Nova Hosting Solution Ltd.
4. **Source and Destination Analysis:**
   - Source Countries: U.S. (16,249), Canada (5,823), followed by Finland, Netherlands, and Russia.
   - Targeted Countries: Primarily the United States (23,768 attacks), followed by the United Kingdom, Ireland, Russia, and Singapore.
5. **Login Scanner Tool Identified:**
   - Three JA4h hashes linked to the scanning activity suggest the use of an automated tool for reconnaissance:
     - ➢ po11nn11enus_967778c7bec7_000000000000_000000000000
     - ➢ po11nn09enus_fb8b2e7e6287_000000000000_000000000000
     - ➢ po11nn060000_c4f66731b00d_000000000000_000000000000

POTENTIAL IMPACT AND EXPLOITATION

- **Precursor to Targeted Attacks:** Similar reconnaissance spikes have historically been followed by the discovery of new vulnerabilities in the targeted technologies.
- **Risk to Exposed PAN-OS Systems:** Attackers could leverage brute-force attacks, known exploits, or newly discovered vulnerabilities to compromise enterprise VPN gateways.
- **Global Targeting Strategy:** The diverse geographical origins and destinations of the attacks indicate a broad, systematic reconnaissance campaign.

RECOMMENDED ACTIONS

- **Monitor and Analyze Logs**: Regularly review access logs for unusual login attempts, failed authentication events, and unknown IP addresses targeting GlobalProtect portals.
- **Enforce Multi-Factor Authentication (MFA)**: Enable MFA to prevent unauthorized access, even if credentials are compromised.
- **Block Malicious IPs**: Use threat intelligence feeds to identify and block known malicious IPs attempting to access your network.
- **Apply Security Patches Promptly**: Keep PAN-OS and all related components updated to protect against known vulnerabilities.
- **Strengthen Perimeter Security**: Restrict access to GlobalProtect portals with IP allowlists and limit exposure of services.
- **Conduct Proactive Threat Hunting**: Investigate any indicators of compromise (IOCs), unauthorized access attempts, or suspicious network activity.
- **Use Network Segmentation**: Implement a zero-trust approach to limit lateral movement in case of a breach.
- **Increase Employee Awareness**: Train employees to recognize phishing and social engineering attacks that could lead to credential theft.
- **Deploy Endpoint Detection and Response (EDR)**: Use EDR solutions to detect and mitigate unauthorized access or suspicious activities.
- **Establish an Incident Response Plan**: Have a tested plan to quickly investigate and contain potential threats.

ADDITIONAL RESOURCES AND OFFICIAL STATEMENTS

https://www.greynoise.io/blog/surge-palo-alto-networks-scanner-activity

https://thehackernews.com/2025/04/nearly-24000-ips-target-pan-os.html

CONTACT US

Vairav Technology Security Pvt. Ltd.

Cyber Defender from the land of Gurkha

Thirbam Sadak 148, Baluwatar

Kathmandu, Nepal

Phone: +977-01-4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

Website: https://vairavtech.com