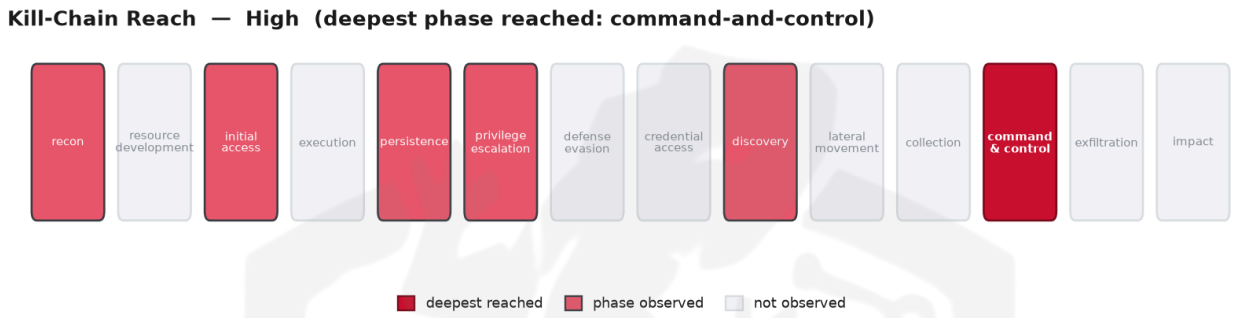
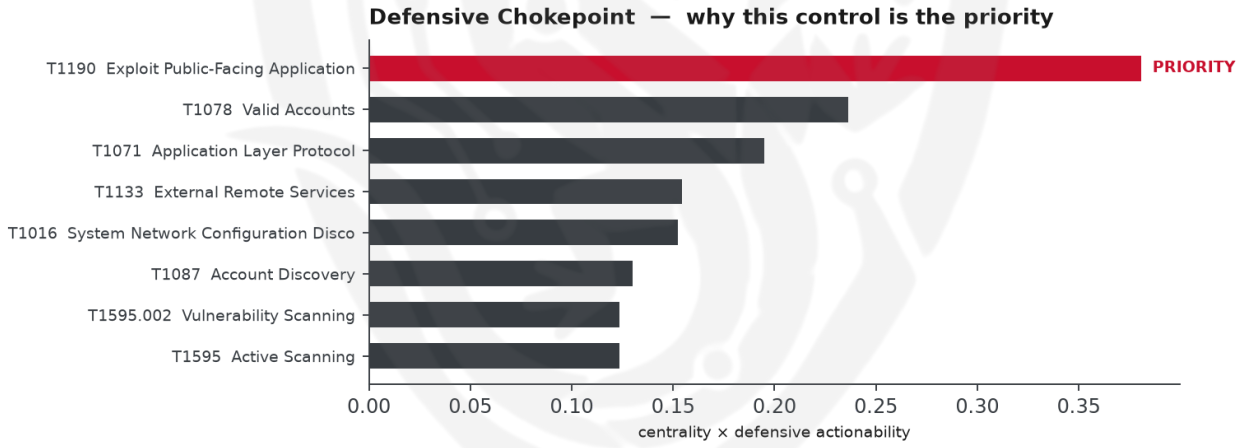
THREAT REPORT: UNKNOWN_ADVERSARY EXPLOITATION OF PAN-OS CVE-2026-0257

Visual Summary



How far down the attack chain this campaign reached; deepest phase in crimson.



The control that most disrupts the attack (priority in crimson).

Summary

The observed cluster of activity is exploiting CVE-2026-0257, a vulnerability in PAN-OS, to target unknown sectors and countries. The threat actor's identity and motivations are currently unknown. Priority should be given to patching the affected systems to prevent further exploitation. The exploitation of this vulnerability poses a high operational risk, reaching command-and-control levels.

Threat Overview

The threat actor is exploiting CVE-2026-0257, a vulnerability in PAN-OS, using various techniques, including external remote services, system information discovery, and application layer protocol. The victimology of this campaign is currently unknown, and the malware families used are insufficient to determine the actor's identity or motivations.

Attack Chain and Priority Control

The observed techniques used by the threat actor form a chain of exploitation, starting with external remote services and system information discovery, followed by application layer protocol and exploit public-facing application. The priority technique is T1190 Exploit Public-Facing Application, which is the graph chokepoint. To mitigate this threat, the priority control is to: Patch CVE-2026-0257 on all affected systems as the top priority, then: Patch the affected public-facing CVE immediately; apply a WAF virtual patch; restrict management interfaces to VPN-only.

Infrastructure and Corroboration

There is no observed hosting provider or ASN associated with this campaign, and no malware families have been corroborated by abuse.ch. Additionally, AbuseIPDB has not flagged any indicators with a confidence level of 80% or higher, with the highest confidence seen being 0%.

Technical Appendix

Ground-truth telemetry from the source pulse; analytical scores are secondary and clearly labelled.

Observed Techniques (ATT&CK, expert-tagged by source)

- T1133 External Remote Services
- T1082 System Information Discovery
- T1071 Application Layer Protocol
- T1190 Exploit Public-Facing Application
- T1595.002 Vulnerability Scanning
- T1595 Active Scanning
- T1016 System Network Configuration Discovery
- T1087 Account Discovery
- T1078 Valid Accounts
- T1046 Network Service Discovery

Analytical Scores

- Priority technique (graph chokepoint): T1190 Exploit Public-Facing Application (centrality 0.3807).
- Operational risk: High (score 0.594, reaches command-and-control).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.3586; reference threshold tau = 0.6).
- These are behavioural resemblances for defensive playbook cross-referencing, not an identity assessment. Where the source pulse names an actor, that attribution is authoritative; the overlaps below neither confirm nor contest it.

Nearest historical profiles by behavioural overlap (resemblance only):

Historical Profile	Behavioural Overlap
Volatile Cedar	0.3586
APT18	0.2981
APT41	0.2949
FIN13	0.2921
Ember Bear	0.2834

Enrichment Signal

- Highest AbuseIPDB confidence among IOCs: 0%.

Indicators of Compromise (defanged — non-clickable)

No indicators were attached to this pulse.

Flame Cell // Adversary Pivot [BETA]

BETA. A hypothetical tabletop projection, anchored to documented ATT&CK behaviour and technique co-occurrence across 170 tracked groups. It is not a prediction; treat it as a war-game prompt and review before acting. Spot a pivot that looks wrong? norbert@salacti.com

- **Control applied:** T1190 Exploit Public-Facing Application (initial-access)
- **Observed here:** the threat actor used T1078 Valid Accounts here as an alternative initial-access technique.
- **Projected pivot:** T1078 Valid Accounts (initial-access)
- **Basis:** observed in this campaign (an alternative the actor already demonstrated).

The actor could pivot to using T1078 Valid Accounts to maintain access and achieve their objectives by potentially exploiting weak passwords or authentication procedures on existing accounts. They may attempt to use compromised credentials to blend in with normal user activity, which would likely require the defender to enhance their account monitoring and authentication controls. The defensive control to counter this potential pivot would be to Enforce MFA on all accounts; disable dormant and over-privileged accounts; alert on impossible-travel and anomalous logons.

Detection and hardening for the pivot (T1078 Valid Accounts)

- **Telemetry:** Windows Security (logon events); Azure AD / IdP sign-in logs; VPN and remote-access logs; Proxy / DLP / data-egress volume telemetry
- **Detect:**
  - Security 4624/4625 (logon success/fail), 4768/4769 (Kerberos TGT/TGS), 4776 (NTLM)

    - Impossible-travel, new-geo, and off-hours sign-ins from the IdP
    - Service or dormant accounts logging on interactively
    - Under valid credentials the identity signal goes quiet: baseline per-account data-egress volume and alert on peer-group and historical deviation (the real exfiltration tell)
- **Harden:**
    - Enforce MFA everywhere; disable stale accounts; rotate exposed credentials
    - Least-privilege review; separate admin from daily-driver accounts
    - Set per-account and per-partner egress baselines with DLP thresholds on sensitive stores
- **MITRE:** M1032 Multi-factor Authentication, M1026 Privileged Account Management, M1027 Password Policies, M1018 User Account Management · DS0028 Logon Session, DS0002 User Account