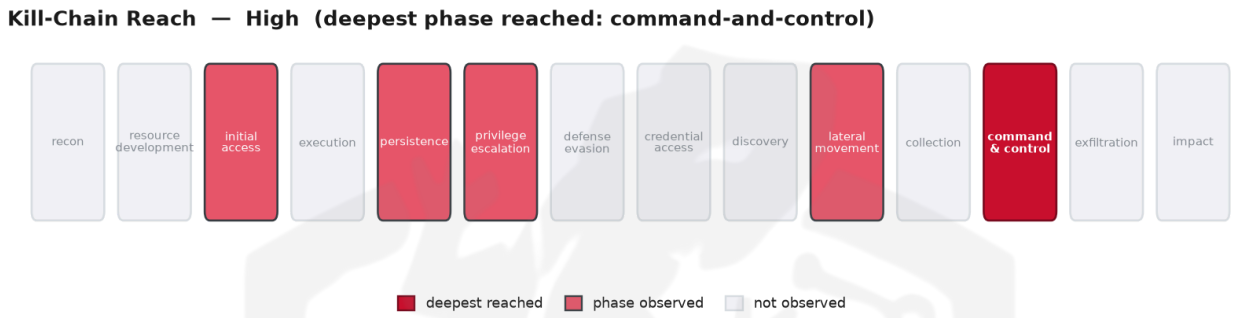
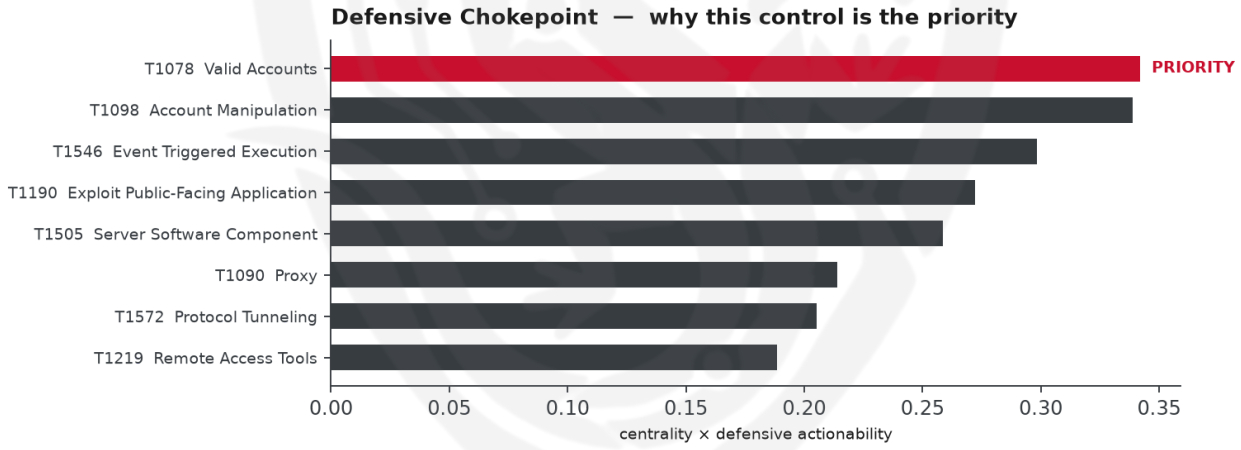
THREAT REPORT: UNATTRIBUTED CAMPAIGN EXPLOITING CVE-2026-18577

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-2026-18577, a vulnerability that poses a significant threat to affected systems. The threat actor is utilizing various techniques to gain access and maintain control over compromised systems. Priority should be given to enforcing multi-factor authentication and patching the exploited vulnerability. The operational risk band is considered high, as the threat actor has reached command-and-control capabilities.

Threat Overview

The threat actor, whose identity is currently unknown, is exploiting CVE-2026-18577, as well as other vulnerabilities such as CVE-2026-18556. The actor is utilizing a range of techniques, including external

remote services, impairing defenses, and exploiting public-facing applications. The victimology and targeted sectors are currently unknown.

Attack Chain and Priority Control

The observed techniques used by the threat actor form a complex chain, including external remote services, windows services, and protocol tunneling. The priority technique is T1078 Valid Accounts, which serves as a chokepoint in the attack chain. To mitigate this threat, the priority control is to Enforce MFA on all accounts; disable dormant and over-privileged accounts; alert on impossible-travel and anomalous logons. In parallel, patch CVE-2026-18577 on all affected systems.

Infrastructure and Corroboration

The malicious infrastructure is hosted on various providers, including Global Connectivity Solutions LLP, DataCamp Limited, Aire Networks del Mediterraneo SL Unipersonal, and Tzulo Inc. According to AbuseIPDB, none of the indicators have reached a confidence level of 80% or higher, with the highest confidence seen being 12%. Abuse.ch has not corroborated any malware families associated with this campaign.

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
- T1543.003 Windows Service
- T1562 Impair Defenses
- T1190 Exploit Public-Facing Application
- T1219 Remote Access Tools
- T1572 Protocol Tunneling
- T1090 Proxy
- T1098 Account Manipulation
- T1078 Valid Accounts
- T1546 Event Triggered Execution
- T1505 Server Software Component
- T1071.001 Web Protocols
- T1136 Create Account
- T1021.001 Remote Desktop Protocol

Analytical Scores

- Priority technique (graph chokepoint): T1078 Valid Accounts (centrality 0.342).
- Operational risk: High (score 0.636, reaches command-and-control).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.375; 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
Orangeworm	0.375
FIN13	0.3464
Cinnamon Tempest	0.3432
BlackByte	0.3385
Medusa Group	0.3313

Enrichment Signal

- Highest AbuseIPDB confidence among IOCs: 12%.

Indicators of Compromise (defanged — non-clickable)

The network and file indicators observed in this activity are listed below for blocklisting:

Type	Indicator	Context
IP	87[.]249[.]138[.]34	AbuseIPDB 4% (US) · AS212238 DataCamp Limited
IP	37[.]153[.]90[.]88	AbuseIPDB 12% (ES) · AS60494 Aire Networks del Mediterraneo SL Unipersonal
IP	92[.]118[.]112[.]181	AbuseIPDB 0% (US) · AS215540 Global Connectivity Solutions LLP
IP	92[.]118[.]112[.]181	AbuseIPDB 0% (US) · AS215540 Global Connectivity Solutions LLP
IP	23[.]234[.]94[.]43	AbuseIPDB 0% (US) · AS11878 Tzulo Inc.

Reputation by AbuseIPDB · malware attribution by abuse.ch · Geo/ASN data by IP2Location LITE.

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:** T1078 Valid Accounts (initial-access)
- **Observed here:** T1078 Valid Accounts was the initial-access control point; blocking a means-of-entry rarely stops a determined actor, so the pivot projects forward to the execution stage they must still reach.
- **Projected pivot:** T1047 Windows Management Instrumentation (execution)
- **Basis:** of the 29+ groups that use Valid Accounts, this pairing runs 1.8x above base rate, a disproportionately-coupled move rather than the obvious one.

The actor could pivot to T1047 Windows Management Instrumentation to maintain access and evade detection, as this technique allows them to leverage the existing Windows management infrastructure to execute commands and gather information, potentially exploiting the same valid account credentials that were previously used. This technique may be particularly appealing to the actor because it enables them to blend in with legitimate administrative activity, making it more challenging to distinguish between benign and malicious behavior. To counter this potential pivot, the mandated defensive control is to monitor wmiprvse.exe child-process creation; restrict remote WMI (DCOM) at the host firewall; enable WMI-Activity operational logging.

Also plausible (same tactic): T1569 System Services (n=13, lift 2.0), T1053 Scheduled Task/Job (n=31, lift 1.4)

Detection and hardening for the pivot (T1047 Windows Management Instrumentation)

- **Telemetry:** Sysmon (WMI events); Microsoft-Windows-WMI-Activity/Operational
- **Detect:**
  - Sysmon 19/20/21 (WMI event filter/consumer/binding) for persistence
  - wmic.exe / WmiPrvSE.exe spawning shells; remote WMI process creation
  - WMI-Activity/Operational operations from unusual users/hosts
- **Harden:**
  - Restrict WMI remote access; monitor permanent WMI subscriptions
  - Least-privilege; segment management protocols
- **MITRE:** M1040 Behavior Prevention, M1038 Execution Prevention, M1026 Privileged Account Management · DS0009 Process, DS0005 WMI, DS0017 Command