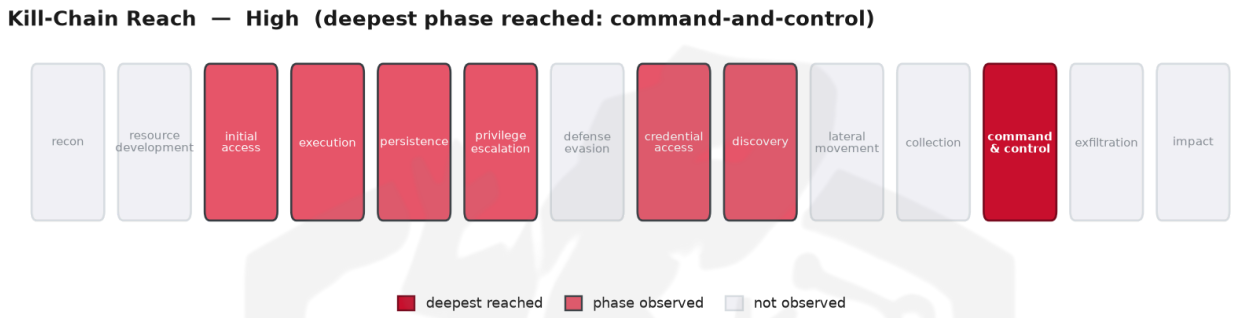
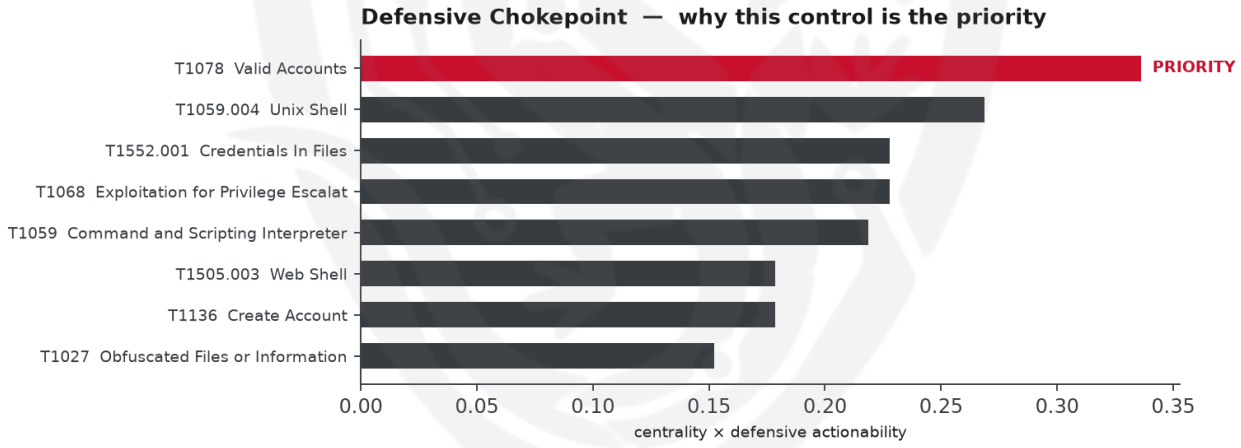
THREAT REPORT: UNKNOWN_ADVERSARY EXPLOITATION OF WP2SHELL

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 the CVE-2026-63030 vulnerability, utilizing the CMSmap malware family to target unknown sectors and countries. The threat actor is leveraging various techniques to gain access and control of systems. Priority should be given to patching the exploited vulnerability and enforcing multi-factor authentication to mitigate the threat. The exploitation of this vulnerability poses a high operational risk, reaching command-and-control levels.

Threat Overview

The threat actor, whose identity is insufficient to determine, is using the CMSmap malware family to exploit the CVE-2026-63030 vulnerability in public-facing applications. The actor is also leveraging other techniques, including deobfuscation, account discovery, and web shell deployment, to achieve their goals.

The targeted systems and sectors are unknown, but the threat actor's use of valid accounts and exploitation for privilege escalation suggests a high level of sophistication.

Attack Chain and Priority Control

The observed techniques used by the threat actor form a complex attack chain, involving deobfuscation, exploitation of public-facing applications, and deployment of web shells. The priority technique is T1078 Valid Accounts, which is the graph chokepoint. To mitigate this threat, the priority control is to: Patch CVE-2026-63030 on all affected systems as the top priority, then: Enforce MFA on all accounts; disable dormant and over-privileged accounts; alert on impossible-travel and anomalous logons.

Infrastructure and Corroboration

The malicious infrastructure is hosted on various providers, including Bezeq- The Israel Telecommunication Corp. Ltd., Akamai Connected Cloud, and Tel Communications L.L.C., as observed by third-party sources. According to AbuseIPDB, none of the indicators have reached an 80% confidence level, with the highest confidence seen being 55%. Abuse.ch has not corroborated any malware families in 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)

- T1140 Deobfuscate/Decode Files or Information
- T1190 Exploit Public-Facing Application
- T1505.003 Web Shell
- T1087 Account Discovery
- T1059 Command and Scripting Interpreter
- T1083 File and Directory Discovery
- T1552.001 Credentials In Files
- T1059.004 Unix Shell
- T1078 Valid Accounts
- T1068 Exploitation for Privilege Escalation
- T1027 Obfuscated Files or Information
- T1027.002 Software Packing
- T1071.001 Web Protocols
- T1136 Create Account
- T1018 Remote System Discovery
- T1046 Network Service Discovery

Analytical Scores

- Priority technique (graph chokepoint): T1078 Valid Accounts (centrality 0.3361).
- 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 0.4059; 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
Fox Kitten	0.4059
APT39	0.3785
FIN13	0.3709
BlackByte	0.3671
Leafminer	0.3599

Enrichment Signal

- Highest AbuseIPDB confidence among IOCs: 55%.

Indicators of Compromise (defanged — non-clickable)

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

Type	Indicator	Context
IP	172[.]235[.]128[.]52	AbuseIPDB 55% (US) · AS63949 Akamai Connected Cloud
IP	79[.]177[.]131[.]206	AbuseIPDB 22% (IL) · AS6810 Bezeq- The Israel Telecommunication Corp. Ltd.
IP	79[.]177[.]131[.]206	AbuseIPDB 22% (IL) · AS6810 Bezeq- The Israel Telecommunication Corp. Ltd.
IP	94[.]100[.]52[.]128	AbuseIPDB 55% (XK) · AS47588 Tel Communications L.L.C.
Hash	2a1410d8e2a8337ac2171cedea8c0fdc47c647a0	

Type	Indicator	Context
Hash	58eca847e9eae9e6b08cc211f1559817b71bc4cc	
Hash	d9a220c8039f1c4d72cae7ccb8b3a33dec8815be	
Hash	e9756e2338f84746007235e4cab7a70d5b3ca47f	
Hash	ebea44890f434d5d67ede22009a3f4bb5cac33f8	

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

With T1078 Valid Accounts blocked, the threat actor could preserve the same objective by pivoting to T1190 Exploit Public-Facing Application, a technique observed in this campaign. Defensive countermeasure: Patch the affected public-facing CVE immediately; apply a WAF virtual patch; restrict management interfaces to VPN-only.

Detection and hardening for the pivot (T1190 Exploit Public-Facing Application)

- **Telemetry:** WAF / reverse-proxy logs; Web server logs; EDR on the DMZ host
- **Detect:**
  - Exploit strings and anomalous request paths in access logs; 500s spikes
  - The web/app service account spawning shells or network tools
  - Outbound connections from a server that should never initiate them
- **Harden:**
  - Patch internet-facing software fast; virtual-patch at the WAF meanwhile
  - Egress filtering from DMZ hosts; least-privilege service accounts
- **MITRE:** M1051 Update Software, M1050 Exploit Protection, M1016 Vulnerability Scanning, M1030 Network Segmentation · DS0015 Application Log, DS0009 Process, DS0029 Network Traffic