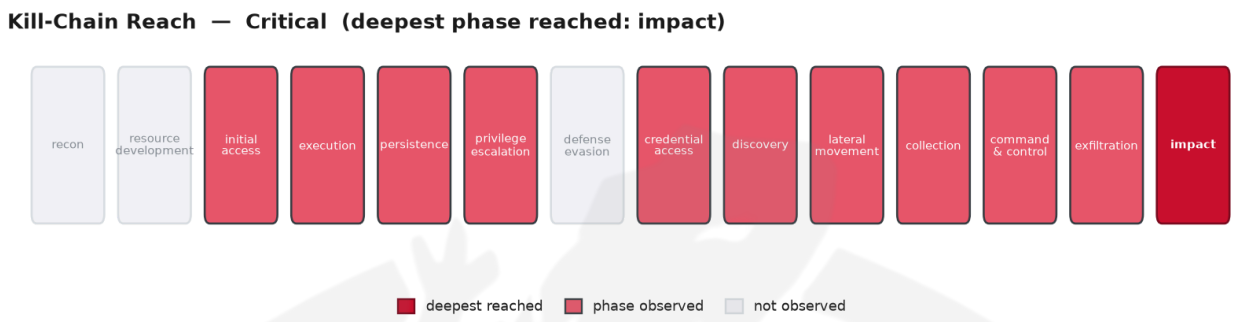
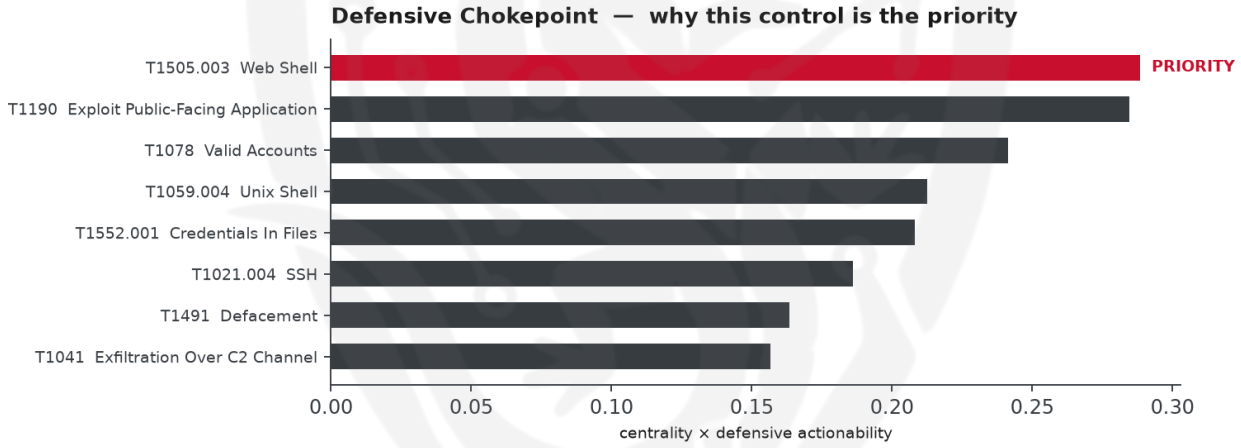
THREAT REPORT: UNC6240

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 source attributes this activity to UNC6240, a threat actor targeting the education sector in the United States of America with an exploit of Oracle PeopleSoft, specifically leveraging the CVE-2026-35273 vulnerability. The malware family used is MeshCentral. Priority should be given to patching the exploited vulnerability to prevent further attacks. The threat actor's activities have been observed to have a critical operational risk band, indicating a significant potential impact.

Threat Overview

UNC6240, the attributed threat actor, has been observed using the MeshCentral malware family to exploit the CVE-2026-35273 vulnerability in Oracle PeopleSoft, targeting the education sector. The victimology indicates that the primary targets are within the United States of America. The exploited vulnerability and the malware used suggest a sophisticated attack chain.

Attack Chain and Priority Control

The observed techniques used by the threat actor form a complex attack chain, including archive via utility, password guessing, and exploit of public-facing applications, among others. The priority technique identified is T1505.003 Web Shell, which serves as a critical chokepoint in the attack chain. The priority action to mitigate this threat is to: Patch CVE-2026-35273 on all affected systems as the top priority, then: Integrity-monitor web-server directories for web shells; restrict server module/plugin installation.

Infrastructure and Corroboration

The malicious infrastructure associated with this activity has been observed to be hosted by Proton66 OOO. There are no corroborated malware families from abuse.ch, and AbuseIPDB has not flagged any indicators with a confidence level of 80% or higher, with the highest confidence seen being 0%. These findings are based on third-party enrichment and corroboration, attributed to their respective sources.

Technical Appendix

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

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

- T1560.001 Archive via Utility
- T1110.001 Password Guessing
- T1133 External Remote Services
- T1069 Permission Groups Discovery
- T1114 Email Collection
- T1036.005 Match Legitimate Resource Name or Location
- T1021.004 SSH
- T1190 Exploit Public-Facing Application
- T1491 Defacement
- T1505.003 Web Shell
- T1083 File and Directory Discovery
- T1552.001 Credentials In Files
- T1041 Exfiltration Over C2 Channel
- T1059.004 Unix Shell
- T1078 Valid Accounts
- T1027 Obfuscated Files or Information
- T1486 Data Encrypted for Impact
- T1573.002 Asymmetric Cryptography
- T1071.001 Web Protocols
- T1018 Remote System Discovery

Analytical Scores

- Priority technique (graph chokepoint): T1505.003 Web Shell (centrality 0.3037).
- Operational risk: Critical (score 1.0, reaches impact).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.4296; 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	0.4296
Akira	0.417
Agrius	0.4068
Ember Bear	0.4042
Ke3chang	0.3977

Enrichment Signal

- Highest AbuseIPDB confidence among IOCs: 0%.

Indicators of Compromise (defanged — non-clickable)

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

Type	Indicator	Context
IP	176[.]120[.]22[.]24	AbuseIPDB 0% (RU) · AS198953 Proto n66 OOO
Domain	azurenetfiles[.]net	malware_download
URL	hxxp://azurenetfiles[.]net:443/agent[.]ashx	malware_download
Hash	c7e9332731b06644fc73e0046a2a89eaa59b09f54250e9bd622467187351711f	
Hash	ebcf977806f68af3147e0b78b55f6aed	
Hash	cc19e502e4201cc974c753b96429027925224f53	

Type	Indicator	Context
Hash	2ab684d93c1553fad87041b4dea97188a97e78589deee2a7bacff905564f3a35	
Hash	68257a6f9ff196179ec03624e849927f26599eb180a7c82e14ef5bc4e93bc309	
Hash	d83fdb9e53c5ff03c4cb0451ea1bebd79b53f29eadc1e2fa394c7af13a86ce2f	
Hash	f02a924c9ff92a8780ce812511341182c6b509d45bc59f3f7b522e37225d24fc	

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