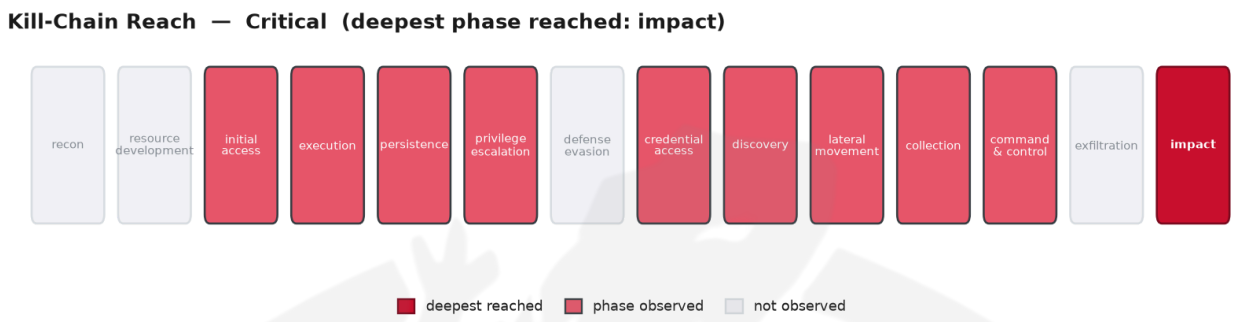
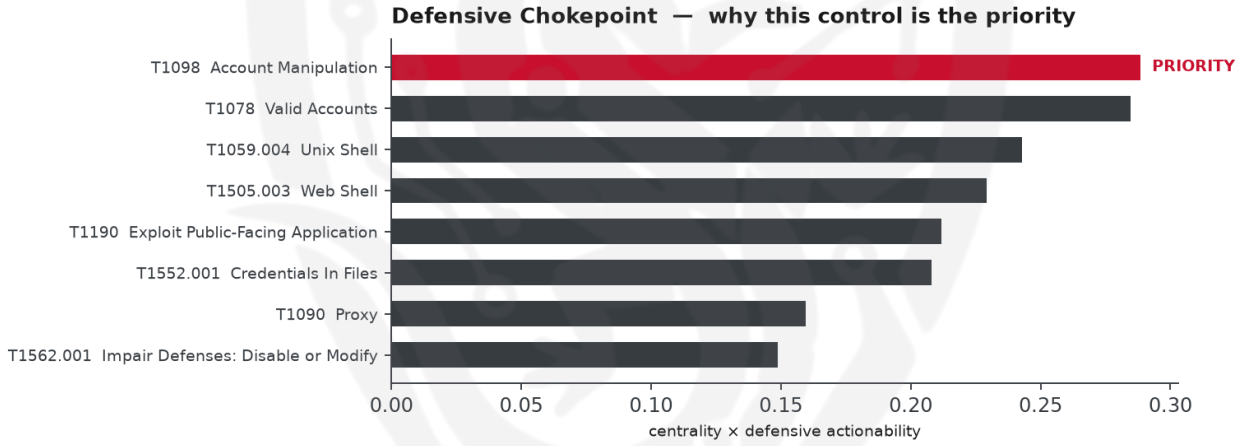
THREAT REPORT: UAT-8616

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 UAT-8616, who is exploiting Cisco Catalyst SD-WAN vulnerabilities, particularly CVE-2026-20128, to target unknown countries and sectors. The threat actor is utilizing various malware families, including XenShell, Godzilla, and Behinder, to gain access to systems. Priority should be given to patching the exploited vulnerability and monitoring for suspicious account activity. The actor's use of multiple techniques, including OS credential dumping and exploit of public-facing applications, poses a significant threat.

Threat Overview

UAT-8616 is exploiting the CVE-2026-20128 vulnerability in Cisco Catalyst SD-WAN, using malware families such as XenShell, Godzilla, Behinder, Sliver, AdaptixC2, XMRig, Nimplant, KScan, and gsocket. The threat actor is targeting systems, although the specific countries and sectors affected are unknown.

The exploited vulnerability allows the actor to gain access to systems, where they can use various techniques to maintain access and evade detection.

Attack Chain and Priority Control

The observed techniques used by UAT-8616 form a complex attack chain, involving OS credential dumping, cloud instance metadata API exploitation, and web shell usage. The priority technique is T1098 Account Manipulation, which is the graph chokepoint. To mitigate this threat, the priority control is: Patch CVE-2026-20128 on all affected systems as the top priority, then: Alert on privilege/group changes and credential additions to accounts (Event ID 4738/4670); review conditional-access changes.

Infrastructure and Corroboration

Although the primary infrastructure details are not available, third-party enrichment sources provide some corroboration. Abuse.ch has corroborated the presence of the CoinMiner malware family, which may be related to the observed activity. However, AbuseIPDB has not flagged any indicators with high confidence, 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)

- T1003 OS Credential Dumping
- T1552.005 Cloud Instance Metadata API
- T1021.004 SSH
- T1005 Data from Local System
- T1190 Exploit Public-Facing Application
- T1505.003 Web Shell
- T1090 Proxy
- T1083 File and Directory Discovery
- T1552.001 Credentials In Files
- T1098 Account Manipulation
- T1059.004 Unix Shell
- T1562.001 Impair Defenses: Disable or Modify Tools
- T1078 Valid Accounts
- T1027 Obfuscated Files or Information
- T1573 Encrypted Channel
- T1496 Resource Hijacking
- T1070.004 File Deletion
- T1071.001 Web Protocols
- T1136 Create Account
- T1018 Remote System Discovery

Analytical Scores

- Priority technique (graph chokepoint): T1098 Account Manipulation (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 0.4355; 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	0.4355
APT39	0.4243
APT5	0.4012
FIN13	0.3926
Ember Bear	0.3841

Enrichment Signal

- Highest AbuseIPDB confidence among IOCs: 0%.
- Malware families corroborated by abuse.ch: CoinMiner.
- Note: enrichment raises the severity signal (an IOC at or above 80% AbuseIPDB confidence, or a confirmed malware-family hit). This is context, not a change to the source assessment.

Indicators of Compromise (defanged — non-clickable)

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

Type	Indicator	Context
Domain	1a820b09-95ba-44eb-b350-417e8241b725-00-1lgwuuen9b77p[.]worf[.]replit[.]dev	
Domain	a820b09-95ba-44eb-b350-417e8241b725-00-1lgwuuen9b77p[.]worf[.]replit[.]dev	
URL	hxxp://83[.]229[.]126[.]195:8081/config[.]json	

Type	Indicator	Context
URL	hxxps://1a820b09-95ba-44eb-b350-417e8241b725-00-1lgwuuen9b77p[.]worf[.]replit[.]dev/download	
Hash	d94f75a70b5cabaf786ac57177ed841732e62bdcc9a29e06e5b41d9be567bcfa	
Hash	d75cb9920d1d3d280518ddccfe4789d2	
Hash	18821dbb53892d6faa14b1f063517a0302057290	
Hash	cf127d66124c390ca0f0b42c6385c3c8	CoinMiner
Hash	01e3dce00ea45829bd9f6a583004976ac63973a0	CoinMiner
Hash	96fc528ca5e7d1c2b3add5e31b8797cb126f704976c8fbeaecdbf0aa4309ad46	CoinMiner
Hash	e22d1b625ee309b60caf0252c5df7656	
Hash	fece5b954e69b2c6a8d0a1029631a0d7	
Hash	d0a851f0b871df60c73d2c7d3f55b031c45e4c2e	
Hash	02654acfb21f83485393ba8b14bd8862b919b9ec966fc6768f6aac1338a45ee8	
Hash	0c87871642f84e09e8d3fb23ec36bf55601323e31151a7017a85dbec929cf15d	
Hash	0ed72d52347bfe4a78afff8a6982a64050c8fc86d8957a20eeb3e0f3f5342ed0	
Hash	17302d903baf182f94dc3be40ab1e0874dd0eb2ec5255bf9131fd53591efe925	
Hash	18d77c9c5bbb5b9d5bdfd366fdfcf26bad9e64c63ca865fad711bcce8e3d5a80	
Hash	5bc5998161056b7c8f70c9724d8a63abc7ff8c3843b91c30cffab0899e39b7f8	
Hash	72f570ce97de3eaaffef33d90b0c337a153fc9690cc34ee207b557d868360060	
Hash	7aa88a64a527ade7d93c20faf23b54f2ee33ad9b1246cdc2f8ded2ab639affb1	
Hash	b0f51b098842cd630097b462aab0ec357e2c7824af37cca6d08165265da2c2d3	
Hash	f6f8e0d790645395188fc521039385b7c4f42fa8b426fd035f489f6cda9b5da1	

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