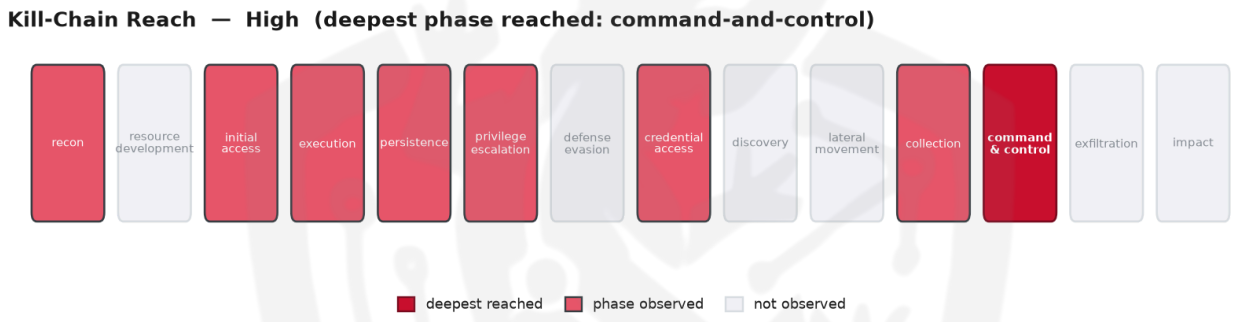
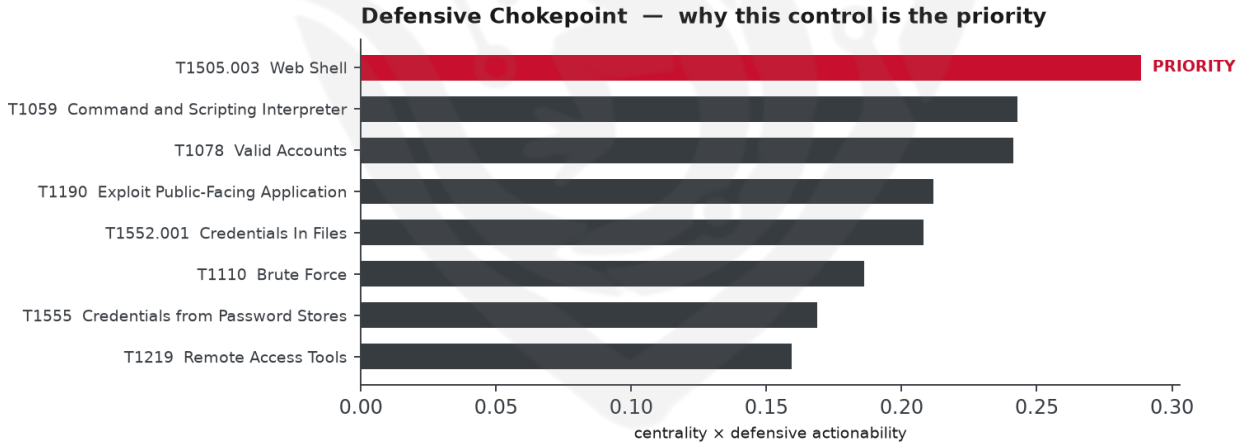
THREAT REPORT: SUSPECTED CHINESE OPERATORS USE CLAUDE CODE AND DEEPSEEK TO BREACH GOVERNMENT SYSTEMS ACROSS FOUR COUNTRIES

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

This brief covers activity involving TencShell, HSEWH-Ur, Vshell, Gshell, with no single central CVE identified, affecting United States of America, Afghanistan, Taiwan, Thailand, Government, Finance, Telecommunications, Chemical, Manufacturing, Semiconductor. The source does not attribute this activity to a named actor. The operational risk is assessed as High. Priority should be given to the control described below, centred on T1505.003 Web Shell.

Threat Overview

The activity is associated with an as-yet unattributed cluster of activity. Malware observed: TencShell, HSEWH-Ur, Vshell, Gshell. Reported victimology: United States of America, Afghanistan, Taiwan, Thailand, Government, Finance, Telecommunications, Chemical, Manufacturing, Semiconductor.

Attack Chain and Priority Control

The source records the following techniques: - T1592 Gather Victim Host Information - T1133 External Remote Services - T1566.002 Spearphishing Link - T1005 Data from Local System - T1190 Exploit Public-Facing Application - T1555 Credentials from Password Stores - T1219 Remote Access Tools - T1589 Gather Victim Identity Information - T1595.002 Vulnerability Scanning - T1505.003 Web Shell - T1059 Command and Scripting Interpreter - T1552.001 Credentials In Files - T1590 Gather Victim Network Information - T1110 Brute Force - T1078 Valid Accounts - T1027 Obfuscated Files or Information - T1573 Encrypted Channel - T1213 Data from Information Repositories - T1189 Drive-by Compromise - T1071.001 Web Protocols

Priority should be given to T1505.003 Web Shell. Recommended control: Integrity-monitor web-server directories for web shells; restrict server module/plugin installation.

Technical Appendix

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

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

- T1592 Gather Victim Host Information
- T1133 External Remote Services
- T1566.002 Spearphishing Link
- T1005 Data from Local System
- T1190 Exploit Public-Facing Application
- T1555 Credentials from Password Stores
- T1219 Remote Access Tools
- T1589 Gather Victim Identity Information
- T1595.002 Vulnerability Scanning
- T1505.003 Web Shell
- T1059 Command and Scripting Interpreter
- T1552.001 Credentials In Files
- T1590 Gather Victim Network Information
- T1110 Brute Force
- T1078 Valid Accounts
- T1027 Obfuscated Files or Information
- T1573 Encrypted Channel
- T1213 Data from Information Repositories
- T1189 Drive-by Compromise
- T1071.001 Web Protocols

Analytical Scores

- Priority technique (graph chokepoint): T1505.003 Web Shell (centrality 0.3037).
- 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 0.3831; 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
Sandworm Team	0.3831
Volatile Cedar	0.378
APT33	0.3501
Sea Turtle	0.3479
GOLD SOUTHFIELD	0.3464

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	112[.]213[.]124[.]159	AbuseIPDB 0% (HK) · AS152194 CTG Server Limited
IP	134[.]122[.]200[.]153	AbuseIPDB 0% (HK) · AS152194 CTG Server Limited
IP	134[.]122[.]200[.]154	AbuseIPDB 0% (HK) · AS152194 CTG Server Limited
IP	134[.]122[.]200[.]155	AbuseIPDB 0% (HK) · AS152194 CTG Server Limited

Type	Indicator	Context
IP	192[.]229[.]115[.]229	AbuseIPDB 0% (HK) · AS138995 Antbox Networks Limited
IP	45[.]64[.]52[.]242	AbuseIPDB 0% (HK) · AS152194 CTG Server Limited
IP	192[.]238[.]134[.]166	AbuseIPDB 0% (HK) · AS138995 Antbox Networks Limited
IP	112[.]213[.]124[.]132	AbuseIPDB 0% (HK) · AS152194 CTG Server Limited
IP	112[.]213[.]124[.]163	AbuseIPDB 0% (HK) · AS152194 CTG Server Limited
IP	134[.]122[.]200[.]114	AbuseIPDB 0% (HK) · AS152194 CTG Server Limited
IP	134[.]122[.]200[.]115	AbuseIPDB 0% (HK) · AS152194 CTG Server Limited
IP	134[.]122[.]200[.]116	AbuseIPDB 0% (HK) · AS152194 CTG Server Limited
IP	192[.]163[.]167[.]10	AbuseIPDB 0% (HK) · AS138995 Antbox Networks Limited
IP	192[.]163[.]167[.]5	AbuseIPDB 0% (HK) · AS138995 Antbox Networks Limited
IP	192[.]163[.]167[.]6	AbuseIPDB 0% (HK) · AS138995 Antbox Networks Limited
IP	192[.]163[.]167[.]7	AbuseIPDB 0% (HK) · AS138995 Antbox Networks Limited
IP	192[.]229[.]115[.]230	AbuseIPDB 0% (HK) · AS138995 Antbox Networks Limited
IP	38[.]55[.]105[.]143	AbuseIPDB 0% (HK) · AS967 VMISS Inc.
IP	45[.]64[.]52[.]245	AbuseIPDB 0% (HK) · AS152194 CTG Server Limited
IP	45[.]64[.]52[.]246	AbuseIPDB 0% (HK) · AS152194 CTG Server Limited

Type	Indicator	Context
Hash	90b7b2c6f3d05234dc55678243039d7e51f0d54190239e5234a0005533337dc8	
Hash	050b84a0d6105a98f443f0165368cc1c	
Hash	4da236de055bfaf08ee21fb6b88442b4	
Hash	1cac633d290a876fc1ead63c58de48575b67b1fc	
Hash	66049dd42a29dde7481d5ca2951efec27214ce15	
Hash	03f26cbfa3ca15fcb43f512aa4041732beeec267f9d1dc74a11f7b0bb32e86bb	
Hash	2954639be599f23c2229a9743aba09a1d9d11bf2becc62bf353384437db37dee	
Hash	64107e3e0a333f685d1be6386426223a030c4126ac7c295aa7b1d54c508bbace	
Hash	643de2a1cf9148b896efecf560c9476fa56118ec477c4e15eb5c2da4b318061f	
Hash	ad1a0b3e22a10a2bd680b773b178a0d3824cfcbdf3551016f3d052a0b823079f	

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:** T1505.003 Web Shell (persistence)
- **Observed here:** the threat actor used T1078 Valid Accounts here as an alternative persistence technique.
- **Projected pivot:** T1078 Valid Accounts (persistence)
- **Basis:** observed in this campaign (an alternative the actor already demonstrated).

With T1505.003 Web Shell blocked, the threat actor could preserve the same objective by pivoting to T1078 Valid Accounts, a technique observed in this campaign. Defensive countermeasure: 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