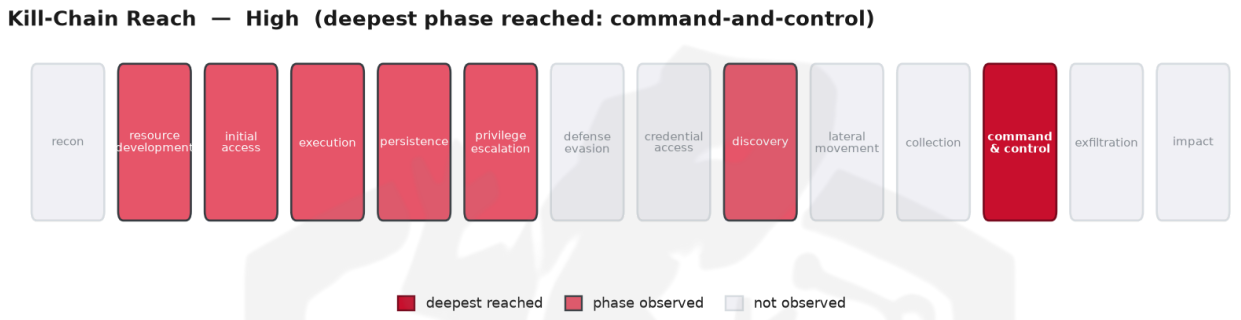
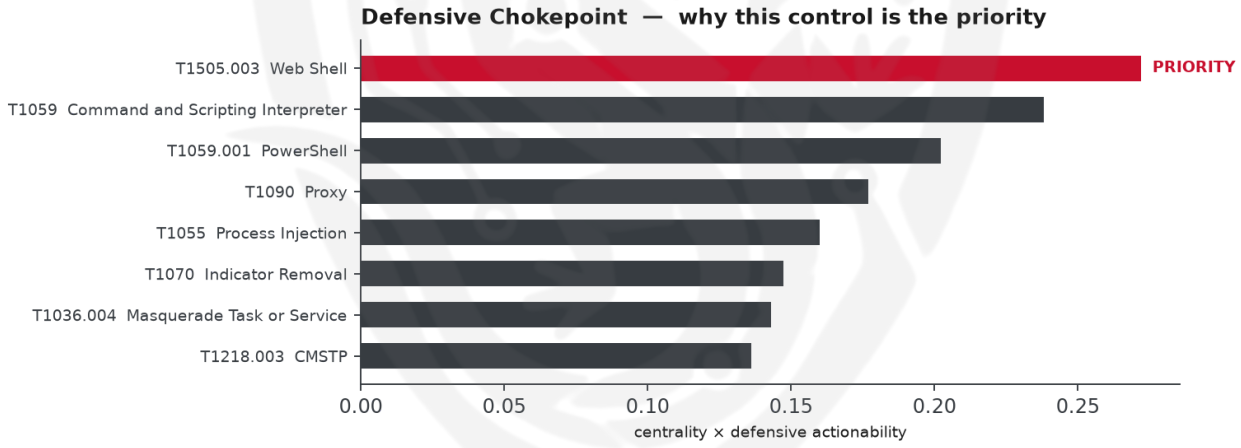
THREAT REPORT: CHINA-NEXUS CAMPAIGN AGAINST GOVERNMENT INFRASTRUCTURE

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 China-nexus threat actor is attributed to a campaign targeting government infrastructure, exploiting the CVE-2025-24813 vulnerability and utilizing various malware families, including GOCS, Meterpreter, and SNOWLIGHT. The targeted country and sectors are currently unknown. Priority should be given to integrity-monitoring web-server directories for web shells and restricting server module/plugin installation, as well as patching the exploited CVE on all affected systems.

Threat Overview

The China-nexus threat actor is observed using a range of malware families, including GOCS, Meterpreter, Neo-reGeorg, and SNOWLIGHT, to exploit the CVE-2025-24813 vulnerability. The

victimology of this campaign is not well-defined due to insufficient data on the targeted country and sectors. The malware families and exploited vulnerability suggest a sophisticated attack chain.

Attack Chain and Priority Control

The observed techniques form a complex attack chain, involving system information discovery, deobfuscation, and exploitation of public-facing applications. The priority technique is T1505.003 Web Shell, which serves as a critical chokepoint in the attack chain. To mitigate this threat, the priority control is to "Integrity-monitor web-server directories for web shells; restrict server module/plugin installation. In parallel, patch CVE-2025-24813 on all affected systems."

Infrastructure and Corroboration

The malicious infrastructure is hosted on various providers, including Light Node Limited, China Unicom China169 Backbone, Alibaba (US) Technology Co. Ltd., and G-Core Labs S.A. Additionally, abuse.ch has corroborated the presence of Cobalt Strike malware families. However, according to AbuseIPDB, there are no indicators with a confidence level of 80% or higher, 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)

- T1082 System Information Discovery
- T1140 Deobfuscate/Decode Files or Information
- T1190 Exploit Public-Facing Application
- T1583.001 Domains
- T1036 Masquerading
- T1055 Process Injection
- T1070.006 Timestomp
- T1218.003 CMSTP
- T1505.003 Web Shell
- T1090 Proxy
- T1059 Command and Scripting Interpreter
- T1070 Indicator Removal
- T1036.004 Masquerade Task or Service
- T1583.006 Web Services
- T1059.001 PowerShell
- T1588.002 Tool
- T1027 Obfuscated Files or Information
- T1573 Encrypted Channel
- T1059.003 Windows Command Shell
- T1071.001 Web Protocols

- T1105 Ingress Tool Transfer

Analytical Scores

- Priority technique (graph chokepoint): T1505.003 Web Shell (centrality 0.3105).
- 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 0.4557; 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
Metador	0.4557
APT38	0.447
LazyScripter	0.4297
BackdoorDiplomacy	0.428
Winter Vivern	0.4249

Enrichment Signal

- Highest AbuseIPDB confidence among IOCs: 0%.
- Malware families corroborated by abuse.ch: Cobalt Strike.
- 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
IP	221[.]198[.]83[.]248	AbuseIPDB 0% (CN) · AS4837 China Unicom Chin a169 Backbone
IP	149[.]129[.]37[.]105	AbuseIPDB 0% (SG) · Cobalt Strike · AS45102 Alib aba (US) Technology Co. Ltd.

Type	Indicator	Context
IP	92[.]38[.]135[.]196	AbuseIPDB 0% (KR) · AS202422 G-Core Labs S. A.
IP	130[.]94[.]30[.]168	AbuseIPDB 0% (KR) · AS154177 Light Node Limited
IP	130[.]94[.]17[.]180	AbuseIPDB 0% (US) · Cobalt Strike · AS154177 Light Node Limited
Domain	google[.]chromeupgrades[.]com	
Domain	speedtest[.]qqmail[.]website	
URL	hxxp://139[.]0[.]0[.]0	
URL	hxxp://130[.]94[.]30[.]168:8080	
URL	hxxp://149[.]129[.]37[.]105:30005	
URL	hxxp://92[.]38[.]135[.]196:8888	
Hash	d7ed70cdd88f6cccbdc0ad6851d7a61b7fce79fdf9c4cd9f9bb375233a96b2dd	
Hash	456233b58bcf8c17ef9ef44b14a966a6	
Hash	71072a8c4adfcde49a4b163959a24283	
Hash	8887c65035893d99996991282553fc19	
Hash	913a572c1bf9da27ee7d21befa3cee0c	
Hash	9ab45387111475d5cfb77fb4e49eba82bad7ca4d	
Hash	a24b4bb466324459f40e6adbc5d481ec6cee48ef	
Hash	b1f71014f4c0e1e61c0b3fe2391a6c6aa03ac3f9	
Hash	d26f84a768062c52179216bf6ca4c551448890be	
Hash	00b0cef237d9619c99c5d90cf902ec768c1ecf4f96d542d31dc5afb0b564cb4f	
Hash	20e1ec6b07abe3b2dd54f7ae4e47dc00afa46de6e6c0ef0239c26c8bae70a43a	

Type	Indicator	Context
Hash	2ac6c953d2d36eb7e7e85aa0822a65961071f7801a25118ab42bcfa9693327a1	
Hash	4738f3559c10f7c62a3be48ec2ce42c584b53d5ffa9e06e6521607a6fdfd535f	
Hash	66543c4f9f4d610a79efa5e52b9aa90ca41dbfc154418435a2902ac48dad2ee4	
Hash	75d39860a5c5ce6c26590265102f25c50f91a22b6769d22046759fb3aff8d0a8	
Hash	9c59a0dadec1f1b73724f3ee4113e4fde696214371b9068fd69774db4cd8b8d2	
Hash	a4989ae1d598e79a87a9e01d0b5966a25b00b23ca234fbdb52b9df7b29db918a	
Hash	adde431d5b78b2b2cfb67c5bcd938be6cc466fbb3ac2786cad97b493f6fcfad5	
Hash	b272e2e4a7c65f2659a8fff8ceec4d9538f74f6dc9bace7d051a4476ba6bc77c	
Hash	b7486bb7fc5f7e659b40dab3366b576d68db61ca0004de7a1e115eb9b541f19a	
Hash	b96cdf8bc96c7288af7624974b1a10b7bf16e5ac03ac8493ade20696a906a81a	
Hash	c0a5374a425ee5030b2219520dfa3a3a51f27d3cc4404b016e695c4450fe3034	
Hash	c2d0e4dd2f2b3f1d4eb4518984b00ed521c73d1e935780786479db690112ef9c	
Hash	dc493eb8367b7d68f4d3d9f2a10c495c6a45c33df72fb5a18bdf62b629f69e31	
Hash	ebc94e24e4df94f988dd0a2275e8a3f1957051814a3c39ec30bfaca2f5ca2607	

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:** T1505.003 Web Shell was the only persistence technique observed in this campaign, so the pivot is projected from cross-actor behaviour.
- **Projected pivot:** T1136 Create Account (persistence)
- **Basis:** of the 12+ groups that use Web Shell, this pairing runs 2.9x above base rate, a disproportionately-coupled move rather than the obvious one.

The adversary could pivot to T1136 Create Account to maintain access and evade detection, as this technique would allow them to create a new account with elevated privileges, potentially leveraging the existing web shell's access to create a more persistent foothold. This technique may be particularly appealing to a China-nexus actor, as it enables them to blend in with normal administrative activities, making it harder to detect malicious intent. The defensive countermeasure to mitigate this would be to alert on new local/domain account creation (Event ID 4720/4728) and enforce an approval workflow for account provisioning.

Also plausible (same tactic): T1133 External Remote Services (n=13, lift 2.5), T1078 Valid Accounts (n=24, lift 2.0)

Detection and hardening for the pivot (T1136 Create Account)

- **Telemetry:** Windows Security (account management); IdP audit logs
- **Detect:**
  - Security 4720 (local user created), 4741 (computer account), 4728 (added to group)
  - New cloud/IdP accounts created outside HR/provisioning workflow
- **Harden:**
  - Restrict account creation to provisioning systems; alert on manual creation
  - Periodic review of recently created accounts
- **MITRE:** M1026 Privileged Account Management, M1032 Multi-factor Authentication · DS0002 User Account