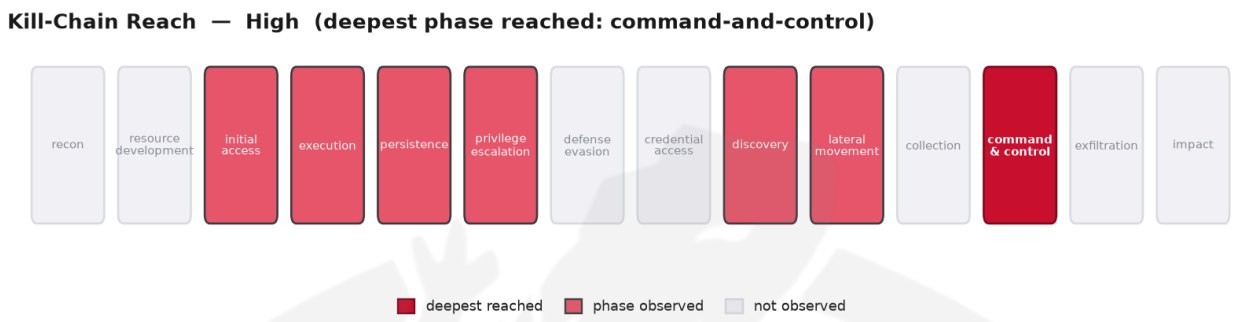
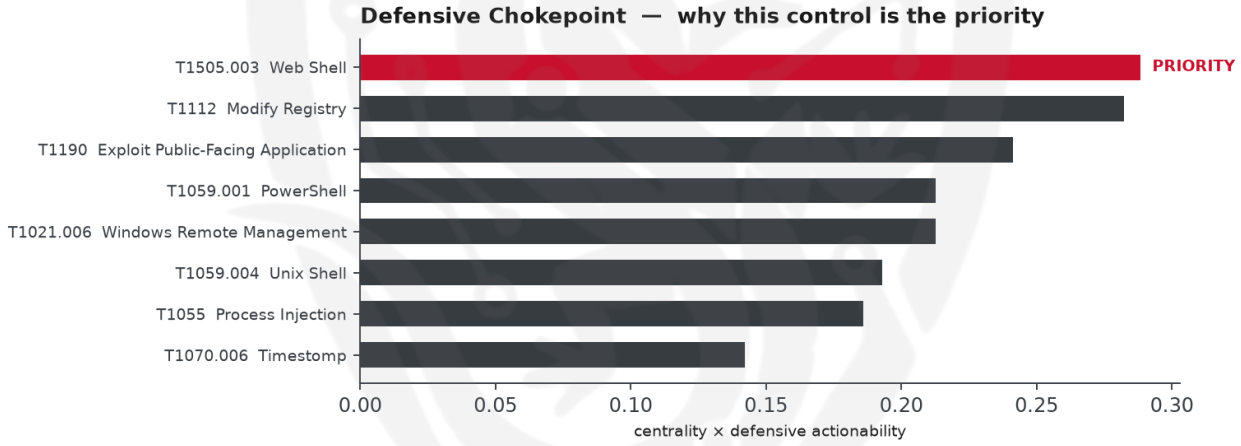
THREAT REPORT: UNKNOWN_ADVERSARY

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 has been identified as utilizing multiple malware families, including China Chopper, AntSword, and Nezha, to target a wide range of countries. The threat actor's targets span across the globe, with a notable presence in the United States of America, among others. Priority should be given to defending against web shell attacks, as this technique has been identified as a key chokepoint in the attack chain. Integrity monitoring of web-server directories and restricting server module/plugin installation are crucial defensive actions.

Threat Overview

The threat actor, referred to here as the observed cluster of activity, employs a variety of malware families, including China Chopper, AntSword, Nezha, Ghost RAT, and others. The exploited vulnerability is not specified, and the victimology is broad, affecting numerous countries across various sectors. The malware families utilized by the threat actor are diverse, indicating a potentially sophisticated attack strategy.

Attack Chain and Priority Control

The observed techniques form a complex attack chain, involving system information discovery, process injection, and web shell deployment, among others. The priority technique, T1505.003 Web Shell, 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."

Infrastructure and Corroboration

The malicious infrastructure is hosted on providers such as CognetCloud Inc and Netlab Global, as observed through third-party enrichment. However, no malware families have been corroborated by abuse.ch, and no indicators have reached an AbuseIPDB 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)

- T1218.011 Rundll32
- T1036.005 Match Legitimate Resource Name or Location
- T1543.003 Windows Service
- T1082 System Information Discovery
- T1140 Deobfuscate/Decode Files or Information
- T1190 Exploit Public-Facing Application
- T1055 Process Injection
- T1070.006 Timestomp
- T1112 Modify Registry
- T1505.003 Web Shell
- T1021.006 Windows Remote Management
- T1083 File and Directory Discovery
- T1057 Process Discovery
- T1059.001 PowerShell
- T1059.004 Unix Shell
- T1562.001 Impair Defenses: Disable or Modify Tools
- T1027 Obfuscated Files or Information
- T1071.001 Web Protocols
- T1018 Remote System Discovery
- T1569.002 Service Execution

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 0.4792; 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
Blue Mockingbird	0.4792
APT38	0.4738
Rocke	0.4543
BlackByte	0.442
APT32	0.4222

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	45[.]207[.]220[.]12	AS401701 CognetCloud Inc
IP	38[.]246[.]250[.]201	AS979 Netlab Global
Domain	gd[.]bj2[.]xyz	
Domain	c[.]mid[.]al	
Domain	host[.]404111[.]xyz	
Hash	d757ec4d5350843c44dd34a95dcb3a50	

Type	Indicator	Context
Hash	ad5e5b00f58396f5a518680e7084dc7dd5f2cc2b	
Hash	7b2599ed54b72daec0acfd32744c7a9a77b19e6cf4e1651837175e4606dbc958	
Hash	35e0b22139fb27d2c9721aedf5770d893423bf029e1f56be92485ff8fce210f3	
Hash	9f33095a24471bed55ce11803e4ebbed5118bfb5d3861baf1c8214efcd9e7de6	
Hash	f3570bb6e0f9c695d48f89f043380b43831dd0f6fe79b16eda2a3ffd9fd7ad16	
Hash	6f336f372c5a642b57413363265e7d7e	
Hash	89cb9c926e136c54011f3e0792b4a28c	
Hash	1c948822cb57763c1d343542ee4ade212d8f4fbb	

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 T1112 Modify Registry here as an alternative persistence technique.
- **Projected pivot:** T1112 Modify Registry (persistence)
- **Basis:** observed in this campaign (an alternative the actor already demonstrated).

The threat actor could pivot to modifying registry settings using T1112 to maintain persistence or evade detection, potentially altering system configurations to achieve their objectives. This modification may allow the actor to bypass existing security controls, assuming they can gain the necessary privileges. To counter this potential move, the defensive control would be to Monitor sensitive registry keys for modification; restrict registry-edit tools for unprivileged users.

Detection and hardening for the pivot (T1112 Modify Registry)

- **Telemetry:** Sysmon (registry); EDR registry telemetry
- **Detect:**
  - Sysmon 12/13/14 (registry object add/set/rename) on sensitive keys
  - Writes to Run keys, service keys, security-provider and policy keys

    - reg.exe / regsvr32 spawned by office or script interpreters
- **Harden:**
    - Audit and restrict write access to security-sensitive registry hives
    - Application control to limit who can modify policy/security keys
- **MITRE:** M1047 Audit, M1024 Restrict Registry Permissions · DS0024 Windows Registry, DS0009 Process