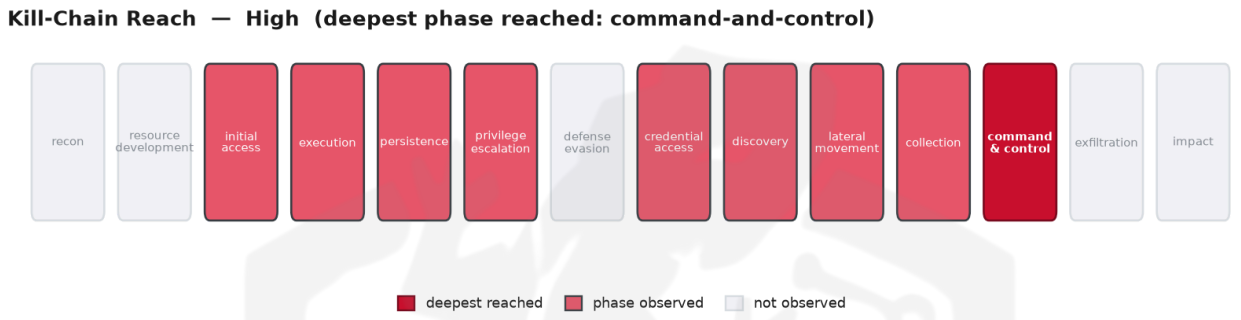
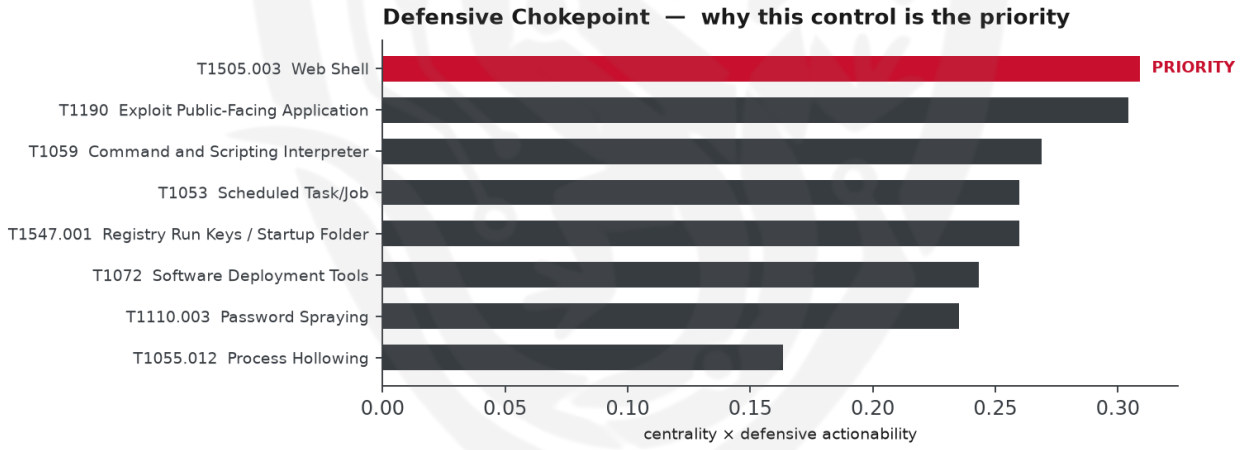
THREAT REPORT: THAILAND MINISTRY OF FINANCE TARGETED WITH HADES AND HERMES

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 targeted Thailand's Ministry of Finance with a combination of Hades and Hermes malware, exploiting CVE-2026-43500. The threat actor has utilized various techniques to gain access and control, making it essential to prioritize defensive actions. Priority should be given to patching the exploited vulnerability and monitoring web-server directories for web shells. The attack has significant implications for the government and finance sectors in Thailand.

Threat Overview

The threat actor, whose identity is currently insufficient to determine, has employed the Hades, VShell, and ShadowPad malware families to target the Ministry of Finance in Thailand. The central vulnerability

exploited is CVE-2026-43500, with other CVEs also cited as potentially exploited. The victimology indicates a focus on government and finance sectors within Thailand.

Attack Chain and Priority Control

The observed techniques form a complex chain, starting with initial exploitation and leading to privilege escalation and command-and-control establishment. The priority technique identified is T1505.003 Web Shell, which serves as a critical chokepoint in the attack chain. To mitigate this threat, the priority action is to: Patch CVE-2026-43500 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 is hosted on providers including Topway Global Limited, Teleglobal Communication Services Limited, and Anyun Internet Technology (HK) Co. Limited, as observed. However, no malware families have been corroborated by abuse.ch, and no indicators have reached an 80% confidence level on AbuseIPDB, 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)

- T1113 Screen Capture
- T1539 Steal Web Session Cookie
- T1036.005 Match Legitimate Resource Name or Location
- T1082 System Information Discovery
- T1053 Scheduled Task/Job
- T1190 Exploit Public-Facing Application
- T1505.003 Web Shell
- T1110.003 Password Spraying
- T1059 Command and Scripting Interpreter
- T1083 File and Directory Discovery
- T1072 Software Deployment Tools
- T1547.001 Registry Run Keys / Startup Folder
- T1055.012 Process Hollowing
- T1068 Exploitation for Privilege Escalation
- T1071.001 Web Protocols
- T1090.001 Internal Proxy

Analytical Scores

- Priority technique (graph chokepoint): T1505.003 Web Shell (centrality 0.3254).

- 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 0.3932; 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
APT39	0.3932
APT18	0.3932
FIN13	0.3612
BlackByte	0.3593
Dark Caracal	0.3349

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	43[.]246[.]208[.]207	AbuseIPDB 0% (HK) · AS132883 Topway Global Limited
IP	103[.]97[.]0[.]57	AbuseIPDB 0% (HK) · AS133073 Teleglobal Communication Services Limited
IP	202[.]181[.]27[.]115	AbuseIPDB 0% (HK) · AS134196 Anyun Internet Technology (HK) Co. Limited
Domain	mail4[.]pl	
Domain	redhatupdating432[.]dnsrd[.]com	

Type	Indicator	Context
Hash	9c9976adbb1f4cda0e3ba85d3ed9c211	
Hash	cfa6312db63b91f8c4022078a487c1c86b7e0901	
Hash	0f8c905aa25c86f85454acb7e77bf5c50220c2a82e5b69a33741e55c8a85f2fc	
Hash	2a4cb412efa93fed7c3b3b3e49d6247b11a95ce9fddf71d9fe9db8e5f0068e0d	
Hash	5633bc0033fde3aad929d6cbd47c554e264180360b017aae04687c2d6d83f753	
Hash	576c70e12be8b2e8e7c35a5feb082e90621989adce8e64400126918d37f13e49	
Hash	58338a93fee4e008ea28e459c4d1598313d1524763ab13894ab63bf2bec4302a	
Hash	9ff4b6d3b7dbb023bad65d2538ade745d46b763e5a12116c9c83aa2f6f5d96aa	
Hash	a9447ae174f4aa54f760b7d7cc985c1a970f31e151d3ff66fac247f99ba1b509	
Hash	b65b7ede835ebba36294d52d7780065523340ee09bb8b209ef2dc495e53dfd53	
Hash	d252ee7b348b7e43e432d8fb154465838f5cd5fb564905323460e6f0a0c7d1e2	
Hash	dbbb8a11a239da11cbaf99f847a2d032f34d3b522e13b0fd4ef7b2649da7123b	
Hash	ec7e9ab43a0cc65d29f0b84a93ba88c43d01fed3dec5c968525dc73c03cbfda2	
Hash	ff662b60f6a142f99292fbdd65dd1ccd79dc9628686ddf5935c92f7fb1b62a81	

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 actor could pivot to creating a new local or domain account (T1136) to maintain persistence and privilege escalation capabilities, as this technique would allow them to establish a more stable and less detectable foothold within the network, potentially leveraging the same initial access vector that led to the web shell deployment. This approach may enable the actor to blend in with legitimate administrative activities, making it more challenging for defenders to identify malicious behavior. To counter this potential move, the mandated defensive control of alerting on new local/domain account creation (Event ID 4720/4728) and enforcing an approval workflow for account provisioning should be implemented.

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