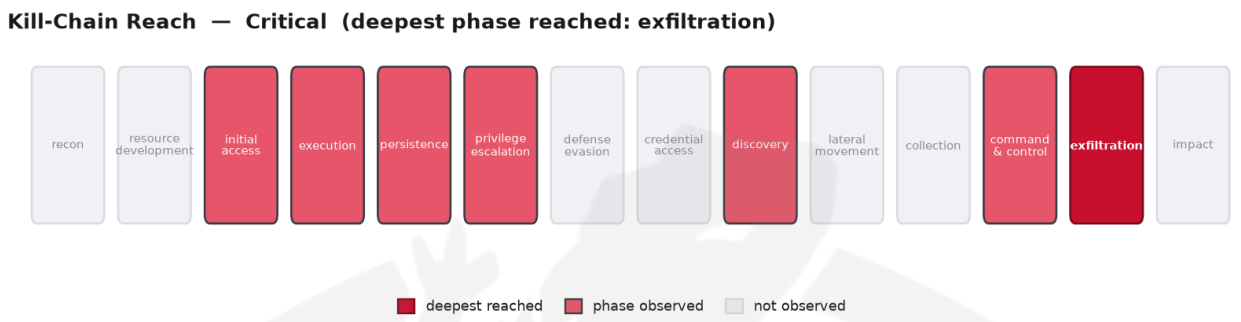
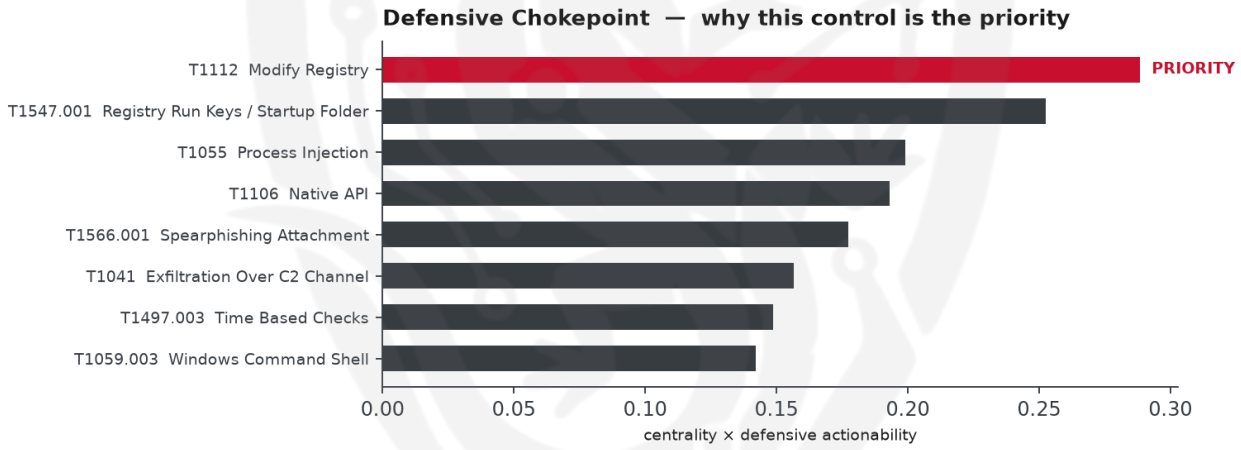
THREAT REPORT: MUSTANG PANDA

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 MUSTANG PANDA, a threat actor targeting India's government and energy sectors with various malware families, including SHARDLOADER, MINIRECON, and ZOHOMURK. The actor's campaign prioritizes the exploitation of system vulnerabilities to gain access to sensitive information. Priority should be given to monitoring sensitive registry keys for modification to prevent further damage. The targeted sectors are at high risk due to the potential for exfiltration of sensitive data.

Threat Overview

MUSTANG PANDA, the attributed threat actor, utilizes a range of malware families, including SHARDLOADER, MINIRECON, ZOHOMURK, TONESHELL, PUBLOAD, ShadowPad, and POISONPLUG.SHADOW, to target government and energy sectors in the British Indian Ocean Territory

and India. The central vulnerability exploited is currently unknown, but the actor's techniques involve various system discovery, spearphishing, and process injection methods.

Attack Chain and Priority Control

The observed techniques employed by MUSTANG PANDA form a complex attack chain, involving system owner/user discovery, scheduled tasks, and native API usage, ultimately leading to data exfiltration. The priority technique identified is T1112 Modify Registry, which serves as a critical chokepoint in the attack chain. To mitigate this, the recommended priority control is to "Monitor sensitive registry keys for modification; restrict registry-edit tools for unprivileged users."

Infrastructure and Corroboration

Although no specific hosting providers or ASNs have been directly linked to this campaign, third-party sources such as abuse.ch have corroborated the involvement of malware families like MustangPanda and Zebrocy. However, according to AbuseIPDB, there are currently no indicators with a confidence level of 80% or higher, suggesting that the infrastructure used by MUSTANG PANDA may not be widely recognized as malicious at this time.

Technical Appendix

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

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

- T1053.005 Scheduled Task
- T1033 System Owner/User Discovery
- T1036.005 Match Legitimate Resource Name or Location
- T1566.001 Spearphishing Attachment
- T1082 System Information Discovery
- T1106 Native API
- T1140 Deobfuscate/Decode Files or Information
- T1055 Process Injection
- T1497.003 Time Based Checks
- T1112 Modify Registry
- T1016 System Network Configuration Discovery
- T1083 File and Directory Discovery
- T1041 Exfiltration Over C2 Channel
- T1547.001 Registry Run Keys / Startup Folder
- T1027 Obfuscated Files or Information
- T1567.002 Exfiltration to Cloud Storage
- T1059.003 Windows Command Shell
- T1071.001 Web Protocols
- T1574.002 Hijack Execution Flow

- T1105 Ingress Tool Transfer

Analytical Scores

- Priority technique (graph chokepoint): T1112 Modify Registry (centrality 0.3037).
- Operational risk: Critical (score 0.968, reaches exfiltration).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.541; 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
Higaisa	0.541
APT37	0.5173
Tropic Trooper	0.5143
Confucius	0.5092
LuminousMoth	0.5048

Enrichment Signal

- Highest AbuseIPDB confidence among IOCs: 0%.
- Malware families corroborated by abuse.ch: MustangPanda, Zebrocy, Zedhou.
- 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	couldinstallup[.]com	Zebrocy
Domain	www[.]zohoapis[.]com	
URL	hxxp://www[.]zohoapis[.]com/workdrive/api/v1/files	
Hash	c04c947efdfdd9ce24617903b6746a83	

Type	Indicator	Context
Hash	43d646eda4166261eb1433c7599bf5cc9129a4f1	
Hash	fcf4efa82d477c924d42cc6b71aa672ab2381ca256769925ae34dabe2e77e025	
Hash	390148f5157c0f6b337ff19d162c3c2ee3e6d782fdfbe11fb1e411c0684fd33b	
Hash	f53fd0626404a129dcddb8ee7589387dd7bda7999814e0df46c670af6b3da5f5	
Hash	8aeba3c711eaa0116807c66390284dfa572d2cc7	
Hash	b267acd1b7c15b18178ae9fd4974f3f4	
Hash	7e7b30071565773d480578537ee3b0e6	MustangPanda
Hash	bca1e295acaacbb19c7e3a7868746f6b772b7b71	MustangPanda
Hash	5f22ec5c14dfd47c92850a5fb3bd8e3754d538b8021b6238238e4020336cfb5c	Zedhou
Hash	a43084f5af861f44c75c5273c779cb26d506cab6b51c33746626da504148a4ec	Zedhou
Hash	cd9397797216fd4c08df324937509124e57258328c8e4c6d795c6a2cd25b69b0	
Hash	ebd533de7ca16daa70093b0b1084fb6136b6ba091d6ee0e4199762581e1b2e5a	MustangPanda
Hash	f2bed071676feb831ed460489643fd57f6c6c1e0d024a1ea447820276fb13828	Zedhou

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