Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ACTOR REPORT

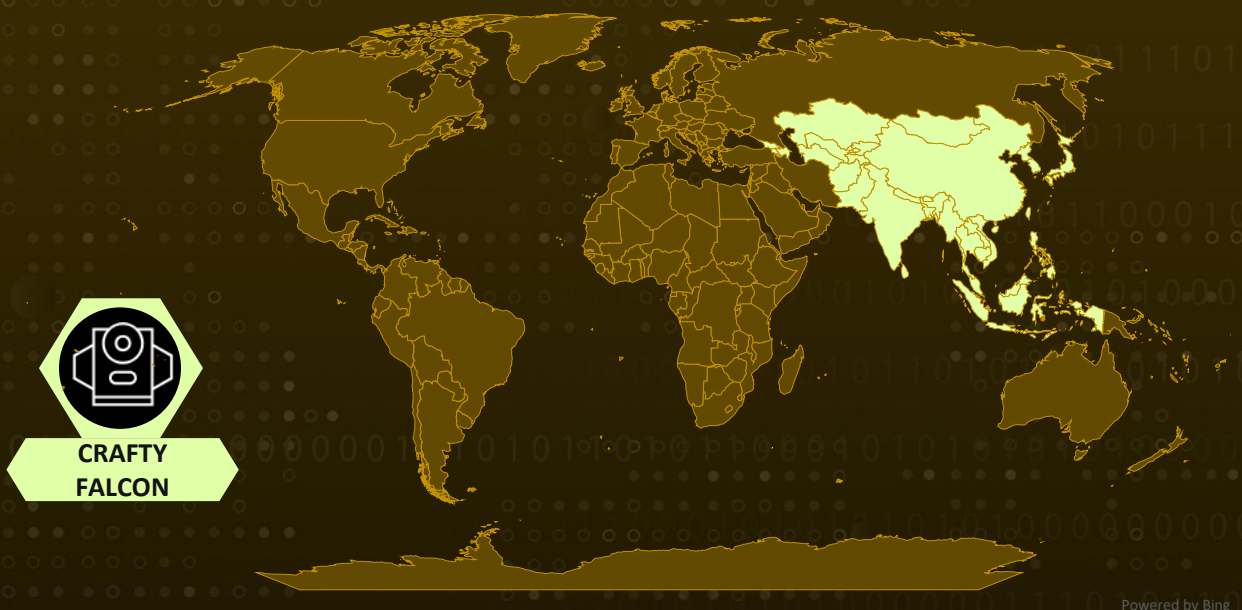
CRAFTY FALCON Weaponizes AI Against Financial Firms

Date of Publication	Admiralty Code	TA Number
November 10, 2026	A1	TA2026329

Summary

First Seen: October 9, 2026
Targeted Regions: Asia
Targeted Platforms: Cloud (AWS), Web Applications
Targeted Products: AWS Systems Manager, AWS Lambda, PHP applications, Node.js applications, Payment and Disbursement APIs, Merchant Settlement APIs, Cryptocurrency Wallets
Targeted Industries: Banking, Financial Services, Cryptocurrency, and Insurance
Threat Actor: CRAFTY FALCON
Malware: ARTEX, PentAGI, Cairn, CyberStrikeAI

Actor Map



Actor Details

#1 CRAFTY FALCON is a financially motivated threat actor that uses artificial intelligence to attack financial organizations in India at machine speed. Its targets include non-banking financial companies, digital lenders, fintechs, payment aggregators, and cryptocurrency exchanges. No country of origin or aliases have been attributed to the actor.

#2 The actor's edge comes from publicly available AI-driven offensive tools. ARTEX is a family of tools built on large language models, PentAGI is an autonomous multi-agent penetration testing system, Cairn is an attack search engine, and CyberStrikeAI is an offensive framework. Together, they let the actor run entire attack chains with little human effort, write and refine custom scripts on the fly, and adapt payloads to how each target responds.

#3 Initial access usually comes through internet-exposed testing and staging environments, or through newly disclosed flaws in PHP and Node.js applications that the actor exploits almost as soon as they go public. Once inside, it plants web shells and abuses AWS Systems Manager and Lambda to run commands, blending in with normal admin activity.

#4 From there, the actor moves into live production systems using shared credentials and tokens. It also tampers with client apps to send unauthorized API calls and routes traffic through trusted third-party services to slip past IP allow-lists.

#5 To cash out, the actor first sends test payments as small as Rs. 1 to confirm a payment route works, then follows with much larger unauthorized transfers. It also abuses merchant settlement systems and steals cryptocurrency wallet keys to drain funds.

#6 The actor strikes during weekends and holidays, rotates its infrastructure within hours to days, and has returned to organizations that did not fully clean up after earlier attacks. Successful fraudulent transfers have already been confirmed, although total losses have not been disclosed.

Actor Group

NAME	ORIGIN	TARGET COUNTRIES	TARGET INDUSTRY
CRAFTY FALCON	Unattributed **MOTIVE** Financial Gain	Asia	Banking, Financial Services, Cryptocurrency, and Insurance

Recommendations

Keep Watch Around the Clock, Especially on Weekends and Holidays: This actor strikes when teams are off duty. Make sure security monitoring runs 24x7, add extra coverage during holidays and weekends, and treat unusual activity during these periods with higher urgency.

Lock Down Cloud Admin Tools and Watch Them Closely: Only approved accounts should be able to run remote commands or change serverless functions, such as AWS Systems Manager and Lambda. Give every account the minimum access it needs, block internet access from these functions by default, and alert immediately when new users, roles, or access keys appear.

Keep Test Systems Completely Separate from Live Systems: Testing, staging, and UAT environments must never share passwords, tokens, or network connections with production. Remove unnecessary internet exposure from test systems and alert on any attempt to reach production from them.

Patch Fast and Protect Web Applications: Apply security updates for internet-facing applications as quickly as possible, especially PHP and Node.js systems. Where patching takes time, use a web application firewall as a temporary shield, and set web folders to read-only so attackers cannot easily drop malicious files.

Verify Every Payment Request and Spot "Test" Transactions: Never trust the app alone. Check every transaction on the server side, and replace IP-based trust with stronger checks such as signed requests or mutual authentication. Flag tiny Rs. 1 style transfers to new beneficiaries that are followed by larger ones, and add cooling periods and dual approval for new beneficiaries and settlements.

Protect Passwords, Keys, and Crypto Wallets: Remove passwords and keys hidden in code, use short-lived access tokens, and rotate credentials regularly. Store cryptocurrency wallet keys in secure hardware or offline storage and require multiple approvals for withdrawals.

Control AI Tool Usage and Respond Decisively to Incidents: Block unauthorized offensive AI tools on company systems and monitor how AI services and API keys are used. If an incident occurs, isolate affected systems, preserve logs, reset all credentials, and assume the attacker may still be present until cleanup is fully verified.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Reconnaissance	T1595: Active Scanning	T1595.002: Vulnerability Scanning
Resource Development	T1588: Obtain Capabilities	T1588.002: Tool
		T1588.007: Artificial Intelligence
Initial Access	T1190: Exploit Public-Facing Application	
	T1078: Valid Accounts	T1078.004: Cloud Accounts

Tactic	Technique	Sub-technique
Execution	T1651: Cloud Administration Command	
	T1648: Serverless Execution	
Execution	T1059: Command and Scripting Interpreter	
Persistence	T1505: Server Software Component	T1505.003: Web Shell
Credential Access	T1552: Unsecured Credentials	T1552.001: Credentials In Files
		T1552.004: Private Keys
Lateral Movement	T1550: Use Alternate Authentication Material	T1550.001: Application Access Token
Command and Control	T1071: Application Layer Protocol	T1071.001: Web Protocols
	T1090: Proxy	T1090.002: External Proxy
Exfiltration	T1041: Exfiltration Over C2 Channel	
Impact	T1657: Financial Theft	

References

https://www.businesstoday.in/technology/news/story/ai-hackers-use-rs1-test-transactions-to-move-bigger-sums-from-financial-firms-cert-in-warns-565805-2026-11-05

https://www.cert-in.org.in/s2cMainServlet?pageid=PUBVLNOTES02&VLCODE=CIAD-2026-0058

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a Demo of **HivePro**.

REPORT GENERATED ON

November 10, 2026 • 12:30 AM

© 2026 All Rights are Reserved by Hive Pro

More at www.hivepro.com