Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

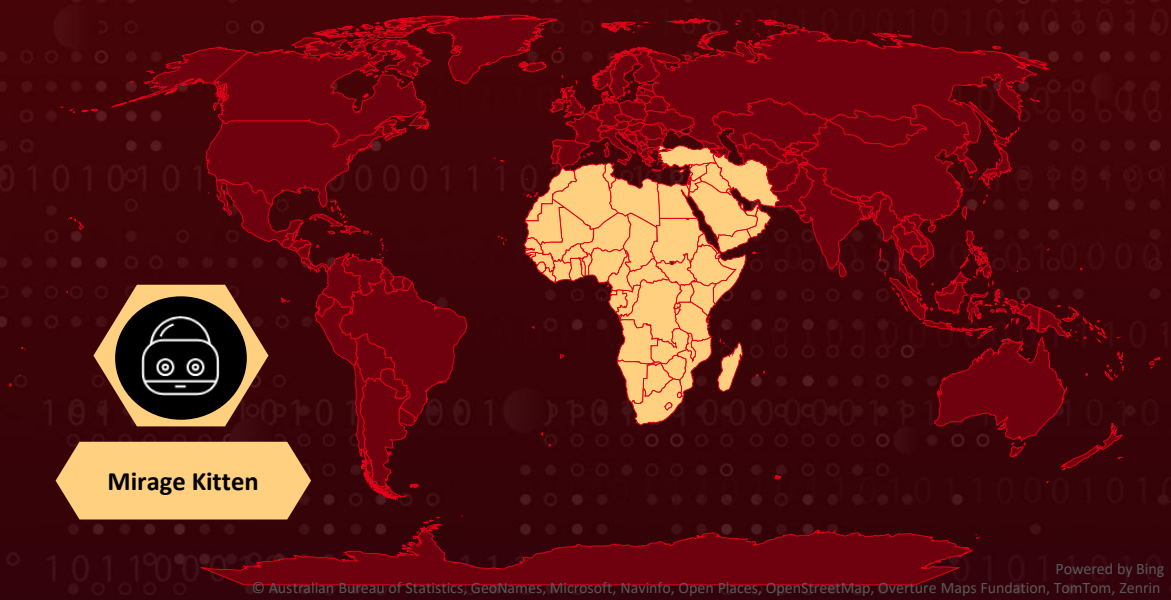
Mirage Kitten Turns Job Interviews into a Gateway for Corporate Espionage

Date of Publication	Admiralty Code	TA Number
September 04, 2026	A1	TA2026256

Summary

First Seen: May 2026
Targeted Regions: Middle East and Africa
Targeted Platforms: Windows, Linux, macOS
Targeted Industries: Aviation, Aerospace, Financial Technology (FinTech)
Threat Actor: Mirage Kitten (aka UNC1549, Smoke Sandstorm, Nimbus Manticore, GalaxyGato, Subtle Snail)
Malware: NodeRabbit, PollCat, Retrograde/MiniFast
Attack: Mirage Kitten (aka Nimbus Manticore), an Iran-linked cyberespionage group active since at least 2022, is targeting aviation, aerospace, and FinTech specialists across the Middle East and Africa with recruitment-themed social engineering. Fake recruiters on LinkedIn and other job-search platforms deliver trojanized coding-challenge archives hosted on an Amazon S3 bucket that bundle malicious npm packages. Running the project executes the group's first Node.js- and JavaScript-based cross-platform remote access trojans, NodeRabbit and PollCat, granting remote access, host reconnaissance, credential and artifact harvesting, and file exfiltration across Windows, Linux, and macOS, with command-and-control concealed behind Microsoft Azure Websites and Cloudflare-backed domains.

Attack Regions



Targeted Non-Targeted

Attack Details

#1

Mirage Kitten, an Iran-linked cyberespionage group (also tracked as Nimbus Manticore, UNC1549, Smoke Sandstorm, and Iranian Dream Job), is targeting aviation, aerospace, and FinTech specialists across the Middle East and Africa, with confirmed victims in Egypt, Ethiopia, and Afghanistan. The operation opens with fake recruiter personas on LinkedIn and other job platforms: posing as a talent acquisition specialist at a major technology company, the actor invites a software engineer to complete a "technical assessment" and pressures them to download and run a coding-challenge archive hosted on an Amazon S3 bucket.

#2

The lure is engineered for both stealth and urgency. One archive, Front-Technical-Challenge.zip, held a TaskFlow app whose README demanded frontend fixes within three hours, banned AI assistants (which would have flagged the malicious import), and falsely declared server.js off-limits, the one file the attackers had altered. Its first line loaded a trojanized npm package (colorized_terminal or pretty-log, v2.1.0) bundled locally, which silently launched the implant as a detached background process.

#3

That implant is NodeRabbit, the group's first Node.js remote access trojan, running on Windows, Linux, and macOS. It fingerprints the host, guards against re-execution, and persists per OS while masquerading as Microsoft Edge Update or Intel Driver & Support Assistant. Across three variants it adds sandbox evasion, corporate-proxy tunneling, Outlook email harvesting, a fake "GitHub Copilot Helper" VS Code extension, and Git-hook injection, growing to 23 commands.

#4

A parallel lure (RankChallenge-react) delivered PollCat, an obfuscated-JavaScript RAT gated behind an attacker-supplied, rapidly expiring six-digit OTP to force speed. PollCat runs regardless of OTP success, registers with its C2, and profiles the host, inventorying processes and hunting for 24 security-vendor directories. Both RATs beacon over HTTP(S) to Microsoft Azure Websites and Cloudflare-backed domains, sometimes embedding the victim's own name in the subdomain to blend in; NodeRabbit encrypts traffic with AES-256-GCM. Attribution to Mirage Kitten is high-confidence, resting on strong structural overlaps with its earlier Retrograde/MiniFast backdoor.

Recommendations

Contain Recruiter-Supplied Coding Assessments: Treat any coding challenge received through LinkedIn or a job platform as untrusted code and never run it on a production, domain-joined, or credential-bearing workstation. Require that such archives be opened only inside isolated, network-restricted virtual machines or containers, and instruct developers to ignore lures that impose artificial urgency (three-hour limits, expiring six-digit OTP codes) or explicitly forbid AI code review, since both are engineered to suppress the checks that would expose the trojanized import.

Block and Hunt for the Known Indicators: Ingest the Mirage Kitten hashes, C2 domains, URLs, filenames, and the MicrosoftEdgeUpdate Run-key indicator from this advisory into EDR, SIEM, and firewall tooling, and alert on any outbound connection to the listed Azure Websites and Cloudflare-backed domains, including subdomains that embed your own organization's name. Treat the Retrograde/MiniFast reference hash (810F8E3B88EB05F710C09552941D6F56) as an attribution comparator rather than a live campaign delivery hash, and hunt proactively since the group rotates infrastructure frequently.

Audit npm Dependencies and Anomalous Node Execution: Sweep developer endpoints for the trojanized packages colorized_terminal and pretty-log pinned to version 2.1.0, and for any package loaded from a project-local node_modules directory that was never installed from the public registry — with particular attention to payloads under node_modules/.cache/.320697f1/. Alert on node.exe copies renamed to nodew.exe or IntelDSA.exe running with a Windows GUI subsystem, and on Node processes spawning from %APPDATA%, %LOCALAPPDATA%, or user configuration directories.

Hunt Persistence Across Windows, Linux, and macOS: Because these RATs are cross-platform, search every operating system, not just Windows. Look for the MicrosoftEdgeUpdate Run key; scheduled tasks named IntelDriverSupportUpdate and NetSync_<username>; WSL-launched daily 10 AM tasks invoking wscript.exe/wsl.exe; @reboot and daily cron entries; and macOS LaunchAgents such as com.microsoft.edgeupdate.plist. Inspect VS Code for a fake "GitHub Copilot Helper" extension and review .git/hooks/post-merge and post-checkout for the injected marker # shepherd-persist.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Resource Development	T1585: Establish Accounts	T1585.001: Social Media Accounts
	T1583: Acquire Infrastructure	T1583.001: Domains
		T1583.006: Web Services
	T1608: Stage Capabilities	T1608.001: Upload Malware
Initial Access	T1566: Phishing	T1566.003: Spearphishing via Service
Execution	T1204: User Execution	T1204.002: Malicious File
	T1059: Command and Scripting Interpreter	T1059.007: JavaScript
		T1059.003: Windows Command Shell
Persistence	T1547: Boot or Logon Autostart Execution	T1547.001: Registry Run Keys / Startup Folder
	T1053: Scheduled Task/Job	T1053.005: Scheduled Task
		T1053.003: Cron
	T1543: Create or Modify System Process	T1543.001: Launch Agent
	T1176: Software Extensions	T1176.002: IDE Extensions
	T1546: Event Triggered Execution	
Privilege Escalation	T1053: Scheduled Task/Job	T1053.005: Scheduled Task
Defense Evasion	T1036: Masquerading	T1036.004: Masquerade Task or Service

Tactic	Technique	Sub-technique
Defense Evasion	T1036: Masquerading	T1036.005: Match Legitimate Name or Location
	T1497: Virtualization/Sandbox Evasion	T1497.001: System Checks
	T1027: Obfuscated Files or Information	
	T1140: Deobfuscate/Decode Files or Information	
	T1070: Indicator Removal	T1070.004: File Deletion
	T1564: Hide Artifacts	T1564.003: Hidden Window
Discovery	T1082: System Information Discovery	
	T1057: Process Discovery	
	T1083: File and Directory Discovery	
	T1016: System Network Configuration Discovery	
	T1518: Software Discovery	T1518.001: Security Software Discovery
Collection	T1114: Email Collection	T1114.001: Local Email Collection
	T1005: Data from Local System	
	T1560: Archive Collected Data	T1560.001: Archive via Utility
Command and Control	T1071: Application Layer Protocol	T1071.001: Web Protocols
	T1573: Encrypted Channel	T1573.001: Symmetric Cryptography
	T1102: Web Service	
	T1008: Fallback Channels	
	T1105: Ingress Tool Transfer	
Exfiltration	T1041: Exfiltration Over C2 Channel	
	T1030: Data Transfer Size Limits	

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	CBAAF0900A13F28E380F49ADECEC932C, 1EA83E4E4592B01E4ACAB63EB867BEE5, 366515822D5AC1CC500711EF57A2E32E, CF449F1992C2819E62AC44A0B06AC2E7, E95A4366686E3F786EA3C056FAB5B0DA, DE5AF16A3757EF700B01DC34D67079AE, BE086789568441D0D7E4679AEE51F566, E259C5EDF158AAC4CFE14F77DDD0B196, 291AC3ABE73C5158E59A437B75D5F0AA, 0962F56D7EC69F4F2A0162DCBE22116B, 795E053A990A1569FFDCB57F48F6D085, 810F8E3B88EB05F710C09552941D6F56
Domains	oracle-challenge[.]s3[.]us-east-1[.]amazonaws[.]com, naturalapplication[.]azurewebsites[.]net, retaildemo[.]azurewebsites[.]net, tubitak[.]azurewebsites[.]net, rgbteller[.]azurewebsites[.]net, wslwebui[.]azurewebsites[.]net, plugplay[.]azurewebsites[.]net, crossdwm[.]azurewebsites[.]net, wdisystem[.]azurewebsites[.]net, wslmenus[.]azurewebsites[.]net, dnshnsdev[.]azurewebsites[.]net, hpjumpsrv[.]azurewebsites[.]net, storview[.]azurewebsites[.]net, healthcomfsdpower[.]com, visitfinancedentists[.]com, kyrasey-f8hfexa5cqamh7fk[.]westeurope-01[.]azurewebsites[.]net, greenyjsgfd[.]azurewebsites[.]net, helptellerbls[.]azurewebsites[.]net, timedrv[.]azurewebsites[.]net, userwellgtfs[.]azurewebsites[.]net, hecowime-aqdphyd4bbdef6es[.]westeurope-01[.]azurewebsites[.]net, msmanagementgrp[.]com, msmanagementgrpmedia[.]com, lifespotify[.]com, gamebarapp[.]azurewebsites[.]net, gamebarappinformation[.]azurewebsites[.]net, sahi-finance[.]com, healthful-hub[.]com,

TYPE	VALUE
Domains	neumedicahealthcare[.]com, optimumhealthcredit[.]com, healthfullyrecipes[.]com, refreshhealthandwellness[.]com, healthvitalitycare[.]com, aceofspadesmanagement[.]com, glmediaagency[.]com, digimediaskill[.]com, healthyweightplan[.]com, mens-health-online[.]com
URLs	hxxps[:]//oracle-challenge[.]s3[.]us-east-1[.]amazonaws[.]com/Front-Technical-Challenge[.]zip, hxxps[:]//lifespotify[.]com/api/users/b879746e-fed9-4211-a6da-4d8223681267/otp/validate
Filenames	FrontEnd-Task.zip, Front-Technical-Challenge.zip, Task-FullStack.zip, fullstack-1536.zip, webapp76592.zip, webapp76531.zip, challenges-17831.zip, challenges-17832.zip, Project-1802.zip, Case-34234.zip, RankChallenge-react-6uJSX3-main.zip, colorized_terminal, pretty-log, msedge_update.js, nodew.exe, idriver_support.js, IntelDSA.exe, requireObject.js, launcher.vbs
Registry Key	HKCU\Software\Microsoft\Windows\CurrentVersion\Run\MicrosoftEdgeUpdate

References

https://securelist.com/mirage-kitten-new-backdoors-noderabbit-pollcat/121244/

https://www.hivepro.com/threat-advisory/mirage-kitten-marks-new-territory-across-the-middle-east-and-africa

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

September 04, 2026 • 01:48 AM

More at www.hivepro.com