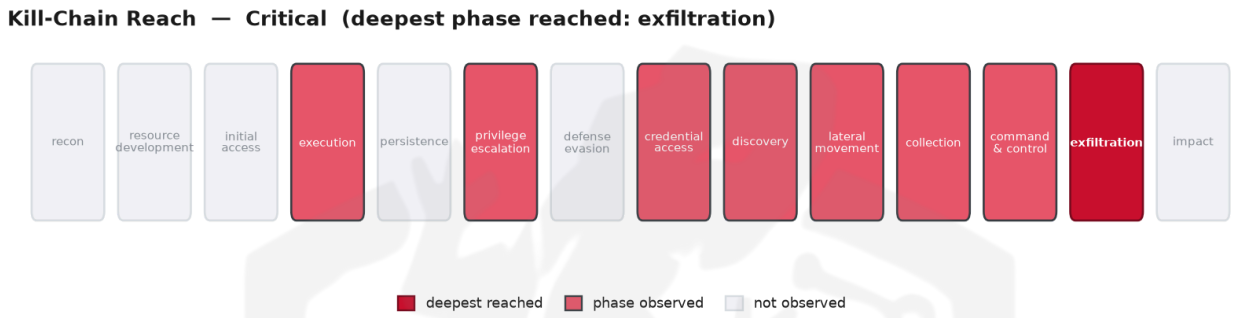
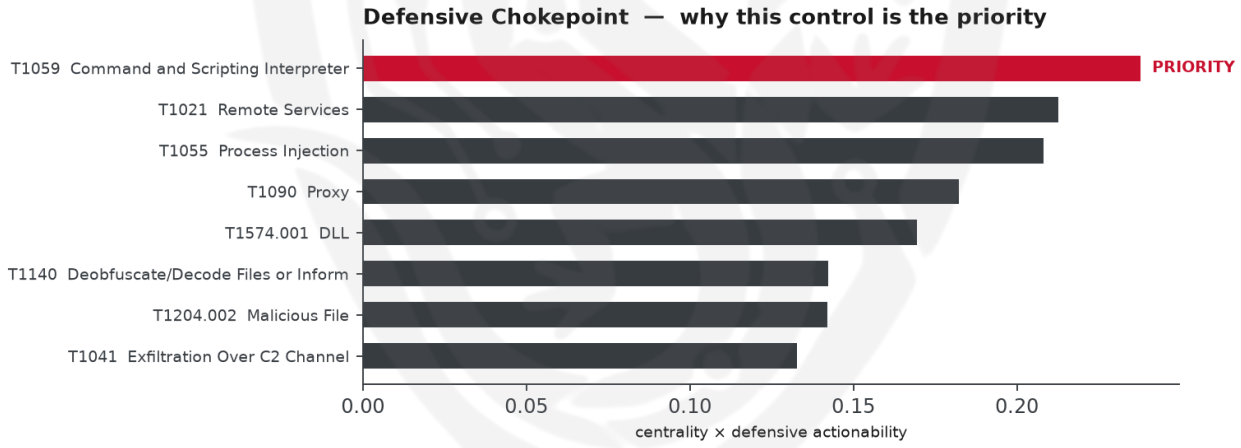
THREAT REPORT: MIRAGE KITTEN'S NIGHTLEDGER BACKDOOR CAMPAIGN

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 Mirage Kitten, a threat actor that has been observed deploying the NightLedger backdoor in an espionage campaign targeting the Middle East and Africa. The campaign has affected several countries, including Egypt, Jordan, and Tanzania, and has targeted various sectors such as aerospace, defense, and government. Priority should be given to constraining PowerShell for unprivileged users to mitigate the threat. The actor's use of multiple malware families, including NightLedger, BridgeHead, and ArcBridge, has allowed them to maintain a persistent presence in compromised networks.

Threat Overview

Mirage Kitten, the attributed threat actor, has been using a range of malware families, including NightLedger, BridgeHead, ArcBridge, and TWOSTROKE, to target organizations in the Middle East and Africa. The central vulnerability exploited in the campaign is currently unknown, but the actor has been observed using various techniques to gain and maintain access to compromised systems. The victimology of the campaign suggests that the actor is interested in gathering sensitive information from a range of sectors, including aerospace, defense, and government.

Attack Chain and Priority Control

The observed techniques used by Mirage Kitten can be described as a chain of events, starting with initial access and ending with exfiltration of sensitive data. The priority technique in this chain is T1059 Command and Scripting Interpreter, which is used to execute malicious scripts and maintain persistence in compromised systems. To mitigate this threat, the recommended priority control is to "Constrain PowerShell for unprivileged users (Constrained Language Mode + AppLocker); enable script-block logging; block wscript/cscript where unneeded."

Infrastructure and Corroboration

There is currently no available information on the hosting providers or ASNs used by Mirage Kitten, and no malware families have been corroborated by abuse.ch. Additionally, no indicators have been flagged with a confidence level of 80% or higher by 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
- T1033 System Owner/User Discovery
- T1056.001 Keylogging
- T1204.002 Malicious File
- T1574.001 DLL
- T1082 System Information Discovery
- T1005 Data from Local System
- T1140 Deobfuscate/Decode Files or Information
- T1055 Process Injection
- T1021 Remote Services
- T1090 Proxy
- T1059 Command and Scripting Interpreter
- T1083 File and Directory Discovery
- T1057 Process Discovery
- T1041 Exfiltration Over C2 Channel
- T1027 Obfuscated Files or Information

- T1573 Encrypted Channel
- T1071.001 Web Protocols
- T1105 Ingress Tool Transfer
- T1090.001 Internal Proxy

Analytical Scores

- Priority technique (graph chokepoint): T1059 Command and Scripting Interpreter (centrality 0.2973).
- Operational risk: Critical (score 0.968, reaches exfiltration).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.4782; 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	0.4782
Tropic Trooper	0.4364
APT39	0.433
Stealth Falcon	0.4215
Dark Caracal	0.4215

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
Hash	a239e655709a2518dd0b7bdbed163679
Hash	79f3ef6c6127edb0a5f43ef7a16bfb3418860e19
Hash	24771d0a69e442b9493ab1406e0253be1acd31d83f593177fd736f7f6d629ed9

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:** T1059 Command and Scripting Interpreter (execution)
- **Observed here:** T1059 Command and Scripting Interpreter was the only execution technique observed in this campaign, so the pivot is projected from cross-actor behaviour.
- **Projected pivot:** T1053 Scheduled Task/Job (execution)
- **Basis:** of the 54+ groups that use Command and Scripting Interpreter, this pairing runs 1.3x above base rate, a disproportionately-coupled move rather than the obvious one.

Mirage Kitten could pivot to utilizing T1053 Scheduled Task/Job to maintain persistence and execute malicious commands at scheduled intervals, potentially leveraging the Windows Task Scheduler to blend in with legitimate system activity, which may allow them to bypass initial detection. This technique in particular may be appealing as it enables the adversary to execute tasks under the context of a legitimate system process, which would likely make it more challenging to distinguish from authorized activity. To counter this potential move, the defensive control would be to alert on new scheduled tasks (Event ID 4698), restrict schtasks/at to admins, and baseline legitimate task creators.

Also plausible (same tactic): T1047 Windows Management Instrumentation (n=40, lift 1.3), T1106 Native API (n=19, lift 1.3)

Detection and hardening for the pivot (T1053 Scheduled Task/Job)

- **Telemetry:** Windows Security (Object Access audit); Microsoft-Windows-TaskScheduler/Operational; Sysmon
- **Detect:**
  - Security 4698 (task created), 4702 (updated), 4700/4701 (enabled/disabled), 4699 (deleted)
  - TaskScheduler/Operational 106 (registered), 140 (updated), 141 (deleted)
  - Sysmon 1 for schtasks.exe and at.exe; Sysmon 11 for writes under C:\Windows\System32\Tasks\
- **Harden:**
  - Restrict schtasks/at to administrators; disable the legacy at.exe
  - Baseline the legitimate task creators and alert on anything outside it
- **MITRE:** M1047 Audit, M1028 Operating System Configuration, M1026 Privileged Account Management · DS0003 Scheduled Job, DS0009 Process, DS0022 File