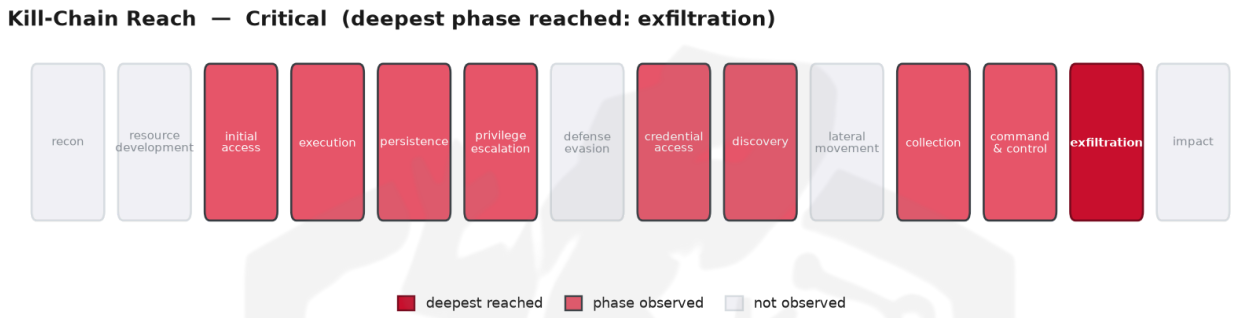
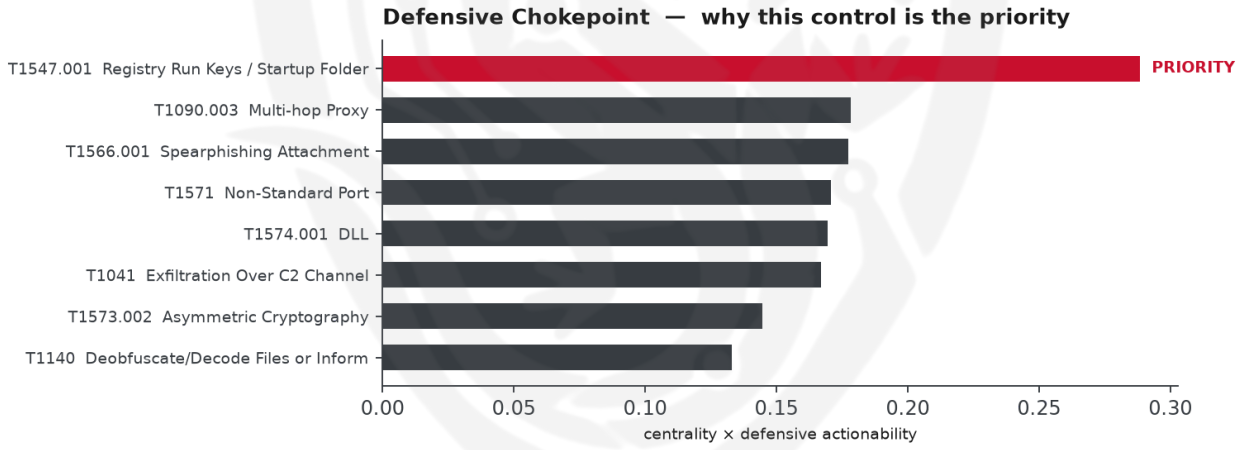
THREAT REPORT: MIRAGE KITTEN TARGETS MIDDLE EAST AND AFRICA

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 targeting the Middle East and Africa region with a range of malware families, including NightLedger, BridgeHead, and others. The targeted sectors include Aerospace, Defense, Telecommunications, Government, and Finance in countries such as Burkina Faso, Egypt, and Pakistan. Priority should be given to auditing Windows Startup folders and Run/RunOnce registry keys for unauthorized entries to mitigate the threat. The actor's use of various techniques, including screen capture and keylogging, poses a significant risk to the targeted organizations.

Threat Overview

Mirage Kitten, the attributed threat actor, utilizes multiple malware families to target organizations in the Middle East and Africa. The malware families involved include NightLedger, BridgeHead, ArcBridge, TWOSTROKE, Retrograde, MiniFast, MiniUpdate, LIGHTRAIL, and POLLBLEND. The targeted countries include Burkina Faso, Egypt, Ethiopia, Jordan, Pakistan, Tanzania, and the United Republic of others, with a focus on the Aerospace, Defense, Telecommunications, Government, and Finance sectors.

Attack Chain and Priority Control

The observed techniques used by Mirage Kitten form a complex attack chain, involving techniques such as screen capture, keylogging, and spearphishing. The priority technique identified is T1547.001 Registry Run Keys / Startup Folder, which serves as a critical chokepoint in the attack chain. To mitigate this threat, the priority control is to "Audit Windows Startup folders and Run/RunOnce registry keys for unauthorized entries; alert on .lnk or script creation in Startup by browser/email temp paths."

Infrastructure and Corroboration

There is no available information on the hosting providers or ASNs observed in this campaign. Additionally, no malware families have been corroborated by abuse.ch, and 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
- T1056.001 Keylogging
- T1204.002 Malicious File
- T1566.001 Spearphishing Attachment
- T1574.001 DLL
- T1082 System Information Discovery
- T1140 Deobfuscate/Decode Files or Information
- T1083 File and Directory Discovery
- T1057 Process Discovery
- T1041 Exfiltration Over C2 Channel
- T1547.001 Registry Run Keys / Startup Folder
- T1090.003 Multi-hop Proxy
- T1571 Non-Standard Port
- T1027 Obfuscated Files or Information
- T1573.002 Asymmetric Cryptography
- T1095 Non-Application Layer Protocol
- T1070.004 File Deletion

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

Analytical Scores

- Priority technique (graph chokepoint): T1547.001 Registry Run Keys / Startup Folder (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 0.522; 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	0.522
Tropic Trooper	0.4963
Inception	0.4777
Darkhotel	0.4777
Windshift	0.4549

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
Domain	neexportfolio[.]com
Domain	buisness-centeral-transportation[.]com
Domain	healthcarezoomcenteral[.]org
Domain	tjconsultingservices[.]com

Type	Indicator
Domain	realhealthshop[.]com
Domain	aecert[.]org
Domain	businessmixture[.]com
Domain	global-reds[.]com
Domain	maadinglobal[.]com
Domain	thehealth-life[.]com
URL	hxxp://businessmixture[.]com/blog
Hash	42f847597109da2a220391bb09d00676
Hash	5fa15ef96808ea82f0a6176f0bb4b386
Hash	6038d42af0affd1fb263f470c0956f6b
Hash	a239e655709a2518dd0b7bdbed163679
Hash	ae628efa305387b633dce82f9364875b
Hash	afb1c1583606599c7272cfb33cc6f498
Hash	c832ecd135781b11f59e3fffb3d2b6ac
Hash	c90f0efadbf322e5eb1c4103a38c30e6
Hash	d09b14a2fe01c7363ecc56f5d046162c
Hash	f7d36cc5904a53252d2bb3d21615134f
Hash	6e85d21c17d68c7c7e3e10433a53486c5371c127
Hash	c4a9de21aad3e71b08bfbcc827d4c242f8915e763117d254e41febe6df4807cc

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:** T1547.001 Registry Run Keys / Startup Folder (persistence)
- **Observed here:** T1547.001 Registry Run Keys / Startup Folder was the only persistence technique observed in this campaign, so the pivot is projected from cross-actor behaviour.

- **Projected pivot:** T1053 Scheduled Task/Job (persistence)
- **Basis:** of the 37+ groups that use Registry Run Keys / Startup Folder, this pairing runs 1.9x 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, as this technique allows them to execute malicious code at a specified time or interval, potentially evading detection by blending in with legitimate system tasks. This technique may be particularly appealing to the adversary in this scenario, as it could enable them to re-establish a foothold in the system by scheduling a task that reinstates their malicious payload. To counter this potential move, the defensive control would involve alerting on new scheduled tasks (Event ID 4698), restricting schtasks/at to admins, and baselining legitimate task creators.

Also plausible (same tactic): T1543 Create or Modify System Process (n=18, lift 1.8), T1098 Account Manipulation (n=12, lift 2.0)

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