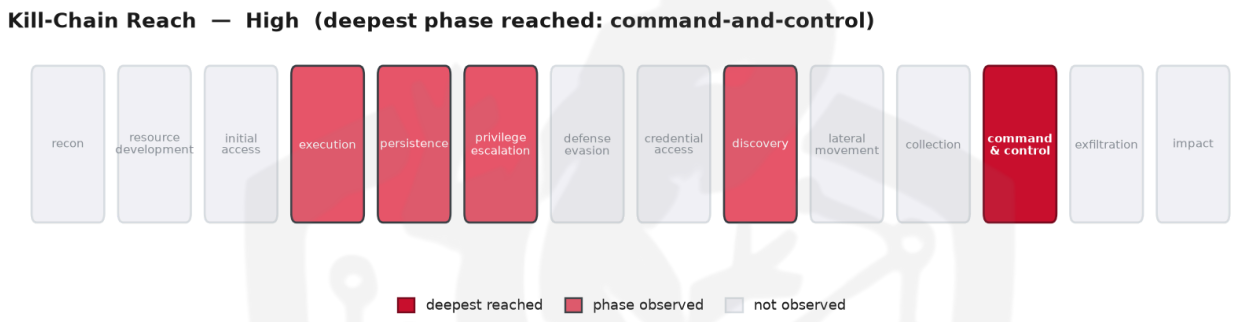
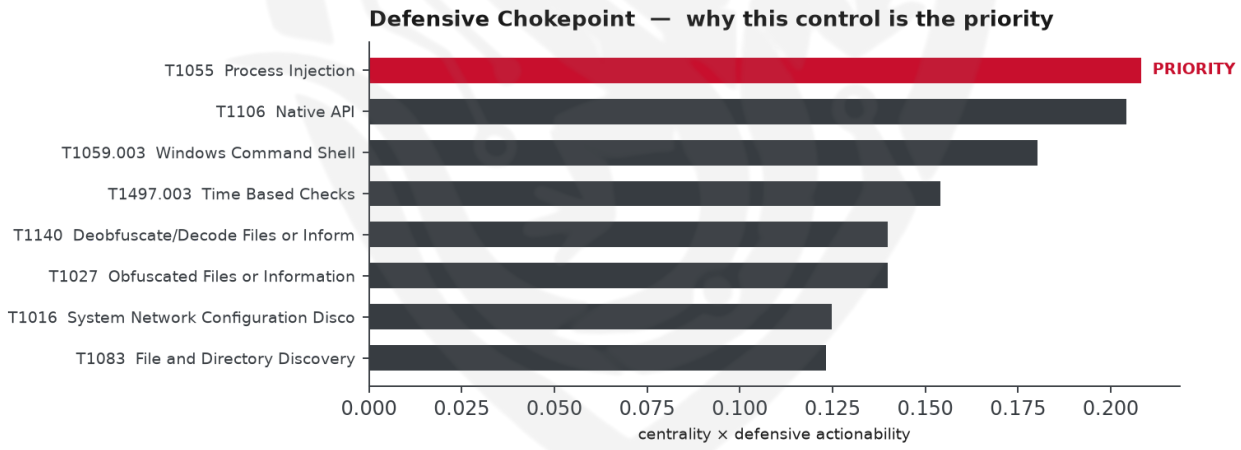
# THREAT REPORT: TARGETED ATTACK ON GOVERNMENT ENTITIES IN THE MIDDLE EAST | PART 1

## 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

This brief covers activity involving TELESHIM, MIXEDKEY, BINDCLOAK, with no single central CVE identified, affecting Government. The source does not attribute this activity to a named actor. The operational risk is assessed as High. Priority should be given to the control described below, centred on T1055 Process Injection.

## Threat Overview

The activity is associated with an as-yet unattributed cluster of activity. Malware observed: TELESHIM, MIXEDKEY, BINDCLOAK. Reported victimology: Government.

## Attack Chain and Priority Control

The source records the following techniques: - T1053.005 Scheduled Task - T1033 System Owner/User Discovery - T1132.001 Standard Encoding - T1497.001 System Checks - T1082 System Information Discovery - T1106 Native API - T1140 Deobfuscate/Decode Files or Information - T1055 Process Injection - T1497.003 Time Based Checks - T1016 System Network Configuration Discovery - T1083 File and Directory Discovery - T1049 System Network Connections Discovery - T1027 Obfuscated Files or Information - T1518.001 Security Software Discovery - T1059.003 Windows Command Shell - T1027.002 Software Packing - T1071.001 Web Protocols - T1574.002 Hijack Execution Flow - T1105 Ingress Tool Transfer

Priority should be given to T1055 Process Injection. Recommended control: Enable EDR detection of process injection (CreateRemoteThread, hollowing); alert on cross-process memory writes.

---

## 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
- T1132.001 Standard Encoding
- T1497.001 System Checks
- T1082 System Information Discovery
- T1106 Native API
- T1140 Deobfuscate/Decode Files or Information
- T1055 Process Injection
- T1497.003 Time Based Checks
- T1016 System Network Configuration Discovery
- T1083 File and Directory Discovery
- T1049 System Network Connections Discovery
- T1027 Obfuscated Files or Information
- T1518.001 Security Software Discovery
- T1059.003 Windows Command Shell
- T1027.002 Software Packing
- T1071.001 Web Protocols
- T1574.002 Hijack Execution Flow
- T1105 Ingress Tool Transfer

### Analytical Scores

- Priority technique (graph chokepoint): T1055 Process Injection (centrality 0.2974).
- Operational risk: High (score 0.636, reaches command-and-control).

## Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.5183; 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 |
|---|---|
| Tropic Trooper | 0.5183 |
| APT18 | 0.433 |
| Darkhotel | 0.4201 |
| APT38 | 0.4187 |
| Patchwork | 0.4115 |

## 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 | cert[.]hypersnet[.]com |
| Hash | 087499849115eb28c4364581d2b28d09 |
| Hash | 28b47bdf16d7af6f8ec21218eac9145a |
| Hash | 3f60d53a2b5737d77e058d9e33cbe9eb |
| Hash | 68926e6c958562deaae35de3d9f59de3 |
| Hash | 78a4f8574830bf7fbaf63d7da09be2b8 |
| Hash | 7a14a99d70d42d3f7bf72f843185fc07 |
| Hash | 7cbc51ada1a4aec88660ec32c408114b |
| Hash | 97124a93766be732e8fef5a56a5346a2 |

| Type | Indicator |
|---|---|
| Hash | b776eb638fbb535708fb92b12fcc1731 |
| Hash | c99f29ac08454855b3d538960bb2f34f |
| Hash | 1099bf51e53bd5fb32401edb4e0be841d8486b19 |
| Hash | 2377c47cfde148c2140faa7105628174f9c4d56d |
| Hash | 577b1cc894636f4ac5ad670b0079b9b7ade137c3 |
| Hash | 86ee99f293a30720bcc898a4a8e391f93fb9be95 |
| Hash | c1f16e31ae71372ee45fa6fd6927c7b887a4e3f2 |
| Hash | ccb2002fe8f5cc1f511d52309625b52d1c507421 |
| Hash | ee287d6a09295502ab2407aec336f9f0d8477d68 |
| Hash | f46c01a5be2e08e36d4ec3302a8650a6ed25ec14 |
| Hash | fee6806c96f87bf1e240a2eb6fd7e045101d58d3 |
| Hash | 0637069c7052118fd5c0f1113541bdd35e5f71cd9689f2516045da152c6fa8d9 |
| Hash | 32529043d15e9111ba284f1d8a9e4b3f58e071c6b69c8f271d4d02feacd44e66 |
| Hash | 3b0c658ebaa2bae80af97f390b9b2bb20a2f815eb584b2251255e84da4fa669d |
| Hash | 3b3eaea783fd6dab90f0408274bf8a9c49adbdc70c0efd70658d65b0e1684a3f |
| Hash | 5c2fe953da53da66fbcbb3be0fd6b63907c10714c337f287b2fc258857bbff6d |
| Hash | 789fd11285642861190dc074c1e9a5957073f1a2afebd5160f9cc907f7f320bd |
| Hash | c84542ac30cbe9bb8bd648bad323c37801023bf9451c1c0990452466e084340f |
| Hash | cac1f37beaa814461f7709a073aeec468c74e5d70f7d693a9e367ece4a3a78be |
| Hash | db11ff3f37a8b2aa25c480871504b886a6364167ecb501eacf7345f6bbf9582b |

## 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:** T1055 Process Injection (privilege-escalation)

- **Observed here:** the threat actor used T1053.005 Scheduled Task here as an alternative privilege-escalation technique.
- **Projected pivot:** T1053.005 Scheduled Task (privilege-escalation)
- **Basis:** observed in this campaign (an alternative the actor already demonstrated).

With T1055 Process Injection blocked, the threat actor could preserve the same objective by pivoting to T1053.005 Scheduled Task, a technique observed in this campaign. Defensive countermeasure: Alert on new scheduled tasks (Event ID 4698); restrict schtasks/at to admins; baseline legitimate task creators.

**Detection and hardening for the pivot (T1053.005 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