Iranian-linked group 'Volant Manticore' reported targeting Cypriot organizations



Dark Reading reports a previously undocumented Iranian threat group, Volant Manticore, is targeting Cypriot organizations in an intelligence-gathering effort for Tehran.

- The group is called Volant Manticore and was previously undocumented.
- It is described as Iranian and working to gather intelligence for Tehran.
- Its reported targets are organizations in Cyprus.
- The source excerpt gives no technical details, victims or indicators.

What was reported

Dark Reading reports that a previously undocumented Iranian threat group, tracked as "Volant Manticore", is

targeting organizations in Cyprus. The activity is described as part of an intelligence-gathering effort on behalf of Tehran, which points to espionage rather than disruption or financial gain.

The material available to us is brief. It does not name victims, sectors, attack techniques, tools or indicators of compromise, and we do not speculate beyond what the source states.

Why it matters for Saudi institutions

The report concerns Cyprus, not the Kingdom, and no Saudi targeting is mentioned. Still, a new state-linked group focused on intelligence collection is a useful prompt for regulated institutions in the region to check that their own detection and threat-intelligence processes can absorb new actor names quickly. Espionage campaigns tend to be quiet and long-running, so readiness depends on visibility rather than on reacting to alerts alone.

Recommended posture

There is no need for emergency measures on the basis of this report. A measured review is appropriate: confirm that threat-intelligence feeds will deliver indicators for Volant Manticore once they are published, and that your teams know how to act on them. Watch for fuller technical reporting from the original researchers and from national authorities before adjusting controls.

What to do now

1. Confirm your threat-intelligence sources will supply Volant Manticore indicators once published.
2. Check that new actor names and indicators can be loaded into SIEM and EDR detection quickly.
3. Review monitoring for long-running, low-noise intrusion activity on systems holding sensitive information.
4. Follow advisories from the National Cybersecurity Authority and the original researchers for technical detail.
5. Brief the security team that no Saudi targeting has been reported, so response stays proportionate.