Volant Manticore: Iran-Aligned Group Uses IPFS-Based KuboShell Backdoor



A newly documented Iran-aligned espionage group, Volant Manticore, has targeted telecoms, airlines and critical infrastructure in Cyprus using a backdoor called KuboShell that relies on IPFS for command and control.

- Volant Manticore is a previously undocumented Iran-aligned cyber espionage group.
- Reported targets include telecommunications companies, airlines and critical infrastructure in Cyprus.
- Its KuboShell backdoor uses the InterPlanetary File System (IPFS) for command and control.
- The group deploys Homa, a post-compromise framework that reimplements an existing tool.
- The source excerpt gives no indicators of compromise or Saudi-specific targeting.

Researchers have described a previously undocumented cyber espionage group, Volant Manticore, which is assessed as aligned with Iran. According to the report, it has targeted telecommunications companies, airlines and critical infrastructure in Cyprus.

What is known

The group's operations centre on a backdoor named **KuboShell**. Instead of relying only on conventional servers, it uses the InterPlanetary File System (**IPFS**), a decentralised file-sharing network, for command and control. After gaining access, the group deploys **Homa**, a post-compromise framework that reimplements an existing tool.

The available excerpt does not list indicators of compromise, initial access methods, or any victims in Saudi Arabia.

Why it matters for Saudi institutions

The sectors named, telecoms, aviation and critical infrastructure, are also core sectors in the Kingdom. C2 traffic over IPFS can look like ordinary web traffic and may bypass controls that depend on domain or IP reputation. Institutions in these sectors should treat the report as a prompt to review detection coverage rather than as evidence of local activity.

Suggested approach

Wait for the full technical report and indicators, then check them against your telemetry. In the meantime, confirm that you can see and control access to decentralised file-sharing gateways from corporate and operational networks.

What to do now

1. Obtain the full technical report and compare any published indicators with proxy, DNS and endpoint logs.
2. Review whether IPFS gateways and clients are reachable from corporate and operational networks, and restrict them where there is no business need.
3. Add detection for unusual outbound connections to decentralised storage services from servers and sensitive systems.
4. Check that telecom, aviation and critical-infrastructure systems have EDR coverage and centralised logging.
5. Share relevant findings with the National Cybersecurity Authority and your sector counterparts through established channels.