Iranian Chafer APT Targeted Air Transportation and Government in Kuwait and Saudi Arabia

By Liviu ARSENE

Archived: 2026-04-05 15:18:10 UTC

Bitdefender researchers have found attacks conducted by the Chafer APT threat group – known to have an apparent Iranian link – in the Middle East region, dating back to 2018. The campaigns were based on several tools, including “living off the land” tools, which makes attribution difficult, as well as different hacking tools and a custom built backdoor.

Victims of the analyzed campaigns fit into the pattern preferred by this actor, such as air transport and government sectors in the Middle East.

During one analyzed incident, the operation potentially lasted more than one and a half years, during which time the APT group deployed various tools for persistence and lateral movement.

Some of the most interesting findings of the investigation involve attacker activity that occurred during weekends and attacker-created user accounts, with a potential end goal of data exploration and exfiltration.

Key findings:

- Campaign targeted air transportation and government
- Attacker activity occurred on weekends
- In the Kuwait attack, threat actors created their own user account
- The Saudi Arabia attack relied on social engineering to compromise victims
- The end goal of both attacks was likely data exploration and exfiltration

For the full report and the complete analysis of the analyzed components, please check the research paper available below. An up-to-date and complete list of indicators of compromise is available to Bitdefender Advanced Threat Intelligence users.

Download the whitepaper

Source: https://www.bitdefender.com/blog/labs/iranian-chafer-apt-targeted-air-transportation-and-government-in-kuwait-and-saudi-arabia/