Lab Dookhtegan hacking group disrupts communications on dozens of Ira

Data: 2025-08-30 10:44:33

Autor: Inteligência Against Invaders

Lab Dookhtegan hacking group disrupts communications on dozens of Iranian ships

Lab Dookhtegan hacking group allegedly disrupted communications of 60 Iranian ships run by sanctioned firms NITC and IRISL.

The hacking group Lab Dookhteganallegedlydisrupted the communications of 60 Iranian ships. The attack hit at least 39 tankers and 25 cargo ships operated by Iranian maritime companies National Iranian Oil Tanker Company and Iran Shipping Lines, which the US sanctioned.

Hackers breached the satellite communications company Fannava, disabling the Falcon communications system and wiping core data. The attack left the Iranian ships blind.

The group published screenshots demonstrating they achieved root access on Linux terminals running iDirect satellite software (version 2.6.35). The software is considered ancient and not compliant with basic cybersecurity standards.

Hackers mapped Iran's fleet modem by modem, seized Falcon comms, and maintained five months of persistence before crippling ships in August.

"Once inside, the hackers went after something called "Falcon" – the software that keeps these satellite links alive. Think of it as the heart of the ship's communication system. Stop the Falcon, and the ship goes dark. No emails to shore, no weather updates, no port coordination, nothing." reported *the blog Nariman Gharib.*

"But here's what the email logs actually reveal – and this is huge: the timestamps go back to May and June. That means Lab-Dookhtegan didn't just hit and run in March. They've been sitting inside Iran's maritime network for five months straight. They had persistent access this entire time, could flip systems on and off whenever they wanted, and probably monitored every communication going through."

Attackers aimed for permanent damage, overwriting six storage partitions with zeros, wiping logs, configs, and recovery data, crippling the ship communications.

"I'm looking at a spreadsheet with phone numbers, IP addresses, and – this is the embarrassing part – passwords in plain text. We're talking passwords like "1402@Argo" and "1406@Diamond."" continues the blog post. "With this data, the attackers could theoretically listen to phone calls between ships and ports, impersonate vessels, or just cause more chaos by killing voice communications too."

This is the second attack launched by Lab-Dookhtegan this year, following its March disruption of 116 ships. This time, the strike coincides with new U.S. sanctions on Iranian oil, making the damage even more severe. The hackers didn’t just cause temporary outages, each affected vessel now requires a complete system reinstall, a process that could keep ships idle for weeks or months. For Iran’s already pressured fleet, which depends on constant communication and coordination to evade seizures, this is catastrophic. Without navigation, communication, or even the ability to call for help, the fleet is effectively crippled. The attack was no accident; it was a precise, calculated move to hit Iran at its most vulnerable moment, and by all evidence, it worked.

Follow me on Twitter:@securityaffairsandFacebookandMastodon

PierluigiPaganini

(SecurityAffairs–hacking,Iranian ships)