



Office of
Deputy Commissioner
of Maritime Affairs

THE REPUBLIC OF LIBERIA

LIBERIA MARITIME AUTHORITY

22980 Indian Creek Drive,
Suite 200
Dulles, Virginia 20166, USA
Tel: +1 703 790 3434
Fax: +1 703 790 5655
Email: security@liscr.com
Web: www.liscr.com

20 September 2026

MARINE SECURITY BULLETIN –35/2026

Dear Shipowners, Operators and Masters

Subject: Cybersecurity Incident in the Atlantic Ocean

A Liberian flagged tanker vessel was the victim of a malware attack on 08 August while transiting the Atlantic Ocean enroute to the United States. Upon detecting the attack, the vessel activated its cybersecurity response procedures. Affected terminals were identified and disconnected, and impacted systems were isolated. Subsequent inspection found that 8 of 11 onboard PCs were infected. The attack resulted in the deletion of a critical server's operating system and data, causing disruption to email services. Both stored and backed up data were also deleted. No abnormalities were identified in navigation or machinery systems, and the vessel continued normal operations throughout the incident.

Investigation revealed repeated unauthorized remote access activity through the vessel's satellite communications firewall prior to the attack, along with several other intrusion attempts. It is suspected that an external threat actor gained remote access to shipboard systems and deployed malware that spread across the vessel's business network. The malware caused the deletion of operating systems and data, resulting in system outages and data loss. Network segregation proved effective in preventing the malware from spreading into safety-critical systems.

Recommendations

Cybersecurity incidents should be treated with the same level of seriousness as a physical attack on a vessel because of their potential impact on operations and critical onboard systems. Operators and Masters should refer to [MSA 02/2020 Rev.2](#) for guidance on incorporating cyber risk management into Safety Management Systems in accordance with International Safety Management (ISM) Code.

Operators and Masters should also consult the [Best Management Practices for Maritime Security \(BMP MS\)](#) for guidance on addressing cyber threats during voyage planning, and when reviewing Ship Security Plans. Vessel owners and Masters are encouraged to review their cyber security response procedures regularly, verify the effectiveness of network segregation and access controls, strengthen monitoring of remote access connections, account for the increasing volume of digital data exchanges between shipboard systems, and ensure backup and recovery procedures are tested and protected from unauthorized access.

Additional maritime security guidance and updates are available through the International Maritime Organization and the Liberian Registry's online library. Further guidelines on measures for cybersecurity can be found in [MSC-FAL-1/Circ.3/as amended](#).

Contact Information

Please keep LISCR's Security Department informed of any security incidents at:
Office of the Senior Deputy Commissioner of Maritime Affairs
Republic of Liberia
22980 Indian Creek Drive, Suite 200 Dulles, Virginia 20166 USA
D: +1 571 495 5944 / O: +1 703 790 3434 / F: +1 703 790 5655
Email: Security@liscr.com
www.liscr.com