OMNIACCESS

A wake-up call for yacht cyber security

A luxury yacht recently fell victim to a phishing attack that escalated into financial fraud and email compromise, resulting in $100,000 in fraudulent transfers and unauthorized access to the captain's email account. Attackers impersonated the captain to request payments from contacts and vendors.

With support from OmniAccess' SOC team, the incident was contained and normal operations restored, highlighting the importance of robust cyber security measures in the yachting industry.

* Representative images. Not the actual vessels referenced in this case.

How malicious actors took advantage & gained access

Attackers gained access through a phishing email.

40% of email users are able to recognize phishing email attacks. The captain of the vessel wasn't trained and became a victim. Malicious actor also got access to a session token theft, which allowed them to manipulate the email application by creating hidden rules that limited captain's visibility on emails, which led to missing important correspondences.

The breach was traced back to several cyber security weaknesses:

- The same password was used for both; the email account and the payment application.
- There was no multi-factor authentication (MFA) in place.
- Multiple misconfigurations left the email system vulnerable.

85% of organizations with a strong recovery plan resume operations within 72 hours of an incident.

Incident response in action: a coordinated recovery effort

Recognizing the urgency of the situation, the yacht's management engaged top-tier cyber security experts from OmniAccess to assist in responding to the incident and strengthening their digital defenses.

According to the NIST Computer Security Incident Handling Guide, organisations with a strong response plan can reduce recovery time by up to 60%.

The first critical step was the deployment of an Endpoint Detection and Response (EDR) solution across all onboard devices and systems. This enabled continuous real-time monitoring, allowing for the immediate detection and containment of malicious activity before it could escalate. The OmniAccess Security Operations Center (SOC) conducted regular scans and closely monitored device behavior to ensure ongoing protection.

To mitigate future phishing risks and secure communications, an advanced email security solution was integrated into the yacht's email system.

Awareness at sea: training the first line of cyber defense

This solution scanned all emails, automatically blocking suspicious messages and preventing unauthorized access. Additionally, crew members underwent comprehensive cyber security awareness training to recognize phishing attempts and enforce security best practices. This led to a significant improvement in a 90% effectiveness to detect and avoid phishing emails.

To further enhancing the vessel's security, the yacht management collaborated with our SOC team, providing 24/7 monitoring and rapid response capabilities.

Beyond recovery: strengthening the yacht's long-term cyber posture

This incident underscores the importance of having comprehensive cyber security strategy in safeguarding luxury vessels from sophisticated digital attacks, as we can see a 56% increase of cyber-attacks & maritime industry.

The SOC's dedicated highly skilled cyber security professionals actively analyzed their network traffic, identified anomalies, and responded to threats in real time. This proactive approach ensured that any potential security incidents were mitigated without disrupting business continuity. 85 % of organizations with a strong recovery plan resume operations within 72 hours of an incident.

With these robust cyber security measures in place, the yacht's security posture improved significantly. The risk of phishing attacks, unauthorized access, and financial fraud was drastically reduced. The yacht's crew and stakeholders could once again operate with confidence, assured that their data and financial transactions were well-protected against cyber criminals.

Why every yacht needs a cyber strategy
- backed by data

This case was just one of many threats uncovered by our Security Operations Center. Get the full picture of today's maritime cyber landscape - from AI-driven phishing scams to hacktivism - in our latest cyber threat report.

Download our Maritime Threat Report

150 +
Cyber security experts

100 +
Cyber security certifications

80 +
Additional IT & OT services

20 +
Technology partnerships

Join us at the Monaco Yacht Show

STAND DS14 DARSE SUD - SEPT. 24-27, 2025

Your global cyber security partner for remote operations

Our cyber security services and solutions are delivered by a global team of over 130 experts split between Threat Intelligence teams, Pentesters, GRC (Government, Risk and Compliance) and advanced maritime SOC (Security Operations Centre) teams, operating from our global Marlink Group Cyber centers in Europe, South America and Asia.

Stop by our stand and explore

- How to protect your vessel from evolving cyber threats.
- How our solutions optimize connectivity and operations.
- What data visibility means at sea.

Whether you're a yacht owner, captain or technical manager, visit us to experience how OmniAccess is helping shape the future of digital operations at sea

Omniaccess.com

THE GROUP | MARLINK | OMNIACCESS | TELEMAR | MARLINK CYBER

Our partners and technology solutions

FORTINET splunk> AVANAN CISCO CROWDSTRIKE paloalto tenable Microsoft