

IN 1459 – IMCA Security Bulletin 04/19

Information Note Published on 20 November 2019

The IMCA [Security Committee](#) is determined to raise awareness of security issues that can potentially harm member companies. Information provided in this regular Security Bulletin is intended to be used by Members to either directly pass on to employees or use the material it contains as part of an existing company security awareness programme.

1. Cyber security

October was the US National Cybersecurity Awareness Month “Own IT. Secure IT. Protect IT”.

The ‘Be cyber aware at sea’ website is recognised as a useful tool to assist in raising awareness. Each IMCA Security Bulletin refers the reader to one of the ‘Be cyber aware at sea’ poster and video campaigns. This bulletin it is, “be discreet when you tweet”. [Download poster](#).

IMCA Contact:



Nicholas Hough
Consultant – Safety & Security

Original IMCA author:



Richard Purser
Technical Adviser – Marine

Committees:

[Security](#)

Tags:

[#Health, Safety & Security](#) [#Security](#)

**BE CYBER AWARE
AT SEA**

**BE
DISCREET
WHEN
YOU
TWEET**



Be careful what you post on social media, you never know who is watching or what locational information you might be sharing.

2. Ransomware attack

A Member has informed us that in the first three months of 2019, there were four ransomware attacks on their vessels. These ransomware attacks completely disabled the computer systems on its vessel.

What happened?

These ransomware attacks completely disabled the following computer systems on the vessel:

- Windows Active Directory Server.
- Network connectivity (DHCP).
- Engine Control Room PC.
- Communications PC.
- Common hard drive and Network Attached Storage (NAS).
- Vessel black box.
- Centralised file sharing system.

The suspected source of the ransomware was from:

- File transfer from external parties directly via USB.
- “Phishing” type of email opened by vessel crew.

The type of ransomware encountered:

- ETH
- COCKISTA (similar on two vessels).
- Unknown but after clicking the attachments on the “Phishing” email, all data was encrypted with strange extension file name (BRBAK and mxq1d131 extension file).

Actions/lessons learnt

- Ensure your Antivirus protection is up-to date.
- Ensure backup is configured correctly and up to date.
- Do not open/click any suspicious email/links or from unknown sources:
 - Check the sender email address
 - Consult with Vessel IT if in ANY doubt as to the genuineness of an email.
- Restrict access to system interfaces.
 - Keep system cabinets and server rooms locked all the time and only allow access to one dedicated person on board.

Members may wish to [refer to the following video](#).

3. Traditional security

A Member company has recently participated in an exercise with NATO in the Mediterranean. The Member reported a very valuable learning event for on-board crew and shoreside support teams.

A brief overview of MED Interceptor is included in MED Interceptor.

Links to recent security related information:

- Combined Maritime Forces Industry Releasable Threat Assessment LATEST.

- Operation Sentinel Arabian Gulf, Arabian Sea and Red Sea.
- Sea Robberies, Sea Thefts and attempted Actions – Approaches to Singapore Strait.

Members are encouraged to report to the Maritime Domain Awareness for Trade-Gulf of Guinea (MDAT-GoG) both on entering the Voluntary Reporting Area (VRA) and on sighting any suspicious behaviour. Contact details are available on the [NATO Shipping Centre website](#).

OCIMF have a Merchant Navy Liaison Officer (MNLO) at the United Kingdom Maritime Trade Operations (UKMTO) in Dubai. If Members need support, advice or would like to visit please contact:

Chris Scothern (ExxonMobil)
MNLO Dubai
mnlo.dubai@ocimf.org
+971 (56) 686 5509 (m)

HSS Security

Technical Library