Marine Safety Information Bulletin
Sector Los Angeles – Long Beach

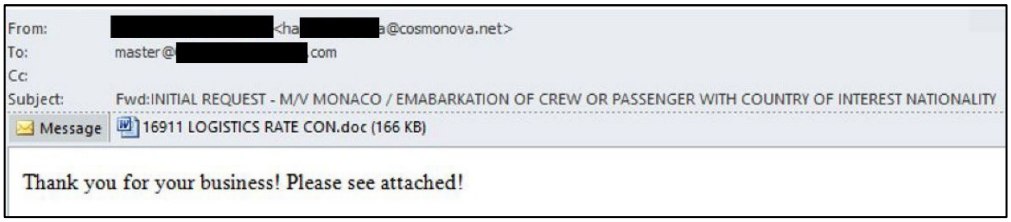
Commander
U.S. Coast Guard Sector
Los Angeles – Long Beach
1001 S. Seaside Avenue Bldg. 20
San Pedro, CA 90731-0208

MSIB Number: 01-21
Date: January 22, 2021

VESSEL CYBERSECURITY ALERT

The Los Angeles-Long Beach maritime community should be on high alert for phishing emails from malicious actors impersonating USCG email addresses, specifically emails containing COVID-19 screening forms for vessels entering port.

Sector Los Angeles – Long Beach responded to a report of a container vessel that received a suspicious email appearing to originate from a legitimate USCG Port State Control (PSC) Officer. The e-mail contained several links as well as an attachment. The recipient was encouraged to open the attachment or click on the links prior to authorization to enter the port. The vessel's master contacted the USCG to verify the validity of the e-mail. The email was not authentic and did not originate from the Coast Guard.



Sector LA-LB Port State Control responded to the incident using their Vessel Cyber Incident Protocol and verified the safety, security, and operational functionality of the vessel's critical systems. Based on numerous recent maritime phishing attempts, the malicious actors prefer to target vessels using spoofed USCG Port State Control e-mails. Several important details in the email include:

- The sender of the e-mail was partially spoofed, and appeared to come from a Coast Guard Port State Control Officer. The sender's e-mail address did not end in "@uscg.mil." (ha[redacted]a@cosmonova.net). Email correspondence from the Coast Guard will end in "@uscg.mil."

- Based on the sophistication of the e-mail, the malicious actor may have some knowledge of the Maritime Transportation System (MTS) and/or may have reviewed a previous legitimate e-mail from the USCG. It cannot be ruled out that the malicious actor may have compromised an e-mail account of a previous recipient of a legitimate USCG PSC e-mail.

- The contents of the e-mail may have been copied from a previous legitimate e-mail.

- The statement, "Until your response is received by this office, the M/V [redacted], is not clear to enter the port" which compels the recipient to click a link or open the attachment.

Vessel operators are encouraged to contact USCG via a confirmed legitimate phone number if they question the validity of a USCG Port State Control e-mail. The Coast Guard urges maritime stakeholders to verify the validity of the email sender prior to responding to or opening any unsolicited email messages.

As always, any potential threat to the cybersecurity of your vessel or facility should be taken seriously, and Breaches of Security or Suspicious Activities resulting from cyber incidents shall be reported to the National Response Center (NRC) at **1-800-424-8802**. For additional guidance on reporting cyber incidents refer to CG-5P Policy Letter 08-16, "*Reporting Suspicious Activity and Breaches of Security."* For further information on spoofing, refer to USCG MSIB: 19-20 "MALICIOUS EMAIL SPOOFING INCIDENTS."