Marine Safety Information Bulletin

Commandant (CG-5PC)
Attn: Inspections and Compliance Directorate
U.S. Coast Guard STOP 7501
2703 Martin Luther King Jr Ave, SE
Washington, DC 20593-7501

MSIB Number: 04-19
Date: May 24, 2019
Contact: LCDR Sam Danus
Phone: (202) 372-2268
E-Mail: PortStateControl@uscg.mil

Cyber Adversaries Targeting Commercial Vessels

This bulletin is to inform the maritime industry of recent email phishing and malware intrusion attempts that targeted commercial vessels. Cyber adversaries are attempting to gain sensitive information including the content of an official Notice of Arrival (NOA) using email addresses that pose as an official Port State Control (PSC) authority such as: **port @ pscgov.org**. Additionally, the Coast Guard has received reports of malicious software designed to disrupt shipboard computer systems. Vessel masters have diligently reported suspicious activity to the Coast Guard National Response Center (NRC) in accordance with Title 33 Code of Federal Regulations (CFR) §101.305 – *Reporting*, enabling the Coast Guard and other federal agencies to counter cyber threats across the global maritime network.

As a reminder, suspicious activity and breaches of security must be reported to the NRC at **(800) 424-8802**. For cyber attempts/attacks that do not impact the operating condition of the vessel or result in a pollution incident, owners or operators may alternatively report to the 24/7 National Cybersecurity and Communications Integration Center (NCCIC) at **(888) 282-0870** in accordance with CG-5P Policy Letter 08-16, *"Reporting Suspicious Activity and Breaches of Security."* When reporting to the NCCIC, it is imperative that the reporting party notify the NCCIC that the vessel is a Coast Guard regulated entity in order to satisfy 33 CFR §101.305 reporting requirements. The NCCIC will in turn forward the report to the NRC that will then notify the cognizant Coast Guard Captain of the Port (COTP).

The Coast Guards urges maritime stakeholders to verify the validity of the email sender prior to responding to unsolicited email messages. If there is uncertainty regarding the legitimacy of the email request, vessel representatives should try contacting the PSC authority directly by using verified contact information. Additionally, vessel owners and operators should continue to evaluate their cyber defense meaures to reduce the effect of a cyber-attack. For more information on the NCCIC's services, cyber-related information, best practices, and other resources, please visit: https://www.dhs.gov/CISA.

The Coast Guard applauds companies and their vessels for remaining vigilant in the identification and prompt reporting of suspicious cyber-related activities. Questions pertaining to this bulletin may be directed to the Coast Guard Office of Commercial Vessel Compliance's Port State Control Division (CG-CVC-2) at PortStateControl@uscg.mil.

-uscg-