SUSPICIOUS ACTIVITY CYBER INCIDENTS CONTINUE ABOARD COMMERCIAL VESSELS

The purpose of this Bulletin is to update the maritime industry of three recent cyber incidents targeting commercial vessels. On January 26th 2019, a commercial vessel received an email from an individual or entity claiming to represent an official Port State Control body. The email originated from an email address noted as "port@pscgov.org" and was sent directly to the vessel's Captain requesting sensitive information about the vessel, its crew, and its cargo. The vessel's master was rightfully skeptical about the request and immediately activated elements of the vessel security plan related to this type of suspicious cyber incident. The vessel's Captain reported the incident and forwarded the suspicious email and information to the local USCG Captain of the Port for investigation and follow-up.

On March 14th, 2019, a different commercial vessel operating in the same area as the previous incident received a SAT-C message by email via the ships Global Marine Distress Satellite System (GMDSS) from an originator claiming to be a U.S. port-specific Port State Control entity. The nature of the inquiry was more direct, requesting information on the nature of the cargo. Specifically, whether the vessel had explosive or radioactive cargo aboard. This same vessel received an identical inquiry again on April 3rd while operating in the same area.

These three spear phishing attempts indicate a troubling trend toward targeting cargo vessels while underway. As a reminder, CG-5P Policy Letter 08-16 titled "*Reporting Suspicious Activity and Breaches of Security*" outlines the criteria and process for Maritime Transportation Security Act (MTSA) regulated vessels and facilities to report suspicious activity (SA) and breaches of security (BoS) including cyber incidents.

The Coast Guard's National Response Center (NRC) remains the federal government's primary point of contact for notifications of all SAs or BoSs including cyber. For cyber incidents that do not impact physical security or cause a pollution incident, the Coast Guard allows reporting parties to report the incident to the National Cybersecurity and Communications Integration Center (NCCIC) in lieu of the NRC. The NCCIC can be reached at (888) 282-0870 and may be able to provide technical assistance to the reporting party.

If contacting the NCCIC in lieu of the NRC, it is imperative that the reporting party inform the NCCIC that it is a Coast Guard regulated entity in order to satisfy the reporting requirements of 33 CFR part 101.305. The NCCIC will forward the report electronically to the NRC, who will notify the appropriate COTP.

Cyber-related risks in the maritime environment continue to be cause of concern. Cyber technologies enable the Marine Transportation System to operate with an impressive record of reliability and at a capacity that drives the U.S. economy and supports national defense, homeland security, and related needs. While cyber systems create benefits, they also introduce risk. Exploitation, misuse, or failure of cyber systems could cause harm to the marine environment or disrupt vital trade activity. As a result, cyber risk management is increasingly important.

Questions regarding this issue should be forwarded to your local USCG Captain of the Port.