US Coast Guard Cyber Command
Maritime Cyber Alert 02-20

May 13, 2020

Information Sharing Protocol: TLP-GREEN

(Recipients may share TLP: GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels.)

PHISHING CAMPAIGN TARGETING MARITIME COMMUNITY

Summary: The Maritime community should be on high alert for phishing emails from malicious actors masquerading as legitimate business contacts. This Maritime Cybersecurity Alert is to provide broad awareness to Marine Transportation System (MTS) stakeholders about techniques used by these threat actors using current economic practices induced by the COVID-19 pandemic as a means of phishing the maritime industry, expound upon observed tactics used by threat actors, and encourage cybersecurity best practices.

Business contact impersonation, which consists of fraudulent emails that are created to fool the recipients into either handing over sensitive information, extort money or trigger malware installation on shore-based or vessel IT networks, is one of the largest cyber threats currently facing the maritime industry. In recent months, the USCG has identified, through publicly available information, a surge in the quantity of phishing emails received by vessels and port facilities, using these impersonating tactics. Successful phishing attacks may compromise networks and result in exfiltration of sensitive data and unauthorized access to critical portions of the facility, to include the operational technology/process control portions of the vessel or facility networks.

Precautions:

Operational Technology (OT) networks are critical to port operations and the safety of personnel at facilities and onboard cargo vessels. Malware intrusion onto IT networks is commonly the first step in compromising an OT network. Coast Guard Cyber Command investigations of two recent cyber incidents at facilities revealed that attackers were moving laterally from IT to OT networks. This traversal was largely due to insufficient cybersecurity measures implemented withinthe facilities. One of the attacks resulted in completely shutting down facility operations due to compromised safety systems. The other resulted in the facility falling back on secondary

communication means and reverting to manual operations of equipment controlled remotely. Forensic evidence showed, that in one case, the attackers had persistent network access for over nine months after the initial compromise, but before the actual ransomware attack was executed.

Be prepared for possible cyber disruptions, suspicious emails, network delays, and report suspicious activity to local law enforcement. As always, any potential threat to the physical or cybersecurity of your vessel or facility should be taken seriously, and any Breach of Security, Suspicious Activity or Cyber Security Incidents shall be reported to the National Response Center at 1-800-424-8802. Consider also reporting the event to your local CG Captain of the Port or the CG Cyber Command 24x7 watch at 202-372-2904 or CGCYBER-SMB-NOSC-BWC@uscg.mil

Mitigations:

Users, administrators and operators in the maritime community who believe that they have been impacted or targeted by phishing campaigns should consider conducting a detailed analysis of their systems to identify malicious files or activities. Outside assistance might be leveraged in the event that local tools and resources are not adequate to identify sophisticated threats. As you assess your organization's readiness to prevent and respond to these types of targeted attacks, reflect on the following:

- Is there training for all employees to identify suspicious emails?
- Are your incident response and recovery plans up to date?
- Has your organization identified third party vendors to provide technical assistance in the event of an attack?
- Are email filtering and anti-spam applications up to date and configured properly?
- Has your organization conducted recent policy audits in both IT and OT networks?
- Does your organization's Change Control Board review patches and updates on OT systems?
- Has your organization created and maintained backups for devices within the OT network?
- Is your OT network adequately segregated from your IT network?

Beyond reflection on these questions, consider implementing the following processes to further reduce the risk and surface for a successful cyber-attack:

- Educate and train all areas within the marine supply chain to understand that they are under constant threat of targeted cyber campaigns.
- Identify and present impacts of cyber consequences, as a result of careless cyber practices or general inattentiveness, through real-world scenarios.
- Provide regular training and guidance to assist in identifying the characteristics of potential email phishing attempts.
- Enforce, when possible, external communications within the supply chain to corroborate and verify factual email communication.

Resources:

For further information and recommended best practices refer to National Institute of Standards and Technology (NIST) SP800-177 (Rev. 1) Trustworthy Email, NIST SP800-45 (Ver. 2) Guidelines on Electronic Email Security, and NIST SP800-82 (Rev. 2) Guide to Industrial Control Systems (ICS) Security. Resources and assistance can be requested from DHS CISA, and more information can be found at cisa.gov/detection-and-prevention