Marine Safety Information Bulletin

Commandant
U.S. Coast Guard
Inspections and Compliance Directorate
2703 Martin Luther King Jr Ave, SE, STOP 7501
Washington, DC 20593-7501

MSIB Number: 19-20
Date: September 30, 2020
Phone: (202) 372-1160
E-Mail: Leslie.M.Downing@uscg.mil

MALICIOUS EMAIL SPOOFING INCIDENTS

This Marine Safety Information Bulletin (MSIB) is intended to highlight several recent cyber events involving increasingly sophisticated malicious email spoofing techniques within the Marine Transportation System (MTS). The types of reported spoofing attacks included impersonating Coast Guard (uscg.mil) email addresses, and Coast Guard industry communications regarding Area Maritime Security Committee meetings. In one case, the opening of a malicious file caused a network compromise that resulted in additional spoofed emails that were sent to MTS port partners. These types of attacks have potential cascading consequences, and impacted organizations should immediately notify all affected stakeholders and local authorities. Coast Guard units along with Maritime Transportation Security Act (MTSA) regulated facilities and vessels should be on high alert and remain vigilant for similar cyber threats within your areas of responsibility.

These events have been analyzed and investigated, and the following recommendations to MTS stakeholders have been provided:

1. Technical Controls: Official Coast Guard emails use Domain-based Message Authentication Reporting and Conformance (DMARC) as an authentication method for protection against spoofing. It is highly recommended that organizations consider implementing DMARC to help ensure all emails that appear to come from the Coast Guard, and other official sources, pass the Sender Policy Framework/Domain Keys Identified Mail (SPF/DKIM) checks to confirm origin. DMARC is designed to fit into an organization's existing inbound email authentication process and protect against direct domain spoofing. It allows a sender to indicate that their messages are protected by SPF and/or DKIM, and tells a receiver what to do if neither of those authentication methods passes. For more information on DMARC please visit https://DMARC.org.

2. User Awareness and Training: Employee awareness and engagement is key to effective cybersecurity protection. It is strongly recommended that organizations implement Information Technology (IT) Security Awareness training programs in accordance with National Institute of Standards and Technology Special Publication 800-50, ISO 27001 or similar standards, and per guidance set forth in Navigation and Vessel Inspection Circular (NVIC) 01-20: Guidelines for

Addressing Cyber Risks at Maritime Transportation Security Act (MTSA) Regulated Facilities to meet this objective.

3. Collaboration with IT Staff: It is highly recommended that Facility Security Officers and Vessel Security Officers quickly collaborate, and socialize this MSIB with your IT staff, to best address mitigating strategies for responding to and protecting against similar cyber threats within your organizations.

The Coast Guard encourages collaborative efforts between MTS stakeholders and Coast Guard field units to recognize and respond to various potential cyber threats, and continues to work with maritime stakeholders to develop guidance, policy, and recommended best practices. Recently released guidance includes Navigation and Vessel Inspection Circular (NVIC) 01-20: Guidelines for Addressing Cyber Risks at Maritime Transportation Security Act (MTSA) Regulated Facilities. This NVIC provides guidance to MTSA regulated facility owners and operators on complying with requirements to assess, document, and address computer system and network vulnerabilities. Additionally, a Facility Inspector Cyber Job Aid was developed to provide Coast Guard marine safety personnel with additional guidance for evaluating facility cyber vulnerabilities. Facility security personnel may likewise reference this guide for familiarization.

As always, any potential threat to the cybersecurity of your unit, 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 at 1-800-424-8802. Consider also reporting the event to your local Coast Guard Captain of the Port or the Coast Guard Cyber Command 24x7 watch at 202-372-2904 or CyberWatch@uscg.mil. Your willingness to comply and report in a timely manner helps the U.S. respond quickly and effectively and makes the maritime critical infrastructure more secure.

Richard V. Timme, RDML, U. S. Coast Guard, Assistant Commandant for Prevention Policy sends