UNITED STATES COAST GUARD
U.S. Department of Homeland Security

MARINE SAFETY ALERT

Inspections and Compliance Directorate

July 8, 2019 Safety Alert 06-19
Washington, D.C.

Cyber Incident Exposes Potential Vulnerabilities Onboard Commercial Vessels

In February 2019, a deep draft vessel on an international voyage bound for the Port of New York and New Jersey reported that they were experiencing a significant cyber incident impacting their shipboard network. An interagency team of cyber experts, led by the Coast Guard, responded and conducted an analysis of the vessel's network and essential control systems. The team concluded that although the malware significantly degraded the functionality of the onboard computer system, essential vessel control systems had not been impacted. Nevertheless, the interagency response found that the vessel was operating without effective cybersecurity measures in place, exposing critical vessel control systems to significant vulnerabilities.

Prior to the incident, the security risk presented by the shipboard network was well known among the crew. Although most crewmembers didn't use onboard computers to check personal email, make online purchases or check their bank accounts, the same shipboard network *was* used for official business – to update electronic charts, manage cargo data and communicate with shore-side facilities, pilots, agents, and the Coast Guard.

It is unknown whether this vessel is representative of the current state of cybersecurity aboard deep draft vessels. However, with engines that are controlled by mouse clicks, and growing reliance on electronic charting and navigation systems, protecting these systems with proper cybersecurity measures is as essential as controlling physical access to the ship or performing routine maintenance on traditional machinery. It is imperative that the maritime community adapt to changing technologies and the changing threat landscape by recognizing the need for and implementing basic cyber hygiene measures.

In order to improve the resilience of vessels and facilities, and to protect the safety of the waterways in which they operate, the U.S. Coast Guard **strongly recommends** that vessel and facility owners, operators and other responsible parties take the following basic measures to improve their cybersecurity:

- Segment Networks. "Flat" networks allow an adversary to easily maneuver to any system connected to that network. Segment your networks into "subnetworks" to make it harder for an adversary to gain access to essential systems and equipment.
- Per-user Profiles & Passwords. Eliminate the use of generic log-in credentials for multiple personnel. Create network profiles for each employee. Require employees to enter a password and/or insert an ID card to log on to onboard equipment. Limit access/privileges to only those levels necessary to allow each user to do his or her job. Administrator accounts should be used sparingly and only when necessary.

- Be Wary of External Media. This incident revealed that it is common practice for cargo data to be transferred at the pier, via USB drive. Those USB drives were routinely plugged directly into the ship's computers without prior scanning for malware. It is critical that any external media is scanned for malware on a standalone system before being plugged into any shipboard network. Never run executable media from an untrusted source.
- Install Basic Antivirus Software. Basic cyber hygiene can stop incidents before they impact operations. Install and routinely update basic antivirus software.
- Don't Forget to Patch. Patching is no small task, but it is the core of cyber hygiene. Vulnerabilities impacting operating systems and applications are constantly changing – patching is critical to effective cybersecurity.

Maintaining effective cybersecurity is not just an IT issue, but is rather a fundamental operational imperative in the 21st century maritime environment. The Coast Guard therefore **strongly encourages** all vessel and facility owners and operators to conduct cybersecurity assessments to better understand the extent of their cyber vulnerabilities.

The Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) provides several free resources to help vessel owners assess the state of their networks and identify cyber vulnerabilities. One such resource is National Cybersecurity and Communications Integration Center's (NCCIC) Hunt and Incident Response Team (HIRT). The NCCIC HIRT is DHS's front line entity for proactively hunting for malicious cyber activity and responding to cyber incidents. HIRT's world-class experts lead response, containment, remediation, and asset recovery efforts in government, critical infrastructure and private sector organizations. Any company can request HIRT services by visiting their website https://www.us-cert.gov or by calling the NCCIC 24x7 watch floor at (888) 282-0870. Following a DHS HIRT engagement, the company will receive a confidential report with analysis and mitigation recommendations, as well as assistance in restoring services.

Please note the Coast Guard has released Marine Safety Information Bulletin (MSIB) 04-19 also related to maritime cyber issues and which covers slightly different subtopics including recent email phishing attempts targeted at commercial vessels. Other MSIBs are available here:

https://www.dco.uscg.mil/Featured-Content/Mariners/Marine-Safety-Information-Bulletins-MSIB/

This safety alert was created by U.S. Coast Guard Sector New York. This alert is provided for informational purposes only and does not relieve any domestic or international safety, operational or material requirement. Questions may be addressed to the Safety and Security Office, Coast Guard Sector New York at D01-SMB-SecNY-VDO@uscg.mil or to the Sector NY Command Center at 718-354-4353.