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: 10-19
Date: December 16, 2019
Contact: Mr. Charles Blackmore
Phone: (202) 372-1109
E-Mail: charles.t.blackmore@uscg.mil

Cyberattack Impacts MTSA Facility Operations

The purpose of this bulletin is to inform the maritime community of a recent incident involving a ransomware intrusion at a Maritime Transportation Security Act (MTSA) regulated facility. Forensic analysis is currently ongoing but the virus, identified as “Ryuk” ransomware, may have entered the network of the MTSA facility via an email phishing campaign. Once the embedded malicious link in the email was clicked by an employee, the ransomware allowed for a threat actor to access significant enterprise Information Technology (IT) network files, and encrypt them, preventing the facility’s access to critical files. The virus further burrowed into the industrial control systems that monitor and control cargo transfer and encrypted files critical to process operations. The impacts to the facility included a disruption of the entire corporate IT network (beyond the footprint of the facility), disruption of camera and physical access control systems, and loss of critical process control monitoring systems. These combined effects required the company to shut down the primary operations of the facility for over 30 hours while a cyber-incident response was conducted.

For more information on Ryuk ransomware, please visit: https://www.us-cert.gov/ncas/current-activity/2019/06/28/ncsc-releases-advisory-ryuk-ransomware.

At a minimum, the following measures may have prevented or limited the breach and decreased the time for recovery:

- Intrusion Detection and Intrusion Prevention Systems to monitor real-time network traffic
- Industry standard and up to date virus detection software
- Centralized and monitored host and server logging
- Network segmentation to prevent IT systems from accessing the Operational Technology (OT) environment
- Up-to-date IT/OT network diagrams
- Consistent backups of all critical files and software

The Coast Guard recommends facilities utilize the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) and NIST Special Publication 800-82 when implementing a Cyber Risk Management Program.

The Coast Guard urges maritime stakeholders to verify the validity of the email sender prior to responding to or opening any unsolicited email messages. Additionally, facility owners and operators should continue to evaluate their cybersecurity defense measures to reduce the effect of a cyber-attack.

This release has been issued for public information and notification purposes only.

For more information on ransomware-related best practices and other resources please visit the Cybersecurity and Infrastructure Security Agency (CISA) ransomware resource page at: https://www.us-cert.gov/Ransomware.

As a reminder, suspicious activity and breaches of security, including breaches of telecommunications equipment, including computer, system and network security measures which support functions described in the facility security plan or could contribute to a Transportation Security Incident (TSI), must be reported to the National Response Center (NRC) at **(800) 424-8802**. For additional guidance on the defining and reporting of cyber incidents refer to CG-5P Policy Letter 08-16, "*Reporting Suspicious Activity and Breaches of Security.*"

The Coast Guard encourages companies and their facilities to remain 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 Port & Facility Compliance's Domestic Ports Division (CG-FAC-1) at (202) 372-1109.

-uscg-

This release has been issued for public information and notification purposes only.