TO: National Security Council
FROM: NSC Cybersecurity Task Force ‘Couldn’t Hack It 2.0’
SUBJECT: *Situational Assessment on Cyber Incident Affecting Pacific Shipping Operations*

ASSESSMENT OF SITUATION:
There is a credible disruptive ransomware threat to the global shipping industry which threatens international trade and commerce, as well as freedom of navigation in the Strait of Malacca.

Additionally, a vulnerability allowing data manipulation was detected in Big Oceans Little Hearts LLC (BOLH) cargo management software (CMS) - SEAFARER - used in over 30 ports and in 70% of all maritime traffic. Three vessels were compromised. CMS systems in the Port of Long Beach and Singapore are affected. One day after the malware was identified, a threat actor issued a ransom threat, which was supported by a release of stolen data from an Israeli pentesting firm. With the
holiday season around the corner, increased spread of this malware, or an associated ransomware attack, would result in significant economic disruption as well as oil price increases.

At this time it is unclear if the SEAFARER vulnerability and the ransomware threat are coordinated, hence we advise containing the spread of the malware, preventing economic disruption and preserving the safety of navigation and personnel.

OBSERVABLE #1: SEAFARER Vulnerability
Situation: A CMS vulnerability was detected by BOLH that allows data to be modified through an automated script and deletes past versions of it. BOLH did not fix the problem which has been detected in three vessels that docked at the Port of Long Beach. A compromised storage device was inserted transfering malware between the ship and port. As of 08 NOV 2022 dockside systems have been affected with a 10% increase in wait times. As of 10 NOV 2022, DHS CISA, Coast Guard, FBI and US Navy have been notified and are coordinating a response.
Severity: Medium-High
Attribution: Unknown Actor, using known developer vulnerability
Known Implications:

- Altered cargo manifest causing port delays and requiring manual inspection.
- Infected ships have since departed for S.E. Asia region - inconsistencies exist on their final destination.

Potential Implications:

- Harbor and Port Congestion on West and East Coast ports.
- Smuggling or intentional redirection of containers.
- Potential economic impact if port operations are significantly impacted

OBSERVABLE #2: Disruption of Trade at Strait of Malacca
Situation: CMS issues are being observed in Singapore on 09 NOV 2020. Personnel at Tuas reported technical difficulties regarding their cargo management system, and a number of ships in the Strait of Malacca reported similar issues. Tuas reportedly handles approximately 100 ships a day.
Severity: High
Attribution: The People’s Militia (Medium), Unknown Actors using TPM M.O. (Low)
Known Implications:

- Substantial delays in handling cargo transfer between ships and storage facilities in Tuas.
- Delays in ship movements in and out of Tuas, increasing traffic in the Strait.

Potential Implications:

- Increased risk of collisions in the Strait due to heavy congestion
- Substantial delays of commercial shipping would have severe economic effect, including supply chain disruption, increase in the price of oil, and could impact productivity in countries highly reliant on the Strait such as China, Japan, and South Korea.
- Increased economic strain could raise tensions in the South China Sea, known to be rich in oil.
- US CTF-73 Naval Logistics for Western Pacific, headquartered in Singapore, could be negatively impacted by either malware or the increased traffic in the Strait.

OBSERVABLE #3: Ransomware Threat To Shipping Industry

Situation: DHS CISA advised companies of a public ransom threat made against their shipping vessels. On 5 NOV 2022 the unknown cyber threat actor demanded $10 billion dollars in bitcoin or risk being attacked with the malware. The credibility of the threat is expanded on 7 NOV 2022 with an New York Times article detailing a substantial breach and release of tools from a penetration testing firm, Ipnos Collective Security.
Severity: Medium
Attribution: Unclear. IP Addresses linked to Russian, DPRK, and Thailand.
Known Implications:

- The initial threat was empty with no known compromised systems
- Leaked material from Ipnos contained ample research on how a threat could be carried out

Potential Implications:

- Locked ship-based navigational systems could cause collisions or groundings.
- Ships Dead In Water would be easy targets for piracy
- Port OT systems could be targeted, causing massive delays and safety hazards at port facilities

POLICY RECOMMENDATION:
To mitigate the risks and impacts of a potential attack on the shipping industry, and global supply chains, the NSC should explore the following options:
Contain the Spread:

1. DHS to be given authority to coordinate activities in the United States
2. DHS's CISA: to liaise with BOHL to identify which port facilities use SEAFARER vulnerabilities and ensure that their personnel are logging out of account, even while underway.
    a) CISA must encourage ships with possible infections to not transfer data with other ports
    b) Share information on CMS vulnerability at POLB with Maritime and Port Authority of Singapore
    c) Update notice to shipping industry from CISA regarding the increased credibility of the threat
    d) Coordinate private sector to develop hotfixes for serious vulnerabilities in shipping software
3. USCG: Hail 'Best Eastern', 'Shoal Express' and vessel #3 using satellite phones and instructing them to redirect to the nearest US port for system inspection.
    a) Clarify the end destination for all three vessels.
    b) Prevent direct interface between infected POLB systems and incoming/outgoing ship traffic
4. State Department to advise strategic partners in the region to coordinate response. Warn authorities in Manila of malware threat.
5. Direct INDOPACCOM through DoD to investigate if MSC ships use SEAFARER. NCIS cyber should screen U.S. Navy port facilities.

Preserve Safety of Navigation and Personnel

6. DOT through Maritime Administration to increase manning on all US-flagged commercial shipping vessels to ensure ship crews can safely navigate using paper charts. Recommend the same to others.
7. DHS to require merchant vessels entering US waters to have enough crew to navigate using paper charts. USCG to conduct manual inspection of incoming containers to investigate potential smuggling operations and conduct system inspection at POLB.
8. Recommend Singapore CG deploy to help vessels experiencing navigational troubles in Straits.

Prevent Economic Disruption

9. State Department Direct the U.S. Embassy in Singapore to:
    a) Divert shipping vessels for non essential trade and explore options for the U.S. to provide Foreign Assistance to help bear the cost of associated diversions.
    b) Advise Singapore government to divert non-essential trade to Sunda and Lombok Straits
    c) Request that the FBI, TSA, CBP officers stationed at the US Embassy in Singapore assist Singapore port facilities with cleaning system of malware and manually verifying cargo.