WRITTEN BRIEF

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.

DECISION DOCUMENT – DAY 1

TO: National Security Council
FROM: NSC Cybersecurity Task Force 'Couldn't Hack It 2.0'
Subject: *Policy to Prevent Economic Disruption and Preserve Safety of Navigation and U.S. Personnel*

Summary:
We believe that the primary objectives for the USG are to **prevent economic disruption** and **preserve safety of navigation and U.S. personnel**. To accomplish this, we recommend DHS coordinate national response and increase information sharing regarding vulnerabilities between stakeholders. State Department should work with foreign partners to inform and coordinate international response. Department of Transportation should bolster manning on U.S. flagged shipping while USCG works to secure U.S. ports and preserve safety of navigation and personnel in U.S. territorial waters.

Policy Options:
A) Minimum Response:

- Direct DHS to coordinate activities in the United States
- Share information on CMS vulnerability at POLB with Maritime and Port Authority of Singapore
- Clarify end destination for all three infected vessels
- State Department to advise strategic partners in the region to coordinate response. Warn authorities in Manila, Yokohama, Qingdao, Hong Kong of malware threat
- U.S. Embassy (FBI, CBP, and TSA) should also coordinate with East Asian and Pacific Affairs (EAP) to inform host governments of potential threats and engage them as necessary. U.S. Embassy in Beijing should inquire about raised security level for shipping vessels
- DHS CISA to coordinate with Big Oceans Little Hearts LLC to conduct an investigation of the SEAFARER vulnerability

We assess that Policy A is necessary but insufficient. Due to the unintrusive nature of these recommendations, they do not adequately address safety concerns and will not sufficiently prevent the spread of the malware. Policy A should be carried out in concert with Policy B.

B) Moderate Response **(RECOMMENDED):**

- DHS CISA to work with BOLH and local Port Authorities to ensure ships with possible infections do not transfer data with other ports
- DHS USCG to prevent incoming vessels from interfacing directly between infected POLB systems and provide assistance to the Singaporian Government, if necessary
- U.S. Embassy in Singapore encourages Singaporian Government to deploy its Coast Guard to aid vessels in trouble and to provide USG assistance as necessary with US Embassy personnel
- U.S. Department of Transportation to increase manning on all US-flagged commercial shipping.
- USINDOPACOM to inquire if MSC ships use SEAFARER. NCIS to screen U.S. Navy ports in region

The following responses were considered extreme at the moment as they would place undue pressure on shipping routes and companies. They are worth revisiting should the threat escalate.

C) Severe Response:

- State Department to recommend Singapore divert shipping vessels for non essential trade to Sunda and Lombok Straits and provide Foreign Assistance to help bear the cost of associated diversions
- Department of Homeland Security to enact regulations on incoming commercial vessels to US territorial waters for safety of navigation and prevent smuggling

Recommendation Justification:

NSC should focus on preventing economic disruption and safety of U.S. personnel while minimizing disruption to shipping activities. Our recommended policy (B) enables responding organizations to contain the spread of the malware and implement measures to protect U.S. shipping operations and personnel, without disrupting shipping routes and imposing restrictions on foreign shipping vessels entering U.S. waters.

DECISION DOCUMENT – DAY 2

To: National Security Council
From: NSC Cybersecurity Task Force 'Couldn't Hack It 2.0'
Subject: Policy Recommendations to Restore Global Ports, Shipping Routes, and Supply Chains

Summary:
The malware affecting SEAFARER cargo management system has spread to ships and ports globally, causing massive port delays and safety of navigation concerns and severely impacting maritime trade. The primary objective for the USG is to **protect our homeland security** and the **global economy** by restoring ports, clearing shipping routes, and protecting supply chains. The situation is no longer purely domestic and will require NSC action to initiate robust international engagement to prevent further spread of the malware and ensure safety of navigation, while launching domestic efforts to alleviate port congestion and identify and deter the threat actor.

Recommendations:
It is necessary for the NSC to coordinate an interagency approach with the following policy responses:

- **Launch an FBI investigation** into potential U.S. based threat actors and gather additional intelligence on North Korean activity from the NSA to anticipate future threats and prevent additional attacks.
- **Engage trade associations through DOC** and **engage ICT Supply Chain Risk Management Task Force** through CISA to work to protect supply chains and manage shipping crises.
- **Work with the International Maritime Organization (IMO) to issue regulations r**egarding Automatic Identification Systems (AIS) through the USCG to ensure safety of navigation.
- **Sanitize all merchant vessels in U.S. waters;** issuing DOT to follow IMO Guidance on Cyber Risk Management to prevent the spread of malware.
- **Engage with the Chinese Government** using the DHS CISA's Cybersecurity Hotline to coordinate a USG-Chinese response to alleviate port congestion.
- **DOS begin dialogue with S. Korea, Japan, India, and Australia** through our security cooperation agreements; encouraging China to engage in USG international response plan
- **Mirror Port of Osaka response** with development of new systems that prioritize critical functions for Port Authority in Long Beach and make it an open-source system through a Public Private Partnership
- **Unlock FEMA emergency grants** to provide assistance to U.S. shipping companies and Local Port Authorities to bolster cybersecurity incident response to restore ports.

Decision Process (Assessment and Risks of Recommendations):
It is important that the USG take swift action to resolve the disruption of maritime trade and supply chains by implementing the policy recommendations above. These options seek to mitigate the global crisis by working to gather intelligence to prevent further attacks and initiate law enforcement efforts to deter potential domestic threat actors, engage China through law enforcement channels, take global lead in response through International Organizations and partnerships, and provide assistance to U.S. companies and Local Government.

However, there are key risks associated with these recommendations that should be weighed carefully before implementation. First, there is the risk that the USG is unable to fully mitigate and contain the cybersecurity threat. Second, there is the risk that the International Community is less responsive to USG actions due to our inability to contain the malware spread originally. Additionally, if the USG takes charge of the situation internationally, our lead could result in an increase in Chinese defensive posture.

Additional Response Options Considered to Alleviate Port Congestion and Further Engage with China

- (Severe) DoD to increase military posture in the South China Sea to aid ship navigation
- (Severe) Declaring National Emergency to unlock funding to provide federal money to ports in need until the other efforts are exhausted