WRITTEN BRIEF

TO: National Security Advisor
FROM: Georgetown University - STIA Cyber Team
SUBJECT: SEAFARER Cargo Management Software Cyber-Attack

Judgements: The cyberattack on Long Beach Port threatens U.S. economic stability and impacts Trans-Pacific trade and failing to deter future attacks will harm U.S. interests. While it is *not* possible to attribute this attack currently, the dissemination of the malware kit online *poses an immediate potential threat to ports in over 30 countries which endangers the global economic system.* A rapidly deployed patch and successful multi-layered approach addressing our immediate, short, and long-term approach will mitigate the impact of future attack attempts and build strategic deterrence.

Background: On October 23 a cyber-attack against a widespread vulnerability the SEAFARER cargo management software corrupted manifests on three sea vessels that departed from Long Beach Port in California. The vulnerability could damage U.S. shipping processes at large, especially during the holiday season. Attackers exploited a Windows XP vulnerability affecting SEAFARER management software. After departing Long Beach Port in November, two vessels identified problems with their manifests while en route to Shanghai. One vessel's manifest did not correspond with containers taken in at Long Beach. Early indications are that *this attack is not limited to just American vessels and there is potential that it may impact dozens of other vessels internationally.*

On November 5, an unknown actor released a cache of sophisticated cyber weapons that threatens shipping entities utilizing SEAFARER systems. SEAFARER software is owned by Little Ocean Big Heart (LOBH), a major player in the shipping industry. LOBH maintains identification, tracing, and manifest systems for more 70% of the containerized and break-bulk cargo. The company handles more than 90% of gross tonnage for the Trans-Pacific market. If SEAFARER system malware is deployed, it could severely impact maritime trade between the U.S. and the Pacific region. 50% of global shipping passes through Asia by sea, and China's economy directs 33% of all world trade through the South China Sea.

Substantiation: We recommend a comprehensive multi-faceted approach to mitigate the immediate impact of this attack against U.S. values and interests. Our approach is designed to limit the potential of further attacks disrupting U.S. commerce, global supply chains, and the international economy. We recommend that the Department of Homeland Security (DHS) Cybersecurity Division spearhead the U.S. government response. DHS will work in tandem with USCYBERCOM's National Mission Teams (NMTs), the National Security Agency's (NSA) Cybersecurity Directorate, and the Federal Bureau of Investigation (FBI) Cyber Crime Division.

We propose a public-private approach, bringing together the DHS led-government response with private stakeholders including Microsoft, who runs the operating system; Symantec, for security expertise; and Cisco Talos, for forensic investigation. We attempt to move away from a *zero-defect approach* to focus on *strategic thinking, agility and innovation*. Private partners will be tasked with developing an immediate solution and patch to the Windows vulnerability. These

companies will also contribute to a mitigation process formulation led by DHS to train SEAFARER users in effective cyber hygiene procedures.

In the immediate term, we recommend that shipping companies cross reference software manifests with paper manifest copies. Container verification will diminish the impact of current attacks until a patch is in place. The U.S. federal government should facilitate inter-state, inter-agency, and public-private communication. The Department of State will act as the executive agent to liaise with other potentially impacted nations, and NSA and FBI will conduct cyber forensics and attempt to attribute the attack.[1]

In the short-term, we recommend that the Department of State engage with international partners to facilitate an international response that corresponds with the U.S. DHS-led effort to unite our partners under a clear set of common objectives. We also recommend that the DHS, NSA, FBI cyber teams, alongside CYBERCOM, engage with private sector and international partners to coordinate technical responses, build resilience, and deter future attacks.[2] Meanwhile, the NSA, CYBERCOM, and FBI should work towards attribution.[3]

In the long-term, the FBI criminal investigation and the Department of Justice should prosecute or indict the parties found responsible. An FBI criminal investigation will enable the Justice department to build an internationally accepted perception of legal normative costs for any actions that fall outside the boundaries of legal behavior in cyberspace and foster long-term deterrence.[4] This step also legitimizes potential retaliation, whether by conventional kinetic means or cyber operations. The criminal investigation sets the stage to provide definitions that allow the formation of legal codes that result in criminal convictions.[5] Furthermore, the results of the criminal investigation *underpin the emergence, acceptance, and internalization of institutional mechanisms that foster legal norms for the scope of actions that constitute legal behavior in cyberspace.*[6] The proposal also establishes a lower threshold in which the U.S. can legitimately respond with the full force of the U.S. criminal justice system to punish and deter other types of attacks.

These steps lay out a tactical and strategic path to protect and advance U.S. security and interests. They clarify government priorities and call for a multi-organizational technical response to mitigate impact of potential future attacks. The response addresses priorities and immediate steps to build up resilience to maintain normal global economic trade. It also calls for a U.S.-led coalition response alongside our allies and partners, which conveys a joint effort that fosters international cooperation and advances U.S. political legitimacy and norms in cyberspace.

---

[1] Under FISA, the government can gain evidence to attribute the attack and prosecute the attacker.
[2] Under the Third-Party Doctrine, individuals who give information to private companies have "no reasonable expectation of privacy" and the government can coordinate with private companies under this.
[3] Using methods such as PRISM and UPSTREAM, and under the Cybersecurity Act (2015).
[4] Under 18 USC 1030, the Computer Fraud and Abuse Act, various illegal behaviors related to computer use are outlined.
[5] Under USC 18 USC 2702, the Foreign Computer Crime Law, prosecution of a foreign actor is discussed.
[6] According to PPD-21, DHS "shall provide strategic guidance, promote a national unity of effort, and coordinate the overall Federal effort to promote the security and resilience of the Nation's critical infrastructure."

DECISION DOCUMENT – DAY ONE

DECISION DOCUMENT - CYBER 9/12, GEORGETOWN STIA STINGERS

Issue: SEAFARER Cargo Management Software Cyber-Attack.

Recommendation: Engage in inter-agency, international, and public-private collaboration to mitigate the immediate threat and prevent the further distribution and impact of the malware.

Policy Alternatives & Analysis:

1. Objective: Lead the mitigation effort via diplomatic means; U.S. government central coordinating agent to share threat information and ongoing mitigations efforts with allies and affected partners.
   Lead & Action: Department of State will lead diplomatic efforts to *bring allies and other partners together* to create a strategic multilateral dialogue to discern the nature of the threat and identify the threat actor. The Office of the Director of National Intelligence (ODNI) will *coordinate intelligence sharing* and vulnerability management with Five Eye partners to rapidly respond to the threat.
   Risk: Potential risk of loss of classified intelligence sources and methods. Diplomacy takes time to execute and domestic political environments can hamper the efficiency of this multi-lateral approach.
   Benefit: A U.S. led comprehensive and holistic policy serves to build an international political platform that contributes to building the international system's cyber resilience.

2. Objective: Immediately work to erode the potential ramifications and avoid escalation of the attack.
   Lead & Action: Deny international ships using BOLH software docking and connection to external networks. *Release an Executive Order* requiring all U.S. flagged vessels using BOLH to 1) implement paper manifest backups, 2) immediately patch or switch software, or if unable 3) stop shipping routes altogether. International flagged ships attempting to dock in the U.S. must also comply.
   Risk: Imposes high economic costs at a domestic and international level since it significantly slows or halts international trading routes. Its unilateral nature could foster diplomatic friction. Benefit: Lowers the threat of importing containers with unknown contents which can put US national security at risk and create bottleneck at ports. The U.S. has the economic heft to lead the international response to confront the threat.

3. Objective: Institute a central coordinating authority for inter-agency collaboration and public-private
   partnership to immediately develop a patch and execute a comprehensive mitigation

procedure.

Lead & Action: Department of Homeland Security (DHS) Cybersecurity & Infrastructure Security Agency (CISA) will lead *coordination between government agencies and private partners* to rapidly develop and deploy a patch for the Windows vulnerability and conduct back-end forensics analysis.

Risk: Potentially time consuming to coordinate which risks more attacks in the interim.

Benefit: Leverage public and private technical know-how to develop a patch. Rapid creation of patch limits economic and political impact of the attack. Forensic analysis enables attribution.

4. Objective: Attribution of attackers for prosecution to deter potential attacks by other actors.

   Lead & Action: The White House and Department of Justice jointly spearheads a public information campaign to "name and shame" the attackers to underscore the *U.S.'s determination to maintain a rules- based international system* that imposes legal costs on actions outside that order.

   Risk: Prosecution must meet high evidentiary thresholds. Sources and methods may be jeopardized in a public trial. Potential diplomatic friction due to public and unilateral nature of the action.

   Benefit: The policy builds a legal and diplomatic framework for the emergence, acceptance, and internalization of norms for the scope of actions that constitute legal behavior in cyberspace.

Justification of Recommended Policy Response:

- Erodes the possibility of long-term exploitation.
- Immediately mitigates economic impact through coordinated use of paper and backup records.
- Provides a comprehensive and holistic approach that provides flexibility as the situation evolves.

DECISION DOCUMENT – DAY TWO

SEAFARER CYBER INCIDENT UPDATE, GEORGETOWN STIA STINGERS

BLUF: Our recommended COAs clarify government priorities, call for a multi-organizational technical response to mitigate potential future attacks. and call for the U.S. to lead the international effort to re-establish normal international shipping activity.

Background: (ICOD: 0500Z 21MAR2020) Major ports around the Pacific Rim are experiencing technical difficulties with the SEAFARER software leading to massive backups and threatening shipping around vital chokepoints. The Automatic Identification System (AIS), is also experiencing malware which severely corrupts its data. Whether these two malware suites or attackers are related is currently unknown.

Policy Recommendations & Analysis:

Policy Alternatives & Analysis:

3. Objective: Establish high-level bilateral dialogue focused on threat information sharing, mitigate shipping bottle- neck, ensure safe navigation, and coordinate responses (Lead: State Department, i.e. applicable Diplomatic Missions. Timeline: five days to contact and establish coordination channels.)
   Recommendation: Immediately engage the most severely affected states including China, the Philippines, Malaysia, and Indonesia to clearly communicate the extent of damage, intended USG response, and (shareable) progress toward attribution and patching. (We remain willing to develop a multilateral framework in the long-term.)
   Key Risks: Risk the loss of classified sources and methods. Diplomacy always takes time and domestic political environments (esp. in China) complicates the successful execution of this approach.

4. Objective: Address the threat to AIS to prevent any at-sea collision or loss of life and minimize further disruption of international shipping lanes. (Lead: Federal Maritime Commission, domestic messaging, International Maritime Origination, international coordination. Timeline: 1-2 weeks)
   Recommendation: Ships immediately cease relying on AIS for navigation—AIS is primarily an identification system vice a navigation system (pursuant to the USCG Navigation Center for Excellence). The FMC and its sister organization at the UN, the IMO will disseminate this information to mariners and harbormasters and instruct them to rely on shipboard navigation equipment and V/UHF radio transmissions for hailing.
   Key Risks: The paramount risk to avoid is any maritime collisions—especially of large, difficult to maneuver, vessels such as oil or LNG supertankers, and especially in a choke

point or port.

5. Objective: Redouble our effort to understand both the malware and the threat actor(s) and develop mitigations for the new threats. (Lead: DHS CISA with analytical support from NSA and USCYBERCOM. Timeline: patching, likely 10-30 days; attribution, 30-60 days—longer to gather evidence for a federal indictment.)
   Recommendation: The Cybersecurity & Infrastructure Security Agency (CISA) will lead the government effort, leveraging technical support from NSA and USCYBERCOM, to advance technical responses, build resilience, and deter future attacks. Furthermore, CISA will serve as the locus for private sector coordination to develop and disseminate patches, and work to attribute the attack. If the Department of Justice determines that bringing federal charges are realistic, DHS will support DoJ's evidentiary gathering.
   Key Risks: tremendous administrative burden testing CISA's ability to coordinate both across federal, state and local government and among multinational corporations, in a highly time-sensitive environment. Delays in development and rollout will have extremely high economic costs (billions per day).

Justification of Recommended Policy Response:

- These represent achievable short-, medium-, and long-term goals to address a rapidly evolving threat.
- Allows ships to continue to navigate shipping routes, and reduces growing bottleneck at affected ports.
- Builds cyber resilience and a multilateral framework to respond to cyber-attacks affecting U.S. partners