CYBERNAUTS

Jordan Bresnahan, Shana Brouder, Matthew Dean, Julia Rapp

"Our ability to guarantee free and timely movement of goods...is vital to our economic and national security." - National Cyber Strategy, 2018

Overview:

Three concurrent threats are impacting international shipping: 1) Malware (designated SEASIQ) infected three vessels leaving the Port of Long Beach (POLB); inventory systems at POLB & allegedly Tuas Mega report similar issues; 2) Unknown actor threatened a ransomware attack against shipping; 3) 20% - 25% increase in demand peak shipping season.

Timeline:

11/1/2022 - China raises threat level for Strait of Malacca.
11/3/2022 - 3 vessels leave POLB with SEASIQ infected manifests.
11/5/2022 - SwipeUp ransomware threat posted.
11/8/2022 - POLB employees report inventory issues.

U.S. Objectives:

1) Maintain continuity of international shipping operations.

2) Prevent actor(s) from using malware to further exploit vulnerabilities within the U.S. shipping industry sector.

3) Reassure the relevant public/private sector stakeholders & enlist their cooperation in mitigating the threat.

4) Ensure the U.S. has adequate sealift capability to respond to its national security needs.

What We Know:

- The People's Militia (TPM) discussed a disruption on DarkNode, but credibility remains inconclusive.
- SEAFARER (found in 70% - 90% of the commercial shipping industry) is highly decentralized & customized by each shipping company; many vessels & ports using SEAFARER are operating a Windows OS that may have unpatched CVEs.

What We Don't Know:

- If malware on vessels & dockside are identical.
- If a proposed LOBH patch would remove SEAFARER vulnerability & how it could be implemented.
- Status of Vessel 3.
- Malware's origin and goal - criminal extortion or purely destructive?
- Connection of malware to Ipnos Security leak, if any.

What We Think:

- USB injection of malware means 1) The actor(s) placed the USB; 2) The actor(s) knew USB usage was necessary for loading vessels; or 3) Both.

Recommendations:

The subsequent policy recommendations are nested - enacting a succeeding option includes the actions in the preceding option. These options increase in intensity and take increasingly defensive/precautionary measures in the event the situation deteriorates.

We recommend moving forward with Policy Option 2 - Getting Ahead of SEASIQ

Policy Option 1 - Information & Monitoring:

- Diplomatic: Direct Sec. State through Embassy Beijing & ASEAN posts to provide information on the Chinese security increase; Direct Embassy Jerusalem to request assessment from Israeli government on Ipnos leak.
- Intelligence: DNI to mobilize all-source intelligence assets in the ASEAN region to assess 1) Extent of SEASIQ-induced damage; 2) Reasons for Chinese threat level increase; FBI to evaluate domestic intelligence concerning TPM especially size, structure, TTPs, & credibility of DarkNode thread.
- Logistic: Expand search for Vessel 3 using NRO, Navy/USGC; CISA to 1) Collaborate with LOBH on SEASIQ patching/replacement strategy; 2) Issue consequent CVEs & TLP Notices; Mobilize transport ISAC & domestic shipping stakeholders (including Port Authorities) to coordinate remedial actions.

Strengths/Opportunities:
- Collects actionable intelligence.

Weaknesses/Threats:
- Focuses only on remediation, not prevention.

Policy Option 2 - Getting Ahead of SEASIQ:

- DHS to lead an Interagency Task Force (ITF): To coordinate both public & private sector efforts on the investigation/response to SEASIQ.
- Diplomatic: Expand contacts with key partners in ASEAN region to alert them of possible spreading malware & potential disruption to shipping logistics.
- Logistic: ITF to 1) perform forensic analysis on infected USB device to ascertain what actions the malware carries out, how it spreads, identify the C2 servers, & TTPs to obtain a comprehensive assessment of recommended remediation actions, 2) coordinate with private sector to develop alternative methods to SEAFARER & how they could be implemented, & 3) communicate updates to relevant state & local governments.

Strengths/Opportunities:
- Mobilizes a cohesive "whole-of-government" response, which capitalizes on Agency/Department advantages.

Weaknesses/Threats:
- Keeps knowledge from the public, which poses a public relations risk.

Policy Option 3 - All Hands on Deck:

- Diplomatic: Raise issue publicly with International Chamber of Shipping regarding remediation of SEASIQ; Introduce UNSC resolution condemning malware exploitation & request assistance of all UN Member States to investigate this incident & take actions to identify the perpetrator(s).
- Logistic: MARAD to activate at least half of the Strategic Reserve Sealift in anticipation that this incident is a precursor to hostilities; Sweep U.S. merchant fleet & defense maritime assets for SEASIQ signature.
- Intelligence: DNI to mobilize all-source intelligence assets to monitor known major threat actors to assess attribution & possible preparations for additional cyber exploitation.
- Private Sector: Direct CISA to urge the private sector to remove SEAFARER & migrate to a remedial system.

Strengths/Opportunities:
- Guarantees American DoN capacity & continuity of operations.

Weaknesses/Threats:
- International recognition can potentially embolden actor(s).