WRITTEN BRIEF

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).

DECISION DOCUMENT – DAY 1

CYBERNAUTS

Jordan Bresnahan, Shana Brouder, Matthew Dean, Julia Rapp

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.

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.

Intelligence Assessment:
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.

Recommendation:
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 maritime 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.

DECISION DOCUMENT – DAY 2

CYBERNAUTS

Jordan Bresnahan, Shana Brouder, Matthew Dean, Julia Rapp

U.S. Objectives:

1) Maintain continuity of international shipping operations
2) Reassure the relevant public/private sector stakeholders & enlist their cooperation in reducing/ mitigating the threat
3) Ensure the U.S. has adequate and secure sealift capability to respond to its national security needs
4) Mitigate negative effects from exploitation of vulnerabilities within the U.S. shipping industry sector

Overview:
Since Nov. 1/2, saBOATeur infected ports and vessels across the globe and spread to other industries that interact closely with the shipping industry. On Nov. 15, the AIS system also suffered an intrusion that resulted in ships sailing virtually 'blind'. This has caused several minor vessel accidents and thousands of near misses. Financial markets contracted due to massive insecurity and uncertainty regarding the malware/ransomware. Global output has slowed 14.5% and is projected to slow by 25%.

Intelligence Assessment:
• U.S. and Indo-Pacific (namely China, Singapore, Malaysia, Indonesia, Japan, & South Korea) have been hardest hit by saBOATeur; Australia and Europe also reporting infected ports/vessels
• saBOATeur has affected LOBH system interfaces in drayage, freight, trucking, and at least one gantry crane linkage. • SEAFARER is built on a larger CIMS framework, which is likely infected with saBOATeur
• Credible evidence from IC highlights DPRK efforts to gain funding for its special weapons program

Short-Term (2-8 Weeks):
Invoke PPD-41:
• CISA to issue an advisory to Maritime, Service, and Supply Chain ISACs directing private sector users of the SEAFARER and CIMS system to immediately change all user passwords and stop attempting to remediate by utilizing data backups
• DoD to re-evaluate its naval systems to ensure firewall protections and airgap measures and ensure U.S. assets are secure and free of saBOATeur infection
• DoD to activate MARAD's Strategic Sealift
• Dept. of Treasury through FinCEN to monitor payments to DPRK
Diplomatic:
• IMO to implement a temporary AIS replacement using INMARSAT system
• Sec. State holds bilateral meeting with the Chinese Foreign Minister to ask why the Chinese initially raised their threat level and help communicate to the DPRK that their cyber attacks are needlessly provocative and should cease
• ASEAN Ambassador proceed to ASEAN regional forum to secure relations with member nations and enlist cooperation
• U.S. Embassy Japan to liaise with Port of Osaka to share information on SEAFARER replacement system
Domestic Reassurance:
• President to address the nation with the goal of calming financial markets, notifying the public about the cyber incident and explaining its effect on the U.S. economy, how our efforts to coordinate with international partners, the president's intention to support involved industries to prevent a recession, and provide an optimistic message that normal shipping operations will resume

Medium-Term (3-6 Months):
Domestic:
• DHS to contract LOBH with a sole-source grant to support full-spectrum remediation of CIMS
• ODNI to coordinate IC all-source intelligence assets to monitor known major threat actors to assess attribution & possible preparations for additional cyber exploitation
• Cyber Command to defend forward when enough credible and verifiable intelligence corroborates with high confidence attribution for the saBOATeur and AIS intrusions

International:
• U.S. Ambassador to the UN to address General Assembly on the persistent global threat saBOATeur presents, name and shame the perpetrator(s) once identified
• IMO to publish formalized protocols instituted during AIS outages and distribute among members

Long-Term (6 Months & Beyond):
Domestic:
• DHS to fund new public-private partnership to create alternative to SEAFARER system.

International:
• Dept. of State to obtain international cooperation to create a more reliable AIS system that will be administered by the IMO
• Share intelligence collection assets including space, under-sea based, and high-altitude UAV to maintain continuity of shipping operations, if necessary