AU 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 the USG is positively addressing the problem, including 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), and enlist collective assistance of all member states to take action against 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