November 26, 2018

TLP: WHITE - The NJCCIC assesses with high confidence that the maritime sector, to include ports, vessels, and shipping companies across the globe, will remain an attractive target for a range of cyber-attacks designed to disrupt daily operations, steal sensitive data, instill fear in the community, and hold critical operations hostage. In addition, the sector experiences disruptions and operational inefficiencies that impact the delivery of critical goods and services. This is particularly true for shipping companies, and vessels, or associated industrial control systems, such as damaged equipment, exposing the environment and public to harmful pollutants, global economic consequences, and even death or serious injury.

The 2018 Maritime Cybersecurity Survey conducted by Jones Walker LLC indicated that 80 percent of large US maritime industry companies surveyed reported that they were targeted by a cyber-attack within the past year. The survey results also revealed a false sense of overall cybersecurity preparedness, with 69 percent of respondents reporting the maritime industry as well prepared in cybersecurity, while only 36 percent believed their own organizations are well prepared. The misperception may stem from the relatively few disruptions within the maritime sector, or a sense of life or significant damage to the environment reported. Nevertheless, extensive vulnerabilities do exist within the MTS and numerous ransomware attacks have been reported by shipping companies, with many choosing to pay the ransom to avoid disruptions in their operational schedules. A cyber-attack has the potential to inflict substantial disruption to port and vessel operations and, due to the sheer volume of business conducted in ports worldwide, could result in grave monetary losses. With the maritime sector’s massive economic reach and the ever-growing advances in the technologies, it is expected that profit-motivated threat actors will continue to target maritime ports, shipping companies, vessels, and associated industrial control systems, such as damaged equipment.

In September 2018, two international maritime ports, Port of Barcelona, Spain and Port of San Diego, CA, suffered cyber-attacks. The Port of San Diego authorities reported a ransomware incident, later revealed to be an infection of the SamSam variant. Impacts were isolated to some of the Port Authority’s administrative functions and did not interrupt port operations or vessel movements. The Port of Barcelona did not immediately disclose the type of incident, but indicated the attack disrupted their internal IT systems, though it did not affect vessel or port operations.

In July 2018, the Port of Long Beach, CA suffered a ransomware attack which was contained and isolated to the China Ocean Shipping Company (COSCO) port terminal. COSCO, one of the world’s largest shipping companies, indicated the attack did not adversely affect vessel movements or operations.

In June 2017, US Maritime Alerts and Advisories indicated multiple instances of GPS interference reported by vessels operating in the Black Sea, and again in April and October 2018 in the Mediterranean Sea, specifically near Port Said, Egypt, the Suez Canal, and vicinity of the Republic of Cyprus.

In June 2017, A. P. Moller Maersk Group, the largest shipping company in the world, suffered a devastating attack as a result of the NotPetya malware. Maersk endured a ten-day halt in operations while it recovered from the attack, which required 4,000 servers, 45,000 PCs, and 2,500 applications be reinstalled.

Recommendations

The NJCCIC advises maritime sector stakeholders to take proactive steps to increase their organization’s overall cybersecurity preparedness and operate in a more resilient manner. Cybersecurity is no longer just a technology, but an integral part of everyday operations that must be integrated into the decision-making processes. As such, there is an overall lack of expertise. Awareness is vital in contending with existing vulnerabilities and due to the sheer volume of business conducted in ports worldwide, could result in grave monetary losses with the maritime sector’s massive economic reach and the ever-growing advances in the technologies. It is expected that profit-motivated threat actors will continue to target maritime ports, shipping companies, vessels, and associated industrial control systems, such as damaged equipment.

In September 2018, two international maritime ports, Port of Barcelona, Spain and Port of San Diego, CA, suffered cyber-attacks. The Port of San Diego authorities reported a ransomware incident, later revealed to be an infection of the SamSam variant. Impacts were isolated to some of the Port Authority’s administrative functions and did not interrupt port operations or vessel movements. The Port of Barcelona did not immediately disclose the type of incident, but indicated the attack disrupted their internal IT systems, though it did not affect vessel or port operations.

In June 2017, US Maritime Alerts and Advisories indicated multiple instances of GPS interference reported by vessels operating in the Black Sea, and again in April and October 2018 in the Mediterranean Sea, specifically near Port Said, Egypt, the Suez Canal, and vicinity of the Republic of Cyprus.

In June 2017, A. P. Moller Maersk Group, the largest shipping company in the world, suffered a devastating attack as a result of the NotPetya malware. Maersk endured a ten-day halt in operations while it recovered from the attack, which required 4,000 servers, 45,000 PCs, and 2,500 applications be reinstalled.

Maersk reportedly lost approximately $300 million in revenue. The attack, which required 4,000 servers, 45,000 PCs, and 2,500 applications be reinstalled, devasting attack as a result of the NotPetya malware. Maersk endured a ten-day halt in operations while it recovered from the attack, which required 4,000 servers, 45,000 PCs, and 2,500 applications be reinstalled. The attack affected nearly 40 different countries and was initially targeted at the shipping company’s management and control systems, however, it spread to other sectors. The attack resulted in the loss of $300 million in revenue and affected the company’s economies. The impact was also felt in the shipping sector, as many businesses faced delays and increased costs due to the disruption caused by the attack.

Traffic Light Protocol: WHITE information may be distributed without restriction.

References:

- US Coast Guard's Maritime Cybersecurity Framework, in
- US Coast Guard Maritime, Commons blog and US MARAD Maritime Security portal are recommended for accessing maritime cybersecurity alerts, advisories and notices. Maritime industry stakeholders are encouraged to continue bringing the gap in cybersecurity expertise by participating in their local Area Maritime Security Committee events and Cybersecurity Sub-committees.

New Jersey Cybersecurity & Communications Integration Cell
2 Schwarzkopf Dr., Ewing Township, NJ 08628
njccic@cyber.nj.gov
609.963.6300 / 7655

© 2015-2018 State of New Jersey. All Rights Reserved.