The Bottom Line

NOVEMBER 2022 | VOL. 155

ARE CYBER PIRATES THE NEXT THREAT TO SHIPPING?

Summary

A study by the Center for Advanced Defense Studies (C4ADS) found that the Russians are hacking the global navigation satellite system on a mass scale to confuse thousands of ships and airplanes about where they are.

Background

In February 2019, a deep draft vessel on an international voyage bound for the Port of New York and New Jersey reported experiencing a significant cyber incident impacting their shipboard network. An interagency team of cyber experts led by the Coast Guard responded and conducted an analysis of the vessel's network and essential control systems. The team concluded that although the attack significantly degraded the functionality of the onboard computer system, critical vessel control systems had not been impacted. Nevertheless, the interagency response found that the vessel was operating without effective cybersecurity measures, exposing essential vessel control systems to significant vulnerabilities.

On July 19, 2019, Stena Impero transited the Straits of Hormuz to pick up cargo in the Persian Gulf. The ship's regular course keeps it well within the Oman waters, away from the border with Iran. But on this occasion, the ship's crew experienced unusual deviations from their voyage plan and had to continuously adjust the vessel's course to stay on their intended path. As a result, Iran's Revolutionary Guard boarded Stena Impero, accusing it of colliding with a fishing boat and failing to respond to calls. Although Stena Impero's Swedish owner Stena Bulk said there was no evidence of the accusation, the tanker was detained for two months during a diplomatic crisis between Iran and western governments. The detention of the Stena Impero was widely seen as Tehran's retaliation for the UK detaining an Iranian tanker, Adrian Darya-1, two weeks before the Stena Impero was seized.

Current Status

GNSS comprises the constellation of international satellites that orbit Earth. The US's Global Positioning System, China's BeiDou, Russia's Glonass, and Europe's Galileo program are all part of GNSS. As a result, law enforcement, shipping, airlines, power stations, your phone, and anything dependent on GPS time and location synchronization are vulnerable to GNSS hacking.

Until the past couple of years, the Center for Advanced Defense Studies (C4ADS) thought the Russians used GNSS jamming or spoofing to disguise Putin's whereabouts.

One of the main cyber-dangers to shipping is the manipulation of navigation systems. This interference can result in the hacker sending false navigation information to the crew or incorrect information regarding the vessel's location to the shore-side team. Hackers can also gain access to monitoring and control systems. Because systems today are interconnected, this could result in hackers accessing anything from the water treatment system to the engine management system.

"In the summer of 2013, a research team from The University of Texas at Austin successfully hijacked the GPS navigation systems onboard an $80 million superyacht using a $2,000 device the size of a small briefcase," C4ADS said. "The experimental attack forced the ship's navigation systems to relay false positioning information to the vessel's captain, who subsequently made slight course corrections to keep the ship seemingly on track."

Communication is another vulnerable area. No communication onboard means that vessels in crisis cannot report critical situations.

Impact

The current state of cybersecurity aboard deep draft vessels is unknown. With engines controlled by mouse clicks, and growing reliance on electronic charting and navigation systems, protecting these systems with proper cybersecurity measures is as essential as controlling physical access to the ship or performing routine maintenance on traditional machinery. The maritime community must adapt to changing technologies and threats by recognizing the need for and implementing basic cyber hygiene measures.

Whether through spoofing GPS, or hijacking a ship's control system, the ability of a hacker to manipulate the movement of maritime vessels can cause billions of dollars of disruption, shock the global supply chain, increase the cost of goods, and even instigate international conflict.

RESOURCES:

Cyber Incident Exposes Potential Vulnerabilities Onboard Vessels (USCG)
Russians Hacking GPS System to Send Ships Bogus GNSS Data (Bus. Insider)
Cyber-Attacks: How Hackers are Targeting Seafarers (Ship Technology)
How Hackers are Targeting the Shipping Industry (BBC News)
Hackers Could Re-Create Ever Given Grounding in Suez Canal (Container News)