Hackers Target Port Facilities in Ransomware Attacks


As September drew to a close, international shipping ports in Barcelona, Spain and San Diego, California fell victim to ransomware attacks. These follow a successful attack on the China Ocean Shipping Company terminal at the Port of Long Beach this past July. This cluster of attacks should serve as a warning to the industry as a whole that there could be a hacker or hacker team targeting shipping companies and the facilities they rely on.

While the details on both attacks are slim, the Port of San Diego did confirm to ZDNet that it was in fact a ransomware attack, though they did not get any more specific than that.

Like most industries, maritime shipping is becoming more reliant on technology. Too often, that technology was not developed with security as a core concept, as shown in the increasing number of reports centered around the critical vulnerabilities in the industrial internet of things (IIOT). The shipping industry has turned to software and hardware solutions to outright handle, or at least assist with, tasks such as loading cargo and navigation while at sea. These types of high-tech hacks could have crippling effects on the shipping companies, individuals aboard the ships, and even national economies.

It seems that these recent attempts align more with standard ransomware attacks: hackers likely gained access through poorly patched networks with external facing vulnerabilities. The other likely vector is social engineering, where a successful phishing attack targeted a known network or software vulnerability.

Ransomware attacks can be absolutely devastating—look at the fallout of the Atlanta attack—and the massive amount of capital involved in literally moving the economy around the globe, the effects are amplified. Looking back, the NotPetya attacks heavily impacted the world’s top shipping company, Maersk, according to ZDNet paid out of $300 million in damages, with their IT staff having to “reinstall 4,000 servers, 45,000 PCs, and 2,500 applications in 10 days.”

Whether your organization has a single facility or maintains operations in a national or international capacity, it’s a good idea to review your cyberhygiene, and facilitate open lines of communication between operational and information security teams.