PORTS TARGETED IN RANSOMWARE ATTACKS

30 October 2018

The ports of Barcelona and San Diego both fell victim to cyber-attacks in September, as cyber criminals appear to be targeting the maritime industry.

The Port of Barcelona reported a cyber-attack on 20 September, although few details of the attack were made public. The port had initially warned that cargo may experience delays, however, the attack was contained and shipping was largely unaffected.

Just days later, the Port of San Diego in California revealed that it had suffered a ransomware attack. On 25 September, a cyber-attack disrupted the port's information technology systems, although operations were swiftly restored. Public access to some port services was affected, including park permits, public record requests and business services. The port, which operates cargo and cruise terminals and is home to hotels, restaurants, marinas and museums, confirmed that it had received a ransom note, although the value of the ransom demand was not disclosed.

Both attacks followed a ransomware attack against shipping company COSCO in Japan. The Chinese group said its vessels were not affected by the attack, although COSCO's terminal at the Port of Long Beach was impacted and customer communications were disrupted. Damage from the attack was reportedly contained because COSCO isolated its internal networks across its global operations, and because of ‘work-arounds’ that enabled cargo handling to continue without allowing the virus to spread.

Ports were also affected by the global malware attacks of 2017, which shut down terminals and disrupted shipping and cargo operations. Shipping company Maersk – which operates some 76 ports and nearly 660 vessels – was forced to switch off its global IT network. It took 10 days for the company to rebuild its entire network of 8,000 servers and 45,000 personal computers.

SMART PORTS

Unlike the 2017 attacks, which affected businesses indiscriminately, those against the ports of Barcelona and San Diego appear to have been targeted, according to Darktrace Industrial, which provides cyber security in a number of ports. The company speculates that the success of last year’s WannaCry and NotPetya malware attacks may have inspired attackers to pursue the maritime sector specifically.

Ports are likely to become more vulnerable to cyber-attacks with growing automation. Many ports and shipping companies are in the midst of a digital transformation – last year the port of Barcelona launched its Digital Port project with 64 initiatives to create digital applications, products and services. Shipping companies like Maersk and Mediterranean Shipping Company are investing in smart container technology that enables them to track and monitor shipments in real-time.

In the past, operating technology (OT), including industrial control systems, has been kept separate from wider IT systems, but it is increasingly becoming integrated. According to Darktrace, the creation of ‘smart’ ports and the convergence of OT and IT systems will challenge cyber security.

Maritime cybersecurity consultant Naval Dome warned that cyber-attacks against shore-based infrastructure, like that suffered by COSCO, could easily spread to ships. Shore-based and ship-based IT systems are linked, and can act as a gateway to vessels and leave them highly susceptible to cyber-attacks.

In the maritime sector, airspace is a gateway to vessels and leave them highly susceptible to cyber-attacks. The St Botolph Building, 138 Houndsditch, London EC3A 7AW Registered in England No. 1388956. A member of the Jardine Lloyd Thompson Group. Registered Office: The St Botolph Building, 138 Houndsditch, London EC3A 7AW Registered in England No. 1388956. © 2018 JLT Specialty Limited. All rights reserved.

Download Cyber Decoder

For further information, please contact Sarah Stephens, Head of Cyber, Content and New Technology Risks on cyber@jltgroup.com.