MAJOR MARITIME CYBER INCIDENTS

A REVIEW

Tuomas Kiiski, University of Turku, Finland

While profoundly transforming society and business, digitalization has also brought growing cybersecurity concerns. The maritime business depends increasingly on various IT systems both at sea and in ports. The Global Positioning System (GPS) and Electronic Chart Display and Information System are particularly vulnerable systems (1). Thus, ensuring the reliability of marine IT systems and their data is becoming increasingly important.

Reports on cyberattacks—malicious intrusions through the digital environment to access delicate information—against various societal and business targets have appeared regularly in the media. The maritime sector has been exposed also, but information about these incidents remains scant. This article aims to depict these events in more detail. The events are divided based on their targets. In practice, such categorization is a simplification, as attacks may simultaneously involve multiple targets.

ATTACKS AFFECTING PORTS

From 2001 to 2017, at least six incidents that affected ports directly can be traced. The attacks typically focus on the cargo management systems of port operators. On 20 September 2001, a denial-of-service (DOS) attack, allegedly created by a teenager, temporarily shut down the Port of Houston (2). In August 2011, the Iranian shipping line IRISL was hit by an attack causing substantial damage (3). Between 2011 and 2013, cargo management systems of the Port of Antwerp were manipulated during a drug trafficking operation (3).

In 2014, the US Coast Guard revealed that the GPS systems of four port cranes at an undisclosed port in the USA were jammed in an incident lasting 7 hours (4), and a DOS attack was reportedly launched against the administrative systems of the Port of Oakland in 2016 (5).

In summer 2017, the NotPetya ransomware initially hit several Ukrainian governmental and business targets before spreading globally, affecting e.g. APM Moller Maersk's terminals at some 80 locations, reportedly causing damages of up to US$300 Million (6).

ATTACKS AFFECTING SHIPS OR SIMILAR

Ships at sea are also susceptible to cyberattacks. Modern navigation relies on positioning systems, which has led to fears of jamming or altering location coordinates. An activity called spoofing refers to sending false data to navigation systems. In 2013, a test verified the possibility to spoof a cruise ship's navigation system (7). Two alleged but unconfirmed incidents, both involving a large number of vessels, have occurred: in 2016 near South Korea, and in June 2017 in the Black Sea (8).

In two other incidents, serious hacker involvement is suspected. In 2010, an oil rig on a voyage from Korea to South America suffered a delay of 19 days due to a system shutdown off the coast of Africa (3). In

February 2017, a German containership reportedly lost control of its navigation systems for 10 hours while sailing from Cyprus to Djibouti (9).

ATTACKS AFFECTING OTHER MARITIME RELATED ORGANIZATIONS

Other maritime stakeholders have also become victims of cyberattacks, including maritime authorities, shipbuilders, ship owners and maritime consultancies. At least three maritime authorities have been struck: the UK Maritime and Coastguard Agency in 2004, the Australian Customs and Border Protection Service in 2012, and the Danish Maritime Authority also in 2012 (10; 3; 2). In 2013, two Korean shipbuilding companies were subjected to malware called "Icefog" (11). In 2016, the French naval contractor DCNS suffered a leak of new submarine construction plans (12). In 2017, ship owner BW Group and maritime consultancy Clarksons reported breaches in their IT systems (9).

EMAIL FRAUDS

The maritime sector is also vulnerable to a common type of threat arising from email communications. Email fraud is usually orchestrated through either the hacking of maritime executives' email accounts or identity theft executed in some other way. Phishing refers to criminal activity used to obtain delicate information, such as bank accounts, or to solicit fake invoices. There have been several reported incidents involving shipbrokers, charterers and suppliers, which often resulted in substantial financial losses (5).

THE WAY AHEAD

Consequently, the plan to include of cybersecurity guidelines into IMO's International Safety Management code by 2021 is a welcome effort, albeit a belated one to say the least. Similarly, classification societies have started to introduce ship cybersecurity regimes (13). At the same time, all of the above efforts emphasize the need for adopting cybersecurity into the ISPS code.

Cybersecurity should not be considered solely as a technical issue; rather, a more holistic approach is needed. A recent cybersecurity survey by IHS Fairplay (9) underlined the role of crew training in mitigating cyber threats. Therefore, effective cybersecurity capability must possess ambidextrous features covering both the technological and the human side.

CONCLUSION

The findings show that the number of incidents is by no means trivial: over a dozen attacks around the world with various levels of consequence have occurred over the past 17 years. Very likely these incidents are but a small part of the whole, with some victims preferring not to publish their involvement in such incidents. Even this rather short review makes clear that cyberattacks take multiple forms, regardless of whether they are successful, in terms of coverage, methods used and parties involved. In the future, the importance of cybersecurity will be accentuated if and when more autonomous ships are deployed.

REFERENCES

1) IHS Fairplay (2016) IHS Fairplay Maritime Cyber-security Survey – the results. https://fairplay.ihs.com/article/4275151/ihs-fairplay-maritime-cyber-security-survey-the-results
2) RISI (2015) RISI Online Incident Database. http://www.risidata.com/Database/
3) Kaspersky Lab (2015) Maritime industry is easy meat for cyber criminals. https://www.kaspersky.com/blog/maritime-cyber-security/8796/
4) Newman, L. H. (2015) What if a Cybersecurity Attack Shut Down Our Ports? http://www.slate.com/articles/technology/future_tense/2015/05/maritime_cybersecurity_ports_are_unsecured.html
5) Belmont, K. B. (2016) Maritime Cybersecurity: Cyber Cases in the Maritime Environment. http://www.ahcusa.org/uploads/2/1/9/8/21985670/k._belmont_-_aapa_maritime_cybersecurity_final.pdf
6) Milne, R. (2017) Moller-Maersk puts cost of cyber attack at up to $300m. https://www.ft.com/content/a44ede7c-825f-11e7-a4ce-15b2513cb3ff
7) Psiaki M. L. and Humphreys T. E. (2016) Protecting GPS From Spoofers Is Critical to the Future of Navigation. http://www.spectrum.ieee.org/telecom/security/protecting-gps-from-spoofers-is-critical-to-the-future-of-navigation/
8) Reuters (2017) Cyber threats prompt return of radio for ship navigation. https://www.reuters.com/article/us-shipping-gps-cyber/cyber-threats-prompt-return-of-radio-for-ship-navigation-idUSKBN1AN0HT
9) IHS Fairplay (2017) Outlook 2018: Cyber attacks remain a major threat. https://fairplay.ihs.com/safety-regulation/article/4295476/outlook-2018-cyber-attacks-remain-a-major-threat
10) Maritime Denmark (2014) The DMA attacked by hackers. http://maritimedenmark.dk/?Id=17968
11) Mimoso, M. (2013) Icefog espionage campaign is hit and run targeted operation. https://threatpost.com/icefog-espionage-campaign-is-hit-and-run-targeted-operation/102417/
12) Siegel, M. and Irish, J. (2016) Data on India's new submarines were hacked, and it could be an act of 'economic warfare'. http://www.businessinsider.com/france-dcns-india-submarine-data-leak-may-be-economic-warfare-2016-8?r=US&IR=T&IR=T
13) MarineLink (2018) Kongsberg Earns First DNV GL Cyber Security Type Approval. https://www.marinelink.com/news/kongsberg-security430915

ABOUT THE AUTHOR

Dr. Tuomas Kiiski is a Research Manager in Turku School of Economics at the University of Turku, Finland. He also holds a M.Sc. and a B.Sc. in Economics and Business Administration and a BBA in Business Logistics. His main research interests are in maritime economics and Arctic shipping.

ABOUT THE ORGANIZATION

This article was produced as part of the HAZARD Project, which aims to mitigate the effects of major accidents and emergencies at major seaports in the Baltic Sea Region. Port facilities are often located close to residential areas, potentially exposing many people to the consequences of accidents. The HAZARD project deals with these concerns by bringing together rescue services, other authorities, logistics operators and established knowledge partners. HAZARD enables better preparedness, coordination and communication, and more efficient actions to reduce damages and loss of life in emergencies, and enhances the handling of post-emergency situations by making a number of improvements. The HAZARD project has 15 full partners from five countries and a total budget of 4.3 million euros. It is scheduled to run from spring 2016 to spring 2019, and is part-funded by the EU's Baltic Sea Region Interregional programme.

ENQUIRIES

Turku School of Economics at
the University of Turku
Operations & Supply Chain Management
20014 University of Turku, Finland
Email: tuomas.kiiski@utu.fi
Web: blogit.utu.fi/hazard