# Noticeable cyber attack cases which have affected the maritime industry in recent years

Jakob P. Larsen, Head of Maritime Security, BIMCO

6 March 2019

# Virus in ECDIS delays ship’s departure

- Technical problem
- No paper charts on board
- Maker’s technician called in
- Virus discovered and isolated
- Virus isolated and ECDIS computers restored
- Deleays cost hundreds of thousands USD

# Crash of integrated navigation bridge

- Ship experienced failure of nearly all systems at sea, in dense traffic and reduced visibility
- Ship had to navigate for two days using paper chart and a stand-alone radar to reach port
- Maker’s technician had performed software updates of navigation software running on ship’s computer
- Outdated operatingn system was unable to run the updated software, and crashed
- Extensive cost was incurred

# Worm attack on maritime IT and OT

- Onboard power management system connected to the internet to allow for software update, remote diagnosis, data collection and remote operation
- Company IT department performed vulnerability scan and discovered a dormant worm that could have activated when ship was connected to the internet
- Worm believed to originate from maker’s service technician
- Worm spread via USB into a running process which executes a program in the memory
- Worm had spread to all servers and associated equipment and was undiscovered for 875 days

# Ship agent/shipowner ransomware incident

- Shipowner reports ransomware attack
- Source was two independent, unwitting ship agents
- Seperate ports and seperate occasions
- Affects limited to business networks
- Ships not affected

# Main application server infected by ransomware

- Ransomware infection on the main application server of a ship caused complete disruption of the IT infrastructure
- Ransomware encrypted all essential files and data was lost
- After restoration, the incident re-occurred
- Poor password policy enabled attackers to log on via remote management services
- The undocumented user was deactivated and stronger password policy was introduced

# [Maersk NotPetya attack]

- I will also show a few slides explaining about the impact, the investigation and the lessons learned of the NotPetya attack experienced in 2017 by Maersk Line. These slides will not be distributed in electronic nor hard copy.

# Q & A