Norwegian Maritime Cyber Resilience Centre

NORMA CYBER

Our Vision:

Unified resilience against cyber threats for Norwegian Shipping and Maritime Sector

Our Values:

Trusted

Solid

Innovative

Our Set-Up:

Mutually owned by Norwegian Shipowners and Operators

DEN NORSKE KRIGSFORSIKRING FOR SKIB
GJENSIDIG FORENING
The Norwegian Shipowners' Mutual War Risks Insurance Association

Norges Rederiforbund
Norwegian Shipowners' Association

History

November 2019

Joint initiative by DNK and Norwegian Shipowner Association

Pre-project started

March 2020

Project group established

3 personnel

Fact Finding – input from members and others

October 2020

Board approval from DNK and Norwegian Shipowners Association.

NORMA Cyber will be established as a Joint Venture

January 2021

NORMA Cyber starts operations

June 2021

Security Operations Centre (SOC) service operational

Current Status

81 Member organisations

Represented with 1956 Vessels

Services:

- Intelligence & information sharing
- Response
- Security Operations

9 Employees

Offices and Operations Room in Oslo, Norway

NORMA Cyber members as of 20 September 2022: 82 members – 2 024 vessels

SOC Service:
4 members
80 vessels
3 000 land-based staff

Membership Services

Intelligence & Information Sharing

Decision Support to members

- Effective information sharing to/from members
- Monthly Threat Assessments
- Intelligence reports
- Tippers
- OT Vulnerability notifications
- Mitigation advice
- MISP portal – indicators of compromise sharing

Monitoring & Detection

External Monitoring

- Deep/dark web monitoring
- Vulnerability scanning of internet facing systems
- Warnings/Alerts to individual members

Managed Security Operations Centre

- Vessel IT/OT
- Land-based/Cloud infrastructure
- 24/7/365 - Early alerts to members before incident escalates

*Additional Service – extra cost

Response

Incident and crisis support to members

- Mitigation advice
- Crisis response advice
- Coordination between members, authorities and other stakeholders
- Provide and manage recourses
- Participate in exercises and provide scenarios

Analysts available for members, Member log-in portal, Webinars / Seminars, User Council

Annual Threat Assessment 2022

Nation state actors

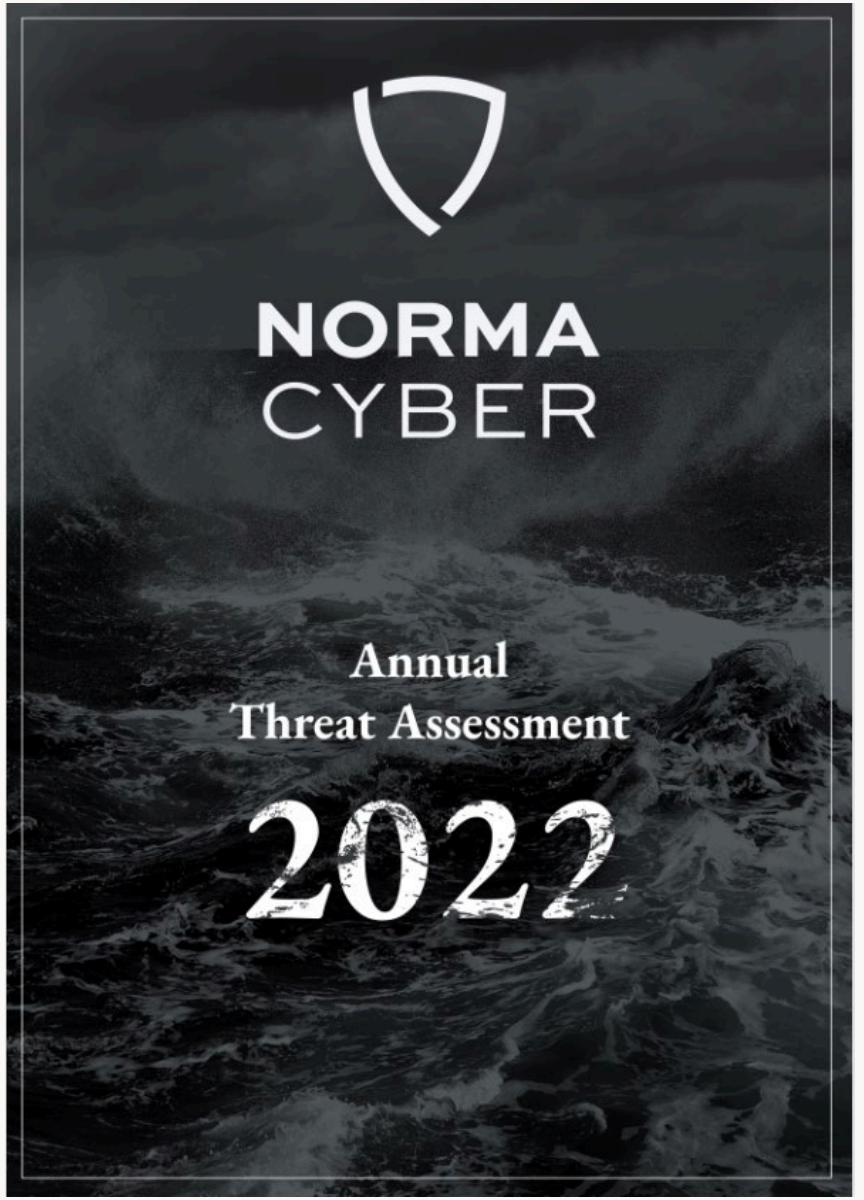
- The espionage threat from Russia- and China-linked threat actors
- Regional conflicts and the impact on merchant shipping
- GNSS interference
- Manipulation of AIS data in vessel tracking services

Cybercrime

- Fraud
- Ransomware

Hactivists

Operational technology



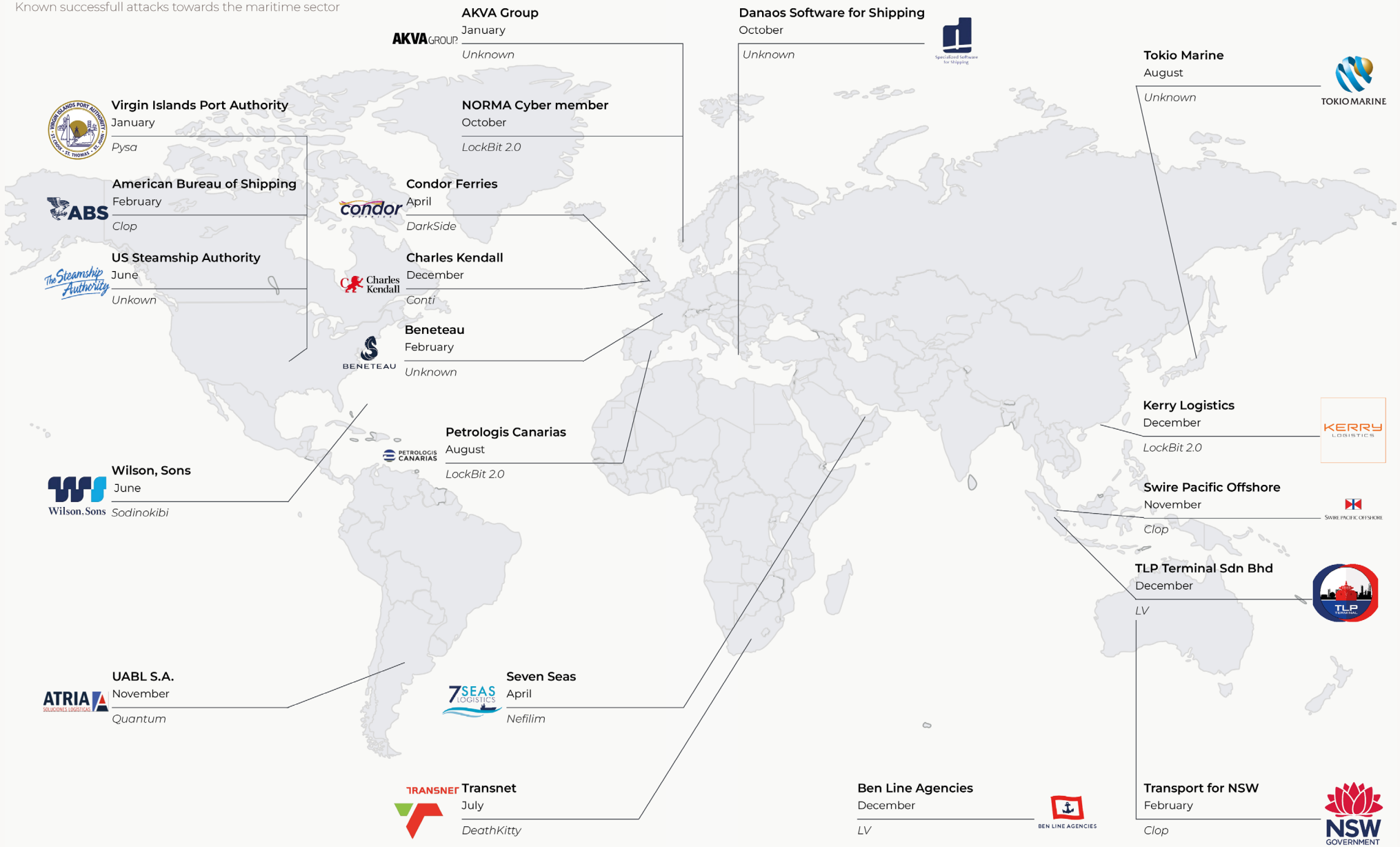
Take-aways

- Stage 3:
  - Out of 88 e-emails, 49 are caught by the **spam filter**
  - Still, 6 **people** click the link while the malware site is active
  - Out of the 6 clicks, 2 downloads are blocked by the **firewall**
  - Out of the 4 remaining downloads, 3 **people** open the excel document and enable macros
  - In the remaining 3 cases, the malware either fails to execute properly or is blocked by the **firewall** due to activity towards known malicious IP's

In this case, the **antivirus** failed to identify the malware. Only 5-11 out of 60 antivirus programs would block the Excel-documents at the time. **They should have now been updated**

Ransomware in 2021

Known successfull attacks towards the maritime sector



Stop talking about Cyber!

Contact information

NORMA Cyber OPS:

ops@normacyber.no

24/7 Incident and Crisis number: +47 90 98 97 37

Administrative queries:

contact@normacyber.no

Questions?