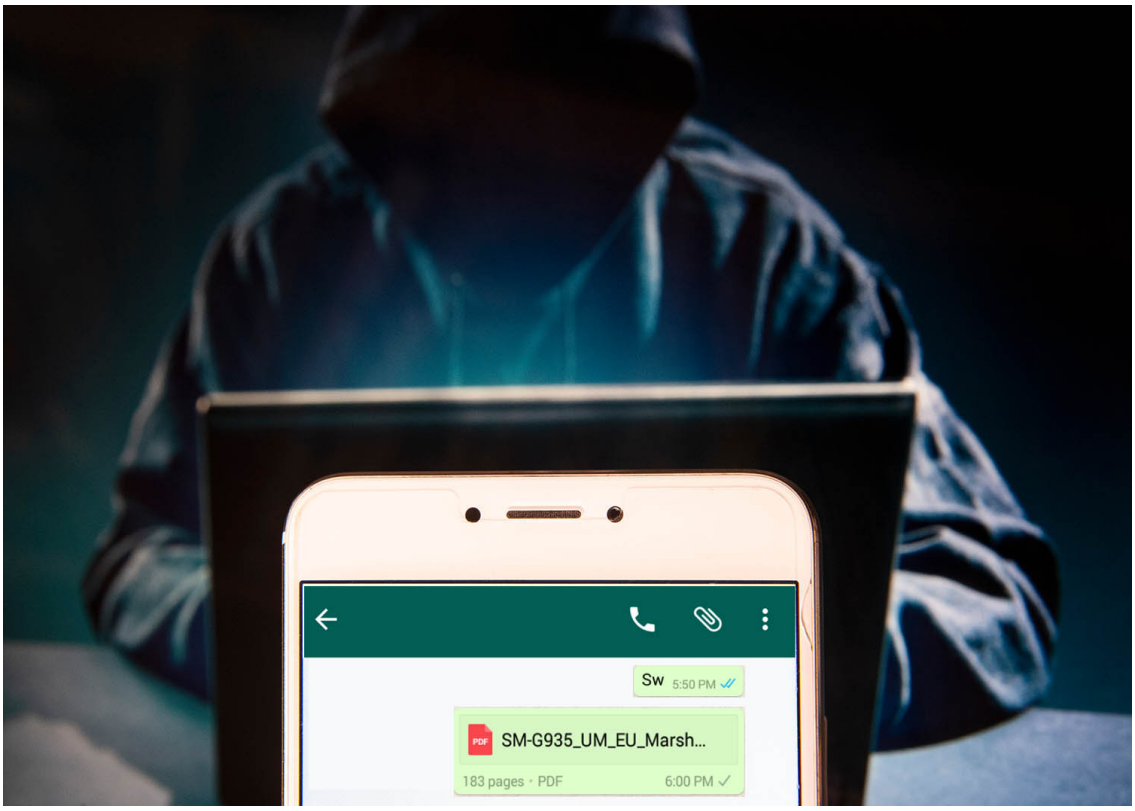

Maritime industry targeted by cyber criminals

An assessment by Norwegian authorities finds that its maritime and oil and gas sectors have recently been victims of cyber campaigns specifically targeting companies in the US, Europe and the Middle East and advise companies to be prepared for continuous activity in the short to medium term.

Published 22 August 2019

In a recent NMD_CyberRisk.pdf to the maritime sector, the Norwegian National Security Authority (NSM) advises of an increase in the number of cyber campaigns targeting several different sectors since June 2019 and states that both the maritime sector and the oil and gas sector have been victims of such targeted attacks.

To this date, the campaigns have used social engineering techniques in e-mails and in personal messages through social media, primarily LinkedIn, but also WhatsApp and Facebook Messenger to:

• install malware on the user's computer;

• gather information about the user, their employer or other users connected to them; and

• further spread the campaigns.

While the scope of these campaigns and the subsequent incidents are reportedly global, " *companies in the United States of America, Europe, and the Middle East have been the main targets* ", says the NSM. It also establishes that the threat actors have demonstrated high ability and capacity to conduct their operations.

Based on the current situation and the risks found, the NMS advises companies and organisations to be prepared for attempts of cyber activity with malicious intent in the short to medium term. It also states that both obvious and less obvious companies may be affected, which means all types of ships as well as shipowners' land-based infrastructure can be vulnerable to cyber incidents. In a statement of 19 August 2019 , the Norwegian Maritime Authority (NMA) further emphasizes that: " *Especially shipowners that operate in ISPS/MARSEC level two areas or higher should be aware of the situation .*"

Recommendations

Although the NSM's information letter is directed at Norwegian companies, we advise all ship operators and companies with responsibility for infrastructure onboard ships to continuously monitor and review digital security and to follow the recommendations made, including:

• Make sure networks are segmented. There should be no physical connection between administrative and operative parts of the network.

• Log activity at all endpoints and in the network. The NSM recommends keeping logs for at least six months.

• Use encrypted communication where possible, also between ships and land-based infrastructure. Manipulation of communication can easily be done if it is not encrypted.

• Restrict access to information and systems in accordance with people's position and role. Restriction of access will in most cases limit the consequences after an incident.

Among the recommended counter-measures, the importance of carrying out cyber security awareness training is highlighted. All 'users', including seafarers, shore staff and other relevant personnel, should:

• Be aware of, and be critical to, emails with links or attachments.
If there are any doubts whether an attachment or a link is safe to open – assess whether it is necessary to open it at all. Report suspicious emails or messages that relate to the company to your employer.
Be careful with documents that suggest enabling macros in Word, Excel or PowerPoint.

• In social media:
Report suspicious messages received through social media, in particular if they can be connected to your employment or the company in general.
Establish and maintain contact only with people whose identity can be verified.
Be very critical to messages with links and attachments in social media, this is the new target arena.
Expect that everyone can see all information shared on social media about work and your private life.
Do not publish work-related information without the consent of your employer.
Do not publish information about other individuals without their consent.
Enable available security settings in products and applications.
Do not reuse the same password across services.
Become a Security
STAR
: Every time you suspect an attack or are unsure of what to do,
S
top –
T
hink –
A
sk –
R
eport

Ship operators should also pay close attention to any cyber security advice provided by their national security authorities. As an example, Norwegian companies are advised to follow the NSM's " Fundamental principles for information and communications technology (ICT) security " as well as its " Measures and recommendations concerning social media " (both are in Norwegian only). We also recommend ship operators and seafarers to report all suspicious activity and breaches of security to their flag administrations and/or national security

shareholders, correspondents, or other contributors.

authorities, as this will support their work to monitor ongoing cyber threats and risks.

Additional guidance

For additional recommendations related to cyber risk management, please refer to our publications " Ship operators cannot afford to turn a blind eye to cyber security " of 10 July 2019 and " It is time to strengthen your onboard cyber security procedures "of 12 December 2018. Our loss prevention awareness video produced in cooperation with DNVGL may also be useful in terms of carrying out awareness training.

Ship operators are also reminded that cyber risks must be appropriately addressed in ships' existing safety management systems, as defined in the ISM Code, no later than the first annual ISM audit after 1 January 2021. Guidelines and best practices for implementation of cyber risk management are described in IMO's MSC-FAL.1/Circ.3 , as well as in the industry guidelines " Cyber security onboard ships ".