NASJONAL
SIKKERHETSMYNDIGHET

Information regarding the cyber risk in maritime sector

The Norwegian National Security Authority (NSM) is a cross-sectoral professional and supervisory authority within the protective security services in Norway.

The National Cyber Security Centre (NCSC) is a part of NSM, and is continuously following and analysing situations that in the cyber domain can affect or have affected Norwegian companies and organisations.

NSM NCSC has since June this year received information about cyber campaigns targeting several different sectors. The scope of these campaigns and the following incidents have been global, but companies in the United States of America, Europe, and the Middle East have been the main targets. The threat actors have demonstrated high ability and capacity to conduct their operations. It has been reported attempts of digital activity with malicious intent against some companies.

Based on the information NSM NCSC has received, NSM NCSC, the Norwegian Maritime Authority, and the Norwegian Shipowners' Association assess that the maritime sector and the oil and gas sector have been victims of targeted campaigns. Companies and organisations should be prepared for continuous activity in the short to medium term.

These campaigns can affect both obvious and less obvious companies. NSM NCSC, the Norwegian Maritime Authority, and the Norwegian Ship owners' Association assess that all types of ships and ship owners' land-based infrastructure can be vulnerable to cyber incidents within the maritime sector. Especially ship owners that operate in MARSEC level two areas or higher should be aware of the situation.

NSM NCSC urges ship owners and employees within the maritime sector to show increased vigilance and to follow and implement the measures given in attachment 1. All suspicious activity should be reported to the Norwegian Maritime Authority and the Norwegian Shipowners' Association. If the suspicious activity appears to be similar to the campaigns described in attachment 2 or other types of cyber activities, a copy should be sent to NSM NCSC. NSM NCSC can be contacted 24/7 at the phone number 02497 and at the email address norcert@cert.no. If calling from abroad, please use the following phone number: +47 23 31 07 50.

With regards,

The Norwegian National Cyber Security Centre

NASJONAL SIKKERHETSMYNDIGHET

Attachment 1: Recommended measures

NSM recommends all companies to follow NSM's fundamentals principles for ICT security (only in Norwegian)[1], and its social media guidelines (only in Norwegian)[2,3].

Ship owners and other companies are recommended to sign up to NSM NCSC's email list (only in Norwegian) to keep up to date in the cyber domain. Please send an email to post@cert.no to sign up.

In addition, ship owners and companies can ask for a technical mapping of their own level of security through NSM's free service called Allvis NOR[4]. Allvis NOR performs technical vulnerabilities scans towards selected, agreed upon services exposed to the Internet. Interested parties can send an email to pentest@nsm.stat.no.

NSM NCSC recommends the following measures based on the current situation and risks:

To ship owners and companies with the responsibility for infrastructure on ships:

- Segmentation of the network. There should not be a physical connection between administrative and operative parts of the network.
- Log activity on all endpoints and in the network. NSM NCSC recommends keeping logs for at least 6 months.
- Use encrypted communication where it is 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 to people that require it due to their position and role. Restriction of access will in most cases limit the consequences after an incident.

Every company associated with Norwegian interests or that manages risk-exposed values, are recommended to perform continuous security monitoring. If the company lack the capability or the possibility to perform such monitoring, NSM has accredited some Norwegian managed security service providers as a part of the NSM national scheme[5].

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 – make an assessment if opening it is necessary. 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:

- Suspicious messages received through social media should be reported to the employer 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 critical to messages with links and attachments in social media.
- Expect that everyone can see all information shared on social media about work and your private life.
- Do not publish work-related information without consent from 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.

[1] https://www.nsm.stat.no/globalassets/dokumenter/nsm_grunnprinsipper_for_ikt-2018.pdf
[2] https://www.nsm.stat.no/globalassets/dokumenter/brosjyrer/socialmedia_web.pdf
[3] https://www.nsm.stat.no/blogg/podcast---some-og-sikkerhet/
[4] https://www.nsm.stat.no/om-nsm/tjenester/sikker-kommunikasjon/allvis-nor/
[5] https://www.nsm.stat.no/om-nsm/tjenester/leverandorforhold/kvalitetsordning-for-bruk-av-leverandorer-av-tjenester-innen-ikt-hendelseshandtering/

Attachment 2: Observed campaigns

NSM NCSC has observed the following campaigns lately.

Social media abuse

In one campaign, a threat actor used LinkedIn to deliver malware after the user had accepted the connection request. NSM NCSC has observed this to be a common approach for threat actors to deliver malware. LinkedIn is a platform that is easy to use to map key personnel within a company and to delivery of malware. The security firm FireEye has described such a campaign in one of their recent blog posts[6].

After a user has accepted a LinkedIn request, the person who is behind the request, if default settings have not been changed, has access to the user's entire contact list. This list can be used to send invitations to other LinkedIn users. The information gathered from different profiles could be used to describe personal and work-related interests, work location, age, position in the company, contact information such as email addresses and phone numbers, education, trainings, security clearances, pictures, personal opinions, political affiliation, family relations, and more.

In addition, one individual does not need to list its employer on LinkedIn for a threat actor to derive sensitive information from the profile. If the threat actor has access to several profiles, he can use the information to perform human or technology based intelligence operations as a next move. This will lead to a higher exposure of vulnerabilities for both individuals and the company.

Emails with links or attachments that can install malware

In another campaign recently observed, the threat actor used emails that pretended to be from an already known company. The emails were sent from a person or a company that the receiver already knew, and looked like a common invoice. In some cases, these invoices will cause a malware to run on the computer if the link or the attachment is opened. In other cases, the threat actor could be seeking to map the person or the company.

These kind of emails can be hard to separate from legitimate emails or regular spam emails. NSM NCSC recommends everyone to be careful with opening an email from unknown senders, especially if they have links or attachments. In several email clients, it is possible to hover over a link with the mouse to check if it is the expected link to the legitimate site. It is also possible to check whether the sender's email address is spoofed. The threat actors will mainly try to use new vulnerabilities in systems and programs. Because of this, NSM NCSC recommends all users to install the newest security updates and versions for programs and operating systems to keep themselves as secure as possible.

[6] https://www.fireeye.com/blog/threat-research/2019/07/hard-pass-declining-apt34-invite-to-join-their-professional-network.html