CENTRE FOR
CYBER SECURITY

Threat assessment:

The cyber threat against operational systems on ships

Threat assessment: The cyber threat against operational systems on ships

The purpose of this threat assessment is to inform public authorities and shipping companies of the cyber threat against operational systems on Danish-flagged ships. Cyber attacks may affect operational systems, and thus threaten safety of navigation and overall ship security. This assessment supplements the general assessment of the cyber threat against the Danish maritime sector, and may serve as input to shipping companies' risk assessments.

April 2020
1st edition

Danish Defence Intelligence Service
Kastellet 30
DK-2100 Copenhagen

Tel.: +45 33 32 55 80
E-mail: cfcs@cfcs.dk
www.cfcs.dk

Key assessment

- The Centre for Cyber Security (CFCS) under the Danish Defence Intelligence Service assesses that the collective threat from cyber attacks against operational systems on Danish ships is **HIGH**.

- Financially motivated cybercriminals, in particular, pose a threat to operational systems on ships. Cybercriminals do not have a specific interest in operational systems on ships, but they conduct opportunistic attacks against targets across sectors.

- Operational systems are also threatened by single individuals, who by technical interest or sheer curiosity attempt to gain access to these systems.

- Treat actors may exploit compromised equipment suppliers as stepping stones to attack operational systems on ships.

- There is a potential threat from destructive cyber attacks from state actors against operational systems on ships. The threat may be higher to ships, who operate in certain areas of conflict or if the shipping company conducts business with companies or states, who are targets of destructive cyber attacks.

Introduction

Digitalization and connectivity make ships vulnerable

Until 15-20 years ago, ships were isolated units that primarily communicated via VHF radio and a narrow satellite connection. Operational technology and systems responsible for propulsion, navigation, steering, etc. were physically isolated from the Internet. However, vessels are no longer isolated due to digitalization combined with cheaper and better communication lines at sea.

Ships operational systems have typically been segregated (segmented) from internet-connected administrative networks, and have thus been better protected against cyberattacks. However, the isolation and segmentation of these operational systems are increasingly being penetraded by connections to ships' administrative systems and on to its onshore offices. Additionally, equipment suppliers more often have access to monitoring and update of the systems. update of the systems.

Operational systems

In this assessment, operational systems on ships entails systems that make the ship operational and safe at sea. This includes systems for propulsion, navigation, steering and communication. These systems are commonly referred to as operational technology (OT).

This development has rendered many business advantages for shipping companies and equipment suppliers, but it also enables cyber attacks from actors, who can exploit the vulnerabilities generated by digitalization and Internet-connectivity. Operational systems on ships are particularly vulnerable if installation of new systems or changes in the segmentation occur with little or no focus on cybersecurity.

Cyber attacks against operational systems on ships may deliberately or inadvertently affect the operation of the systems, and thus impact the safety of navigation and general security of the ships. Consequently, it is relevant for shipping companies to include the threat from cyber attacks in the risk assessments of individual vessels.

Unreported incidents challenge the assessment process

Public reports on cyber attacks against operating systems on ships are generally limited. There is likely several explanations to this. One could be that the segmentation and cybersecurity in general is so solid that cyber attacks against operational systems are difficult to conduct. Another explanation could be that the typical threat actors, who usually target administrative systems, simply lacks interest in these operational systems.

However, behind the low number of reported incidents, there are probably significant unreported incidents as shipping companies are either reluctant to report and speak in public about the incidents or because the attacks have gone unnoticed. Many shipping companies. do not monitor or scan their operational systems, raising the probability of unidentified malware.

On February 1st 2019, a new Order came into force directed at Danish-flagged ships operating under the International Safety Management Code (ISM). According to the Order, all shipping companies must now notify the Danish Maritime Authority and CFCS of cyber incidents that may affect safety and navigation of ships.

This threat assessment is primarily based on publically reported cyber incidents and information from partners and actors within the Danish maritime industry.

The cyber threat

CFCS assesses that the cyber threat against the operational systems on board Danish ships is **HIGH**. This entails that within the next two years, the operational systems on board one or several of the 700 Danish-flagged merchant ships will likely become target of a cyber attack. The threat reflects the numerous examples of such attacks seen across the world. The threat also applies to ships operated by Danish shipping companies sailing under foreign flags.

It is likely that operational systems on ships are subject to cyber threats from a number of different actors whose intentions and techniques vary. Irrespective of intentions and techniques, any type of attack against operational systems on ships may affect the operation of the ship.

The cyber threat will be described in the following section followed by a description of attack paths against operational systems on ships.

Operational systems are threatened by cross-sector attacks

The CFCS assesses that overall the biggest cyber threat emanates from financially motivated cybercriminals. This wide group of attackers do not have a specific interest in operational systems on ships, but attack targets across all sectors of society.

Cybercriminals are generally opportunists, and CFCS assess that they would be ready to attack operational systems, which for instance could become accessible by compromising connected administrative networks or that are vulnerable to attacks directly via the Internet.

Control units affected by botnet malware

According to an IT security company, the antenna control unit of a ship-borne satellite communication system was infected by malware in 2018. The malware, known as Mirai, is used to build so-called botnets comprising a very high number of compromised computers and internet-connected units such as routers, CCTV cameras and in this case also antenna control units.

The units in a botnet may be used to launch overload attacks, so-called DDoS attacks, for instance against websites the hacker wants to take down, or to distribute spam and malware. There are examples were hackers inadvertently have disturbed units in a botnet because they had no technical knowledge of the consequences of their hacking. In 2016, a hacker for instance exploited 900,000 home routers from a Mirai botnet to launch a DDoS attack. The attack inadvertently prevented the 900,000 Deutsche Telecom customers from accessing the internet for two days.

Part of the threat derives from cybercriminals, who compromise computers, IT systems and digital units to exploit computing power, storage or communication capability to financial gains. Such compromised systems may for instance be used by criminals to generate crypto currency through so-called crypto miners or as platforms for additional attacks.

A threat is also posed by cybercriminals who compromise systems to encrypt them with ransomware and hold them hostage for ransom.

CFCS assesses that cyber criminals behind ransomware attacks have no specific interest in operational systems on ships. Rather, they attack computers and IT systems across sectors which are vulnerable to their attack techniques and malware.

Operational systems on ships may be attractive targets for criminal extortioners, because they are vital to the shipping company, which may serve as leverage against the victim to pay ransom. Some types of ransomware have furthermore been programmed to spread autonomously to connected systems and networks. This was the case in the 2017 WannaCry attacks when more than 300,000 computers worldwide were infected by ransomware.

Infection of administrative systems may spread
In 2017, a ransomware attack in a shipmaster's computer spread to the ship's operational systems cutting the power supply. The crew was unable to resolve the issue and had to fly in IT support. It took three days to regain power. The ransomware had successfully spread despite segregation of networks.

In an example from 2019, a container ship in route to New York discovered that its network had been severely weakened by malware. The US Coast Guard and the FBI visited the ship before it reached port. They could establish that the malware called Emotet had not affected any essential operational systems. However, their investigations revealed several serious IT security weaknesses, including critical vulnerabilities to critical control systems.

Some criminal hackers send phishing emails targeting specific ships and their crew. CFCS assesses that such attacks generally do no target operational systems on ships. Similar to broader campaigns, the primary objective of such attacks is financial gain, and the hackers thus employ techniques that are common across all sectors.

CFCS knows of phishing emails sent to recipients on board ships with the purpose of spreading malware, which is typically used to steal financial information and spread ransomware.

Single individual hackers also pose a threat

While CFCS assesses that hackers generally do not target operational systems on ships, there are exceptions. Operational systems that are exposed to the Internet and has inadequate protection, is threatened by individual hackers who, out of technical interest or sheer curiosity try to gain access to operational systems on ships and potentially manipulate them.

Cyber security researchers and companies have proved that in some cases compromising operational systems on ships does not require a high level of technical knowledge.

According to open sources, in 2019 a curious individual found a so-called dynamic positioning system at a mobile drilling platform using the Shodan search engine. The system was vulnerable to hacker attacks and the person unintentionally took the system offline. There are no reports on the consequences to the drilling platform, but other examples of consequences are available in open sources. One example is a cyber attack on a mobile drilling platform of the coast of Africa. The impact here was that the platform tilted to a degree that productions were shut down for a week, before the problem was identified and resolved.

Potential threat from destructive cyber attacks from states

There is a potential threat from destructive cyber attacks against operational systems on ships from state actors – in particular in connection to military conflicts. However, CFCS assesses that no foreign states currently have the intent of launching destructive cyber attacks against Danish ships.

The threat from destructive cyber attacks may be higher against ships operating in areas of conflict where states have been known to use destructive cyber attacks against civilian targets.

The 2017 NotPetya attack, which hit victims such as the Danish shipping company A. P. Moeller Maersk, was directed against companies operating in Ukraine. During the conflict between Ukraine and Russia, Ukraine have been subject to several destructive cyber attacks. Other countries, including Saudi-Arabia and the Republic of Korea, have also been hit by destructive cyber attacks.

Software update was entry point for NotPetya

The NotPetya attack had its origin in a compromised Ukrainian software company behind the M.E.Doc. software. Hackers infected companies through an update to the M.E.Doc software that contained malware. The malware was a so-called worm that quickly spread to other parts of the affected companies' IT infrastructure, infecting other companies as well .

The threat may also be higher against operational systems on ships whose shipping company does business with companies or states, who themselves are targets of destructive cyber attacks. In 2018, the Italian oil services company Saipem, which operates a number of special-purpose vessels, was victim of a targeted destructive cyber attack. Saipem is a sub-contractor of the Saudi oil company Saudi Aramco, and the attack took place using variants of the same malware, which was used in previous attacks against Saudi Aramco. The destructive cyber attack destroyed data on several hundreds of Saipem computers across the world.

Maritime equipment suppliers are especially targets of cyber espionage. Hackers may exploit compromised equipment suppliers to launch destructive cyber attacks against operational systems on ships. These can for instance be distributed disguised within legitimate system updates.

Cyberespionage against shipping companies also occur. Similarly, this espionage can be used to launch destructive cyber attacks against operational systems on ships if the company’s administrative systems are connected to the ship’s operational systems.

Disruption of GNSS signals also poses a threat

Disruption of GNSS signals, such as GPS, which for instance are used for positioning of ships within navigation systems, is another type of threat to operational systems on ships using the signals.

Interruption of GNSS signals occurs through local transmission of electronic signals that drowns out legitimate signals. This can happen for instance through noise signals, a method known as jamming, or by transmitting alternative signals, changing the position. This technique is called spoofing.

The Danish Defence Intelligence Service categorizes these attack techniques as electronic warfare, and there have been numerous instances of GNSS disturbance in the waters close to Russia, Iran, Syria and China among other. NATO’s maritime command monitors GNSS disruptions across the world, and ships can report incidents to the command.

Foreign states and criminals alike use these methods. CFCS assesses that the motives behind these disruptions vary. One motive can be to protect an area against drone traffic that use GNSS signals. It can be authorities aiming to prevent drones from disturbing air traffic at airports, or criminal smugglers making efforts to avoid border control drones. During a conflict, the aim may be to disturb air and ship traffic.

The CFCS is not aware of any incidents in which hackers have compromised systems for the purpose of GNSS disruption.

Several entry points of attacks against operational systems on ships

The different threat actors attack operational systems on ships in different ways and through different entry points of attack. These entry points may be divided into three categories:

1. Attacks through external units or Internet connections.
2. Attacks through connections to administrative systems.
3. Attacks through equipment suppliers' access to operating systems.

Combinations of these entry points of attack also occur.

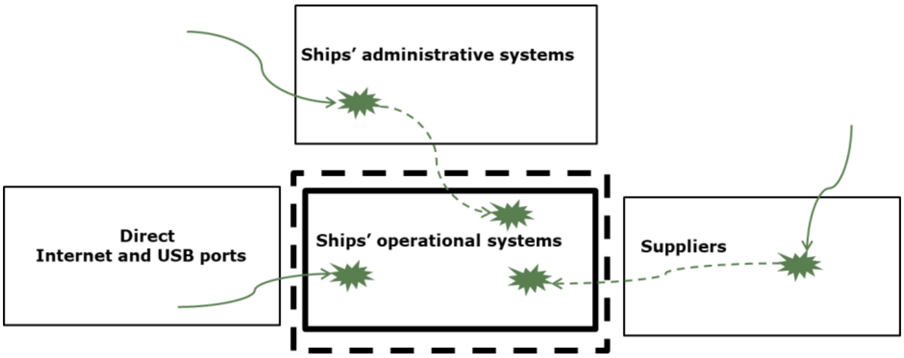


Figure 1. Points of attack to operational systems on ships.

Vulnerable systems may among other be attacked directly via the Internet

Operational systems may be vulnerable to relatively simple cyber attacks launched directly via the Internet or external units, such as USB flash drives, mobile phones, etc. which can be connected to the systems. These attacks do not presuppose prior compromise of the shipping company or sub-suppliers.

Operational systems on ships are particularly vulnerable if they are directly connected to the Internet without sufficient security measures, or if it has not been adequately protected against transfer of malware via external units. Over the past few years, the shipping industry has been particularly focused on the risk of malware infections through open USB ports on operational systems' hardware.

Another common technique used by hackers is taking control of digital units that are protected by known standard passwords or weak passwords. They do this by scanning the Internet for such digital units and guessing their password. These hackers often do not have a particular interest in shipping, but want to compromise and exploit units independently of their normal function or significance.

Supplier infects system via a USB connection
In their December 2018 guidelines, BIMCO, described an example in which a ship's power management system was infected by malware transferred in connection with a system update carried out by a supplier's technician. The infection occurred inadvertently as a result of the technician's use of a USB device connected to the ship's system.

Connections facilitate attacks through administrative systems
Like administrative systems on land, administrative systems on ships are exposed to a persistent threat in particular from cybercriminals with a number of attacks having occurred against administrative systems on ships.

By compromising the administrative systems, the attack may spread to the operational systems if these systems are interconnected, or if the attackers are able to penetrate potential network segregation.

Even if attacks against administrative systems do not spread, attacks that lock or disrupt the administrative systems, such as ransomware attacks, may affect the commercial aspects of ship operation. This might happen for instance if the staff is unable to access the freight or passenger systems.

Equipment suppliers may be used as stepping stones for cyber attacks
Operational systems suppliers increasingly have network access to the ships in order to monitor and update the systems. This potentially enables cyber attacks through trusted equipment suppliers.

Some of the suppliers of specialized ship equipment have very large global market shares. A cyber attack through such a supplier could affect the operation and safety of a large number of ships worldwide across industry.

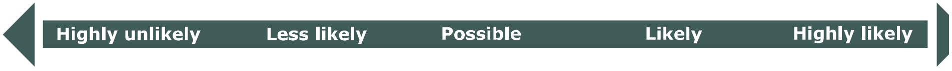
There have been examples where updates from equipment suppliers have been used as entry points for cyber attacks against ships. In 2017, a recognized organization described an incident in which the ECDIS navigation system onboard two bulk carriers shut down following chart updates from a chart supplier. A file containing the update was e-mailed to the ship and transferred via a USB flashdrive. First, the ECDIS system on one of the ships shut down. Because the crew did not report the incident, a similar incident occurred on the sister ship later as the same file was used to update its ECDIS system. There are conflicting reports on whether the update was infected with a malware or just a case of a bad software. Regardless, the incident shows how a vulnerability can impact ship safety.

The threat via suppliers and sub-suppliers is called the supply chain threat. For more information on this type of threat, go to CFCS' website to read the 2019 threat assessment: Cyber attacks on suppliers.

Definition of threat levels
The DDIS uses the following threat levels, ranging from **NONE** to **VERY HIGH**.

NONE	No indications of a threat. No acknowledged capacity or intent to carry out attacks. Attacks/harmful activities are unlikely.
LOW	A potential threat exists. Limited capacity and/or intent to carry out attacks. Attacks/harmful activities are not likely.
MEDIUM	A general threat exists. Capacity and/or intent to attack and possible planning. Attacks/harmful activities are possible.
HIGH	An acknowledged threat exists. Capacity and intent to carry out attacks and planning. Attacks/harmful activities are likely.
VERY HIGH	A specific threat exists. Capacity, intent to attack, planning and possible execution. Attacks/harmful activities are very likely.

The DDIS applies the below scale of probability


Highly unlikely
Less likely
Possible
Likely
Highly likely