ON2IT AND AMS-IX PRESENT: THREAT TALKS

Threat Talks
Hack the Boat

IT vs OT:
The two sides of marine cybercrime

If banks, factories, and retail shops can be hacked, it's no surprise that boats and ports are also vulnerable. In fact, **the Port of Los Angeles recently announced** that it records twice as many attacks as it did just a few years ago and must now contend with 40 million ransomware, malware and spear-phishing incidents each month.

For years, maritime companies have focused on protecting their data and IT environments, but securing operational technology (OT) was less of a priority. One reason for this is that, until recently, said operational systems simply weren't connected to the internet.

Modern shipping operations however rely heavily on both Information Technology (IT) and Operational Technology (OT) for navigation, communication, and operational management. Especially the conventional OT systems, which have been built with fairly open and unencrypted, sometimes decades old systems, are like an open invitation to hackers.

With marine cybercrime steeply on the rise, what can maritime companies do to bring their IT and OT in line with today's cybersecurity standards?

In this episode of Threat Talks we will discuss the following threats:

- Ballast System Hack
- Securing AIS

A significant number maritime professionals foresee cyber attacks leading to collisions 60% & groundings 68%

90% of respondents anticipate disruptions to ship and/or fleet operations due to cyber incidents.

76% Over three-quarters believe a cyber incident could shut down a strategic waterway.

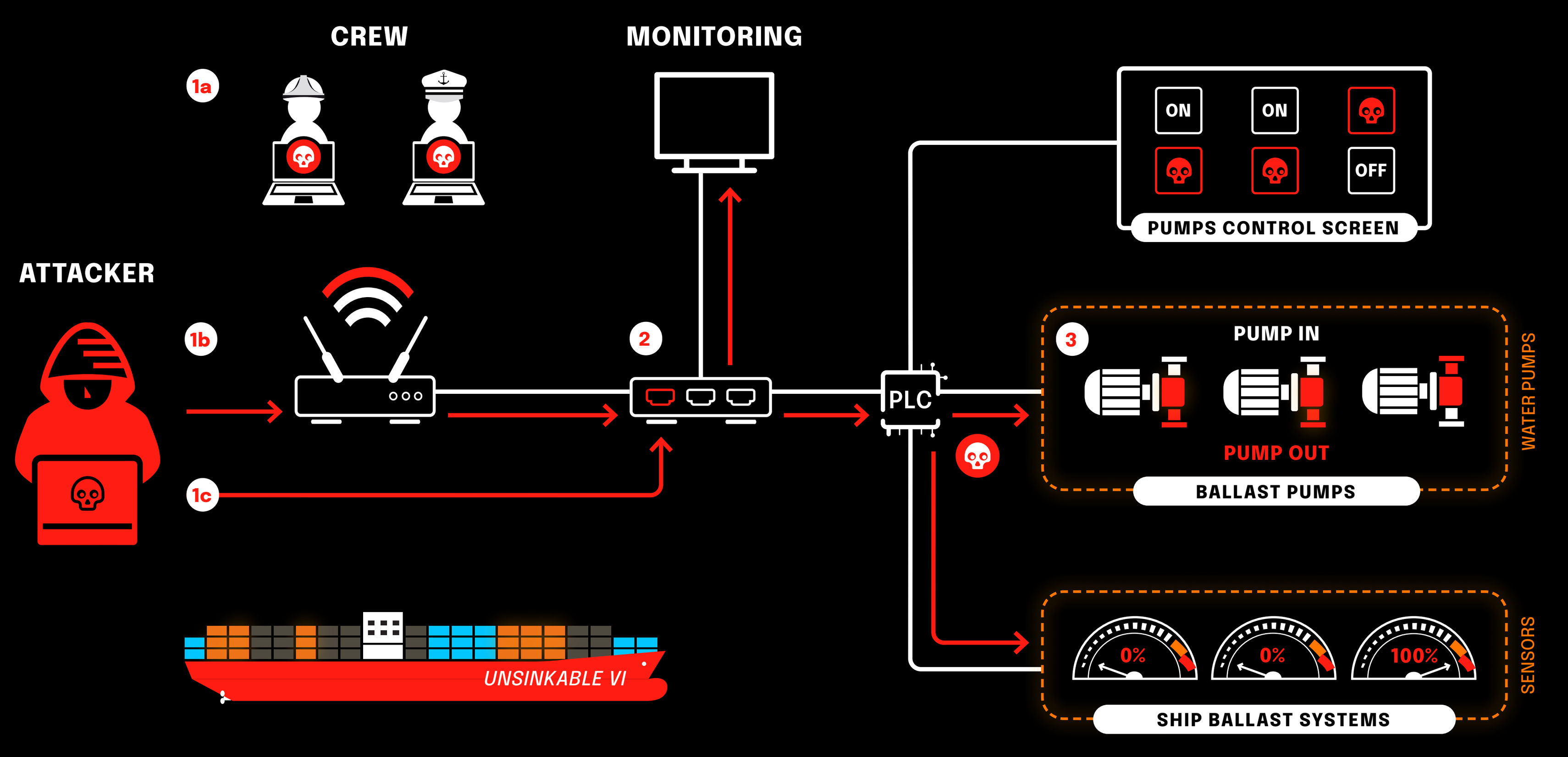
56% of maritime professionals expect cyberattacks to cause physical injury or death in the industry within the next few years.

Sources: DNV report - Maritime Cyber Priority 2023

Ballast System Hack
Exploiting vulnerabilities in Operational Technology

The ballast system is crucial for maintaining a ship's stability by regulating its center of gravity through water level adjustments in the ballast tanks. It ensures proper trim, structural integrity, and draft, while also reducing the risk of rolling in rough seas.

For a hacker to manipulate these systems, they would first need to breach the ship's operational technology (OT) network, which manages key systems like the ballast. Once inside, they could exploit vulnerabilities in the control software, bypassing safety protocols to alter the water levels in the ballast tanks, ultimately disrupting the ship's stability and safety.



Intial Access

1. **(a-b-c)** The attacker can gain entry into the network through various methods. This could involve cracking the Wi-Fi password, compromising an employee's laptop with a backdoor, or even exploiting an unsecured Ethernet port in the facility.

M Implementing strong network security practices, such as network segmentation and secure Wi-Fi configurations, can help mitigate risks related to initial access. Layer 2 security measures, such as using parked VLANs, can prevent attackers from exploiting available Ethernet ports.

Additionally, deploying Endpoint Detection and Response (EDR) solutions on crew laptops can detect and prevent the introduction of malware or infected devices into the network, minimizing the chances of initial compromise through employee devices.

Lateral movement

2. After gaining network access, the attacker begins enumerating network hosts. They can then move laterally across the network, targeting other systems such as monitoring computers by exploiting unknown vulnerabilities or taking advantage of common misconfigurations.

M Network segmentation should be used to isolate critical systems like PLCs [1], from less secure parts of the network.

Tools such as intrusion detection systems (IDS) and regular network monitoring can be employed to detect and alert on unusual behavior, such as unauthorized host enumeration or lateral movement attempts.

Keeping systems and devices updated with security patches further reduces the risk of attackers exploiting known vulnerabilities during this phase of the attack.

Compromising the Ballast System

3. Once the attacker identifies the PLC controlling the ballast [2] pumps, they can manipulate it by sending crafted network packets. This allows them to activate the pumps at will, which could lead to overfilling the ballast tanks, causing the vessel to tilt or even capsize.

M Proper segmentation and strict policies on a next-gen firewall would forbid these webshell connections. Additionally, blocking well-known malicious sources (IOCs) could help limit the chance of a successful attack.

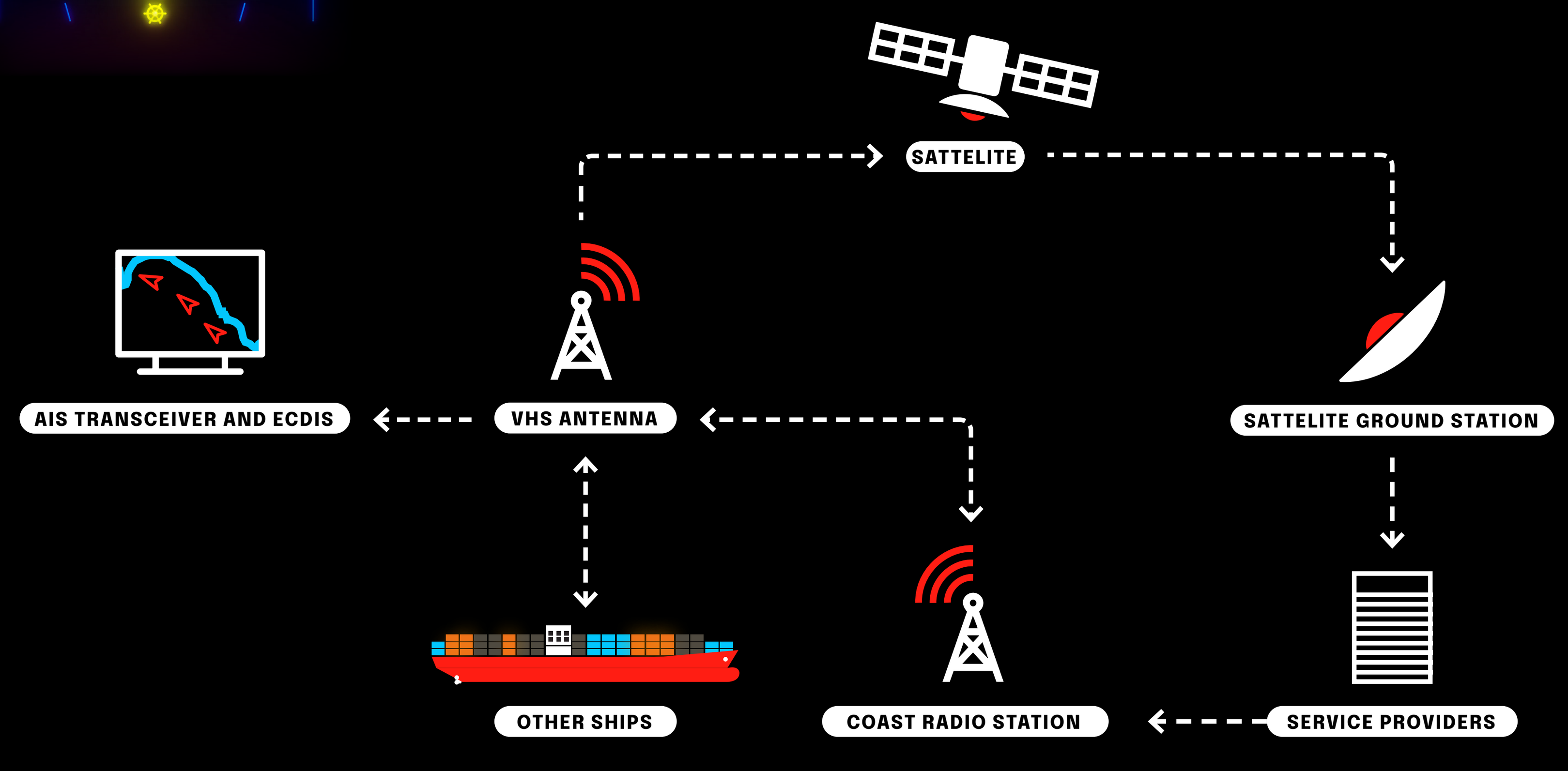
Notes

[1] A PLC (Programmable Logic Controller) is an industrial digital computer used to control various automated processes, including machinery and equipment. In the case of a ballast system, the PLC manages the activation and regulation of pumps that control water flow into and out of the ballast tanks.

[2] A ballast is a compartment within a ship or other floating structure that can be filled with water to maintain stability and balance during navigation. By adjusting the amount of water in the ballast tanks, the vessel's weight distribution and buoyancy can be controlled.

Securing AIS
Advanced Identification System

What is AIS - Automatic Identification System? AIS is a system to send identity, position, speed, time and course information to nearby ships and shore. The idea of Universal U-AIS was coined in 1990 and in 2001 AIS became mandatory, but depending on government. The range of U-AIS is +/- 74 km (about 40 nautical miles), to overcome this relatively short distance Sattelite S-AIS is developed.



Why is AIS a critical system for maritime safety?

AIS is used for:

- Collision avoidance
- Situational awareness
- Search and rescue operations
- Maritime security, detect unauthorized or suspicious activity
- AIS is not only available for ships, but also rescue system, like AIS-MOB (Man Overboard)

Is the AIS mandatory on all ships?

- For most ships it is, think of passenger and cargo ships
- For fishing vessels it depends on the country, however most countries require AIS
- Recreational boats, pleasure yachts, or non-commercial crafts are generally not required to carry AIS. The same goes for AIS-MOB (Man Overboard)

AIS Vulnerabilities/weaknesses

Vulnerabilities/weaknesses of AIS:

- Spoofing
- Unencrypted signal
- No authentication
- Modification of signals
- Jamming

How could these vulnerabilities be exploited?

- Impersonation - pretend you are another ship
- Ghost ships - deception
- False information - illegal fishing

Examples

- OIL tankers disabling AIS to evade international sanctions
- North Korean ships doing the same
- Pirates using AIS to track and target high-value ships

Spoofing Technique

Signal spoofing - Many AIS spoofing attacks rely on broadcasting false location data, which can mislead nearby ships or shore authorities. Attackers can pretend to be another vessel (impersonation) or even create "ghost ships" that don't exist, potentially for illegal purposes like smuggling or piracy.

Mitigation

TDFOA and CRFS - To defend against AIS spoofing, authorities can compare the actual source of the transmission with the location data provided in the AIS message. Tools like CRFS's RFeye Nodes[1], deployed on ships or shores, use the TDOA[2] technique to geolocate radio signals. If there's a significant difference between the reported and actual locations, it signals a spoofing attack. This allows maritime authorities to track down the source of the transmission and respond quickly to prevent further exploitation.

Notes

[1] CRFS's RFeye Nodes (Cognitive Radio Frequency Systems) are sensor devices used for monitoring and geolocating radio frequency signals in real time. They help detect and track the source of transmissions, aiding in the identification of spoofed or unauthorized signals.

[2] TDOA (Time Difference of Arrival) is a technique used to determine the location of a signal by measuring the time difference at which the signal is received by multiple receivers. This method is commonly used to triangulate and locate the source of radio transmissions.

Key Conclusion

AIS is a critical, life-saving protocol in maritime operations, providing essential data for safety and navigation. Its simplicity and openness have made it widely adopted, but these same qualities also expose it to significant security challenges.

Securing AIS won't be easy, given its global use and integration into countless systems. While discussions on improving its security surface regularly, we've yet to see any concrete, industry-wide solutions.

The question remains

How can we secure a system that was designed to be so open, without compromising its accessibility and effectiveness?

Taxonomy

ATT&CK Technique
Which technique of the MITRE ATT&CK framework does the threat correspond to.

ATT&CK Mitigation
Which mitigation of the MITRE ATT&CK framework can be applied.

Attack Strategy
Plan devised by the attacker to exploit specific system vulnerabilities.

Attack Vector
What is the primary method of attack.

Evasion
Tactics used by the attacker to avoid detection or bypass security.

Detection
Mechanism to identify malicious activities or system anomalies.

Complexity
How easy it is to exploit the vulnerability or carry out the attack.

Threat Level
How severe the threat is.

Target Type
The category of organization that may potentially be targeted.

Threat Actor Type
What type of threat actor may be involved.

CONTACT US

mSOC score explanation

We assign scores to both our sources and the news items. Sources are scored on a numeric scale ranging from 0 (untrustworthy) to 5 (verified), while news items are scored with a letter, ranging from E (unreliable) to A (reliable). By considering the scores of both the source and the news item and the quality of the available information, we classify the overall reliability into three categories: Confirmed, Verified, and Credible. Interested in learning more about our reliability scoring system for sources and news items? Our Threat Intelligence team would be happy to walk you through our procedure, so please don't hesitate to reach out.

threat-talks.com

ON2IT ZERO TRUST INNOVATORS amsix