

Ship hit the fan!

Malware on a cruise ships control systems

Certain details may have been altered to protect the identity of the ship, as the details were never made public
All ship images are AI generated

MARITIME CYBER GUILD



About me

Christopher Stein

Location:
Copenhagen, DK

Current role:
Lead Engineer, Maritime Cybersecurity @ Major Cruise Operator
Focus: OT: Automation, Navigation, Propulsion, Power, etc..

Guild master @ Maritime Cyber Guild

IMO Delegate:
ECRAM @ Danish Flag
Cyber Code @ CLIA (Cruise Line International Association)

WÄRTSILÄ
L3 Technologies
NORRIQ Your Business - Simplified
MACROware
esoft systems
STEINGROUP

I am presenting in my own capacity and not as part of my current employment.
The opinions expressed in this presentation and on the following slides are solely my own and not necessarily those of my employer

MARITIME CYBER GUILD

Before we begin

No fingerpointing!

I will not tell you which ship it was

Certain details have been omitted to protect the identity of the ship

This is about sharing experience and knowledge

MARITIME
CYBER GUILD

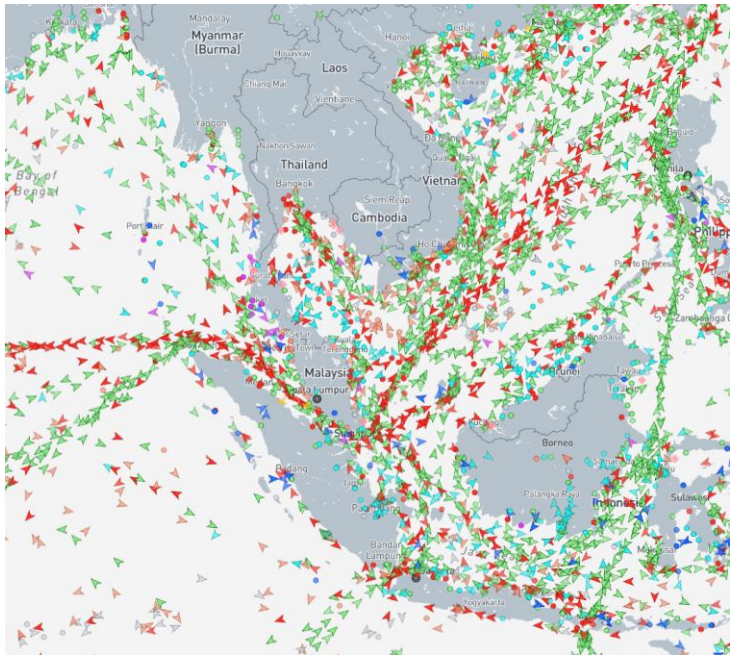
2018

Somewhere in SEA

The ship:
Approx. 150.000 GT
3300 pax
1700 crew

Delivered 2016
Cost: approx. USD 1Bn





MARITIME
CYBER GUILD

Ship observes:

-Slow / unresponsive automation and navigation HMI
-Automatio system process controllers (embedded computer PLC, running Windows) status cycling between active & offline
-Loss of remote control and monitoring of systems connected to automation system (including power management)
-Propulsion, power and other automation data no longer available in ECR and on Bridge

Current status:
-Ship is now operating all systems in local control

-Tugs have been called to escort the vessel to port

<u>Current cruise is cancelled</u>



Process controller

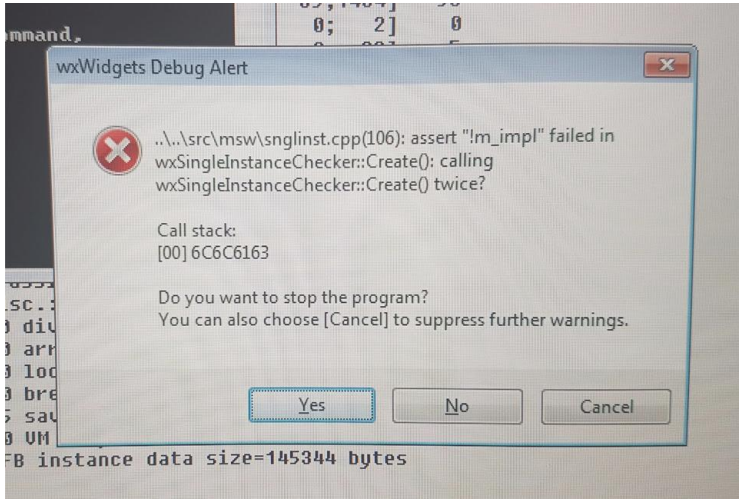
MARITIME
CYBER GUILD

Service engineer dispatched from local office

Troubleshooted and tried restarting and redeploying software

Spent almost 2 days with no success

Called for assistance after 1 day and mentioned suspected malware based on lack of ability to fix



WxWidgets (c++ library) failure on controllers prior to crash

MARITIME CYBER GUILD

What happened?
-An event has caused issues with OT systems, causing strange behaviour. Some systems /devices were unusable due to slowness and erratic behavior; others crashing after running for a few mintes.

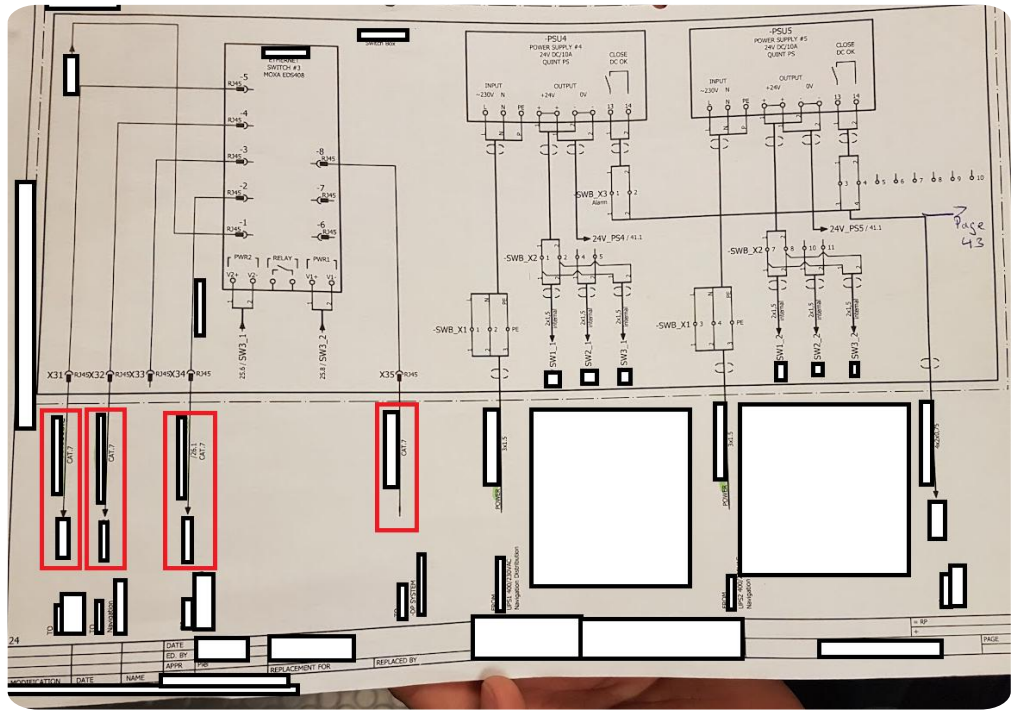
Steps taken:
-Service engineer has troubleshooted the system and could not find any abnormalities beyond reported symptoms

Which systems are affected?
-**Navigation, IAMCS**, PCS, Stability system, and safety management system

Is it malware?
-A quick initial scan with an antimalware live-CD indicated malware was present on the system.

MARITIME
CYBER GUILD

Getting back in operation



Contain the spread: Isolate systems – Informed decision

- Navigation and IAMCS are on the same platform and networked.
- If disconnected, some information will not be exchanged between the systems.

- PCS is networked with IAMCS. If disconnected, ship will lose monitoring and control from IAMCS.

- Stability and Safety management systems are networked with IAMCS for data exchange. Similar to removing the network connection between Nav and IAMCS, data exchange will no longer happen.

- Due to time constraints, the first attempt would be to clean rather than redeploy

MARITIME CYBER GUILD

Asses the state: Can we use the systems now?

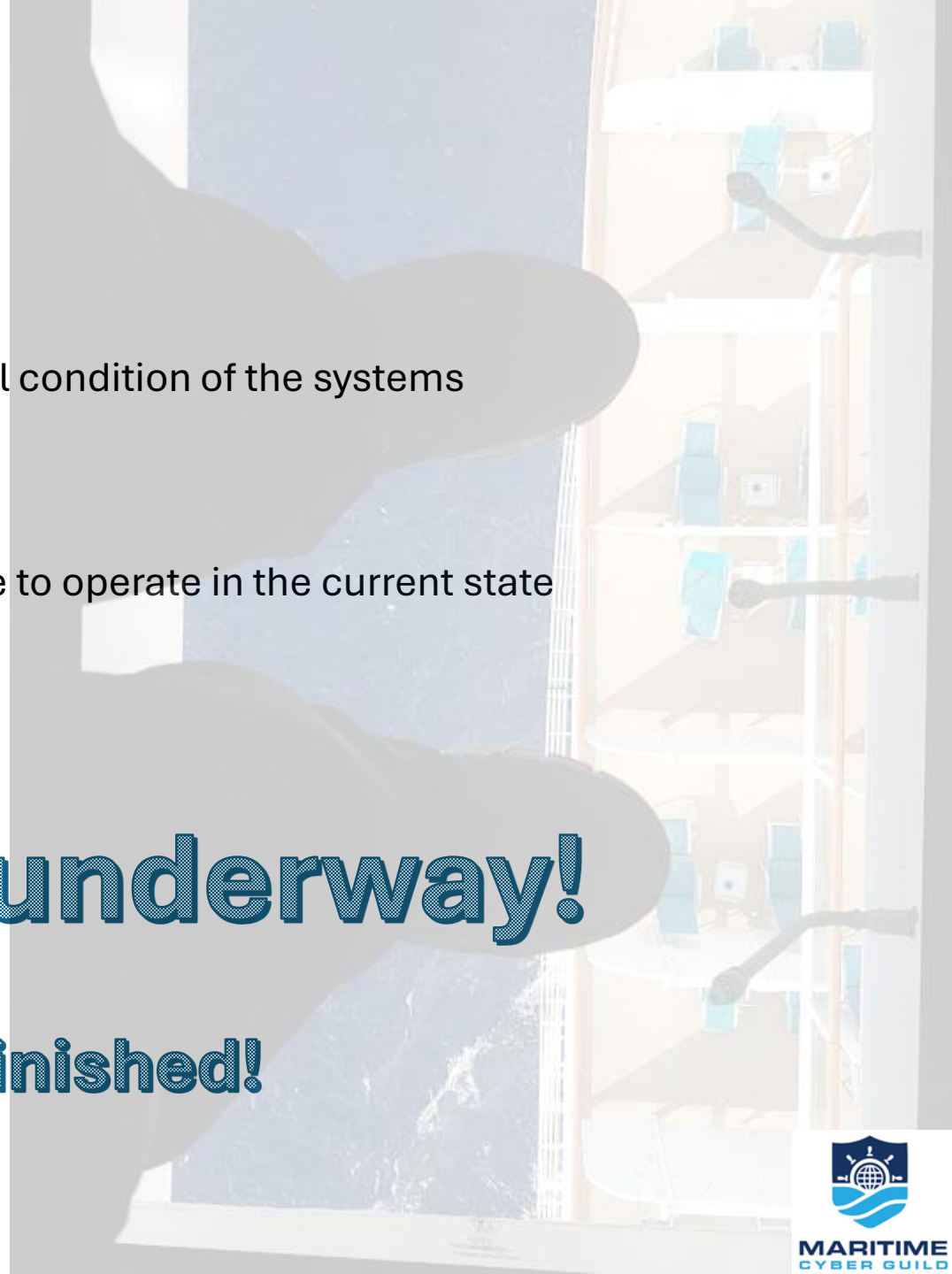
-Response team and service engineer investigated the operational condition of the systems

-Functionally in good working order

-Together with Master, it was determined that the systems are safe to operate in the current state

And now we are underway!

...but we are not finished!



<u>Prevent reinfection:</u> What is the best course of action to take?

Reimaging / redeployment considered.
-Not done, as system was deemed safe and clean of infection. Ship did not want to lose more time (Redeployment planned for later)

Patching
-MS17-010 patch was not installed on the systems, although a bulletin was released by vendors advising about its criticality.
-While underway, noncritical devices/systems were taken down and patched
-During port calls, essential devices/systems were patched
-Response team patched Stability system
-PCS was patched by vendor

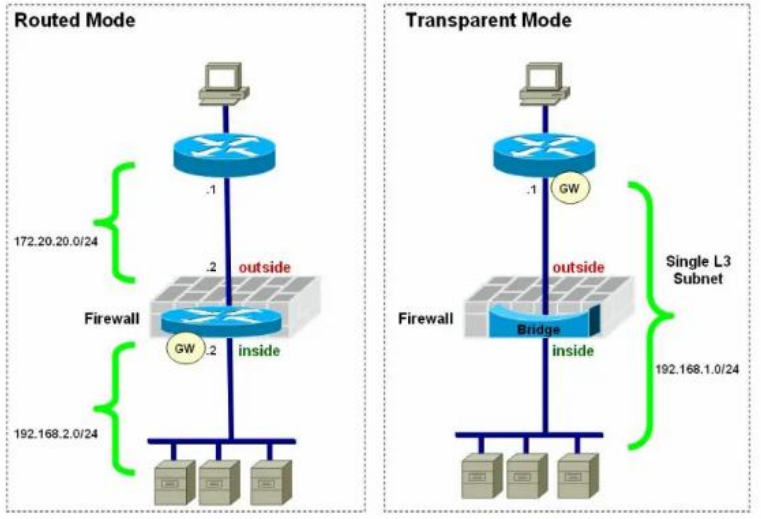
Review segmentation
-Firewall configurations were reviewed
-Configuration errors discovered

Show

Filter List (10/256)

Enable	Index	Input	Output	Protocol	Source IP	Source Port	Destination IP	Destination Port	MAC Address	Target
✓	3	WAN	LAN	TCP	All	All	All	49372	–	ACCEPT
✓	4	WAN	LAN	TCP	All	All	All	49373	–	ACCEPT
✓	5	WAN	LAN	TCP	All	All	All	57072	–	ACCEPT
✓	6	WAN	LAN	TCP	All	All	All	57203	–	ACCEPT
✓	7	WAN	LAN	TCP	All	All	All	49687	–	ACCEPT
✓	8	WAN	LAN	TCP	All	All	All	2025	–	ACCEPT
✓	9	WAN	LAN	TCP	All	All	All	445	–	DROP
✓	10	WAN	LAN	All	All	All	All	All	–	





Serial interfaces to externa

4.28 [redacted]

Field Interfaces

SLOT	PORT	Connected Device	Card Type	IP address	IP address (external system)	Electrical	Baud Rate	Data Bits	Stop Bits	Parity	Interface	Valmet Mode
SLOT1 (PCIe)	COM11	[redacted]	MOXA CP 132EL-I (ch1)			RS 485 2 wire	9600	8	1	None	Modbus RTU	Mast
SLOT1 (PCIe)	COM12	[redacted]	MOXA CP 132EL-I (ch2)			RS 422	9600	8	1	None	Modbus RTU	Ma
SLOT2 (PCIe)	X1	[redacted]	Intel PRO/1000PT 2 port Ethernet	[redacted]	[redacted]					None	Modbus TCP/IP	M
SLOT2 (PCIe)	X2	[redacted]	Intel PRO/1000PT 2 port Ethernet	[redacted]	[redacted]					None	Modbus TCP/IP	

Comments:
- For [redacted] & [redacted] is 255.255.255.0. For [redacted] Gateway is [redacted]

4.29 [redacted]

Field Interfaces

SLOT	PORT	Connected Device	Card Type	IP address	IP address (external system)	Electrical	Baud Rate	Data Bits	Stop Bits	Parity
SLOT1 (PCIe)	COM11	[redacted]	MOXA CP 132EL-I (ch1)			RS 422	9600	8	1	None
SLOT2 (PCIe)	X1	[redacted]	Intel PRO/1000PT 2 port Ethernet	[redacted]	[redacted]					None
		[redacted]	Intel PRO/1000PT 2 port Ethernet	[redacted]	[redacted]					

MARITIME CYBER GUILD

Forensics investigation: Establishing a timeline of infection

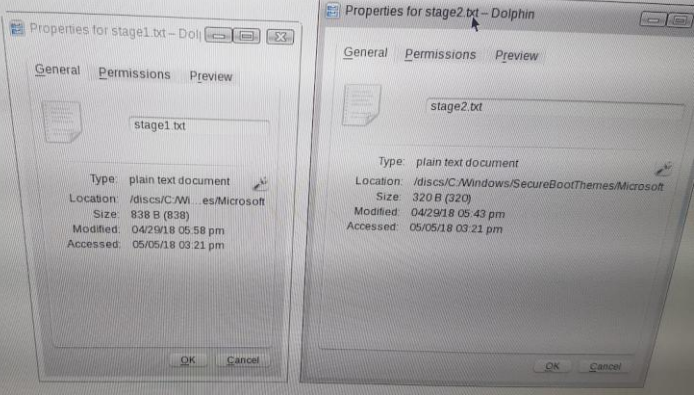
-Getting the ship underway was **top priority**!
Forensics was a secondary consideration and some data was lost in the process.

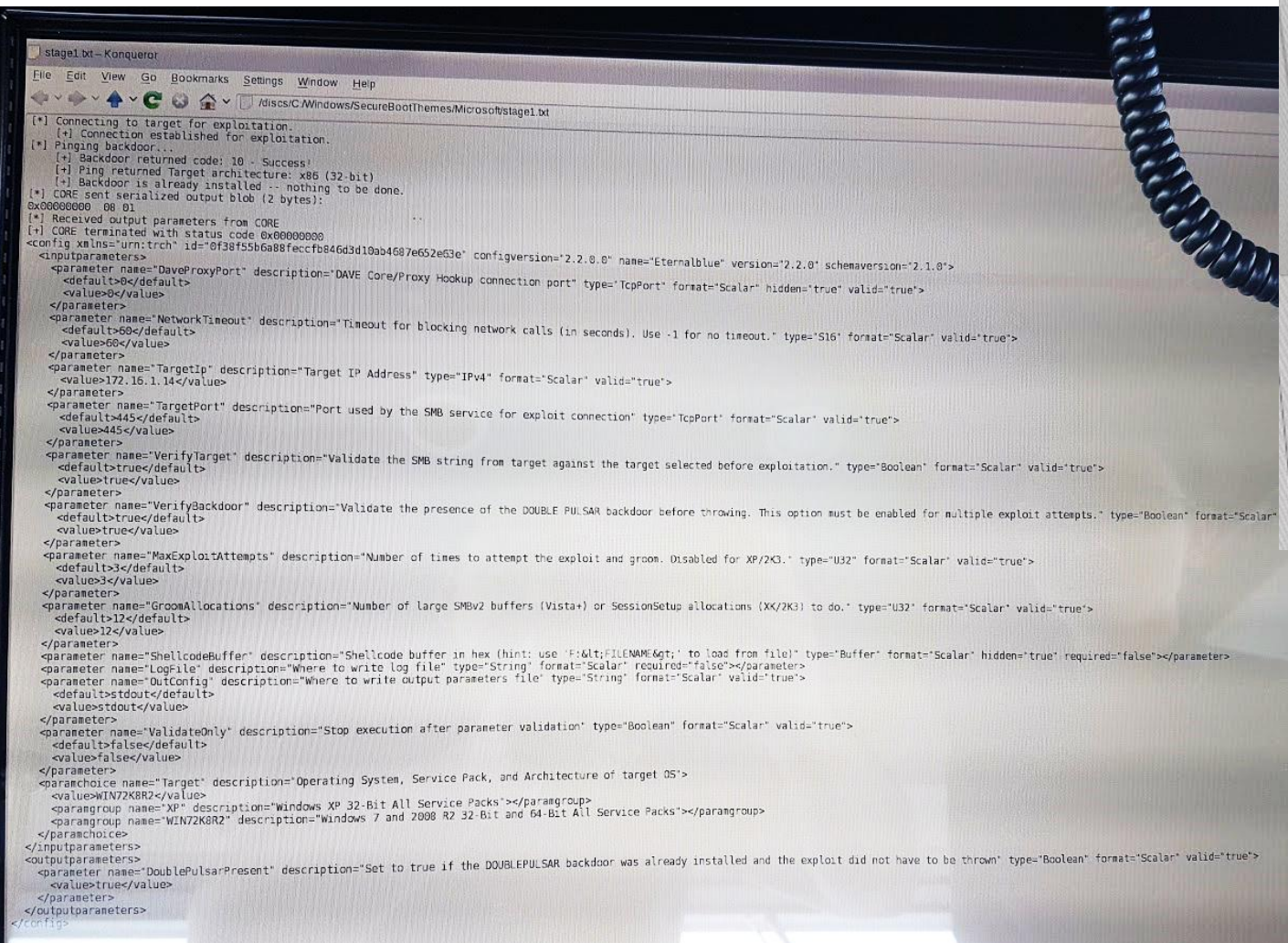
Fragments:
-Residue from infected devices
-Stories from the crew
-AV logs from the ships IT network

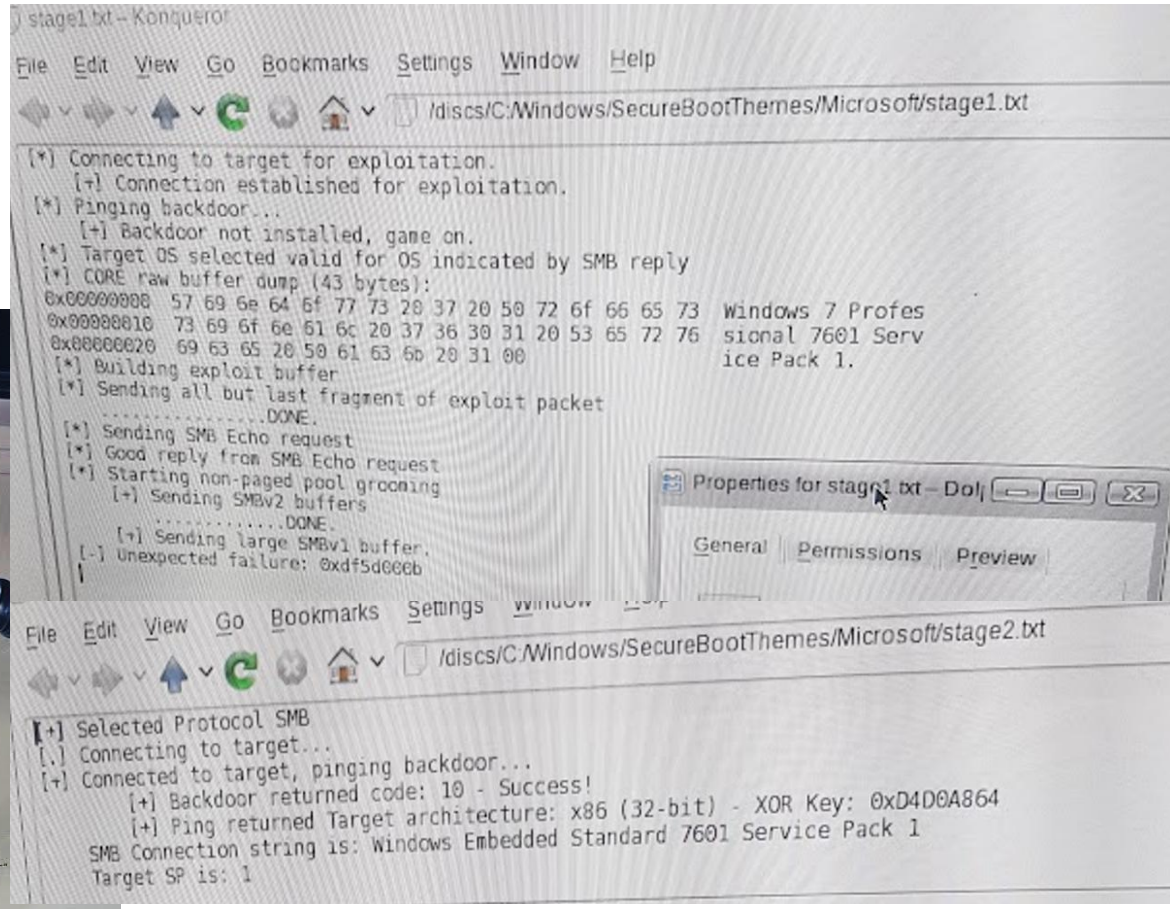
Issues:
-No more infected devices to check
-Timestamps across devices and systems not synced
-Devices had been rebooted (no data in RAM to extract)
-Time critical operation requirement

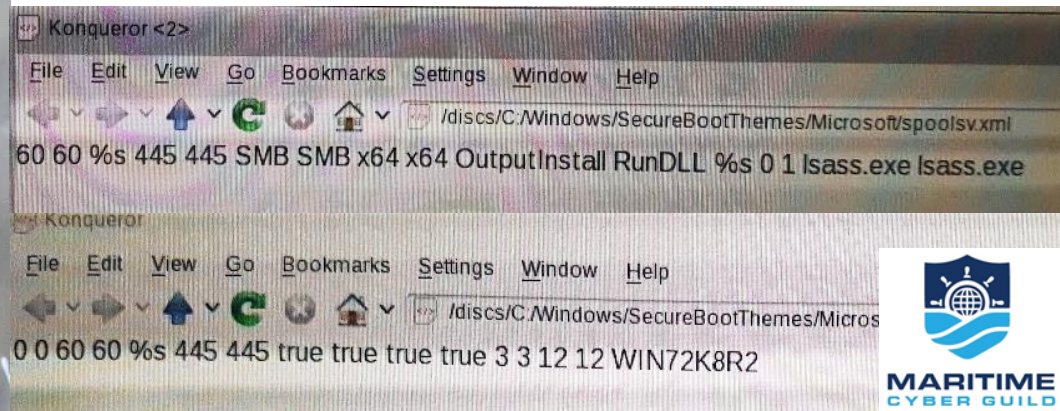
MARITIME
CYBER GUILD

Residue found on both ships IT network and Navigation/Automation









MARITIME CYBER GUILD

Established timeline of events:

-Malware circulated in ships IT network for weeks. Different devices were circulating the worm.
It is unknown how the ships network got infected

-Electrical engineer connected ECR service/VDR replay laptop to ships IT network for file exchange

-Laptop got infected from IT network

-Laptop was connected to IAMCS network

-IAMCS HMI workstations and NAV workstations infected by the laptop

-IAMCS and NAV workstations infected IAMCS Process controllers

-IAMCS process controllers ramdrive filled up and BSOD'ed. Restarted in clean state. Got reinfected

-IAMCS and NAV infected PCS, SMCS and Stability computers through wrongly connected and configured firewalls

Note:
Propulsion Control System logic resides in PLCs, not server or HMI. Therefor core functionality including steering was not affected

MARITIME
CYBER GUILD

What went wrong?

(1/2)

-IT department did not monitor the IT network and antivirus

- Active monitoring of the IT network antivirus, would have shown signs of the malware weeks prior to the incident.

-OT service laptop was unpatched and unprotected

- The service laptop is not part of the critical scope of the machinery, and could be considered an IT asset. Considering its role, it could/should have been protected by enterprise AV.

-OT service laptop was used beyond its indended scope

- Connecting to unspecified networks was not within the scope of the role of this laptop.





(2/2)

-OT systems were unpatched and unprotected

A common sight in maritime OT. When patching is unavailable, safeguards should be established within the possibilities of technology, processes and people, to reduce risk to systems

-OT system segmentation failed

Wrongly configured edge devices contributed to the spread of malware. As that variant of malware spread through SMB (TCP/445) blocking all unneeded ports would have prevented the malware from propegating to other systems.

The vendors poor design choices at system design and development, meant that the integrated IAMCS and NAV were not logically segmented. A flawed understanding of the meaning of ”integrated” systems, meant that integration was considered as the two systems being *one large system*.

-Ship did not respond to the vendor bulletin about the risks regarding MS17-010

Prior to the incident, the vendor had released a technical bulletin to all customers informing about the risk associated with this vulnerability. The customer had received it, but had not acted on it. The vendor did not actively follow-up with customers, and did not patch the systems as a precaution at regular service visits preceeding this event.

MARITIME CYBER GUILD

Lessons learned in brief

-SRtP stations are not sufficiently independent in case of a cyber incident!
SRtP as outlined in SOLAS chapter V only addresses fire and flooding, and does not protect against cyber events

-Having a restore capability (and testing it) is key
Identify critical systems and test their respective fast-restore capabilities

-Segmentation is important
If one system gets infected, segmentation will help contain the spread.

-Policies and procedures need technical safeguards – also: training!
Prevent people from making costly mistakes. Technology has evolved, and training needs to keep up!
And when things DO go wrong, identifying the issue and applying appropriate action is key!

-Patching the systems
If the vendor who normally *never* patches their system tells you that *this* patch is important, you better listen!

-A $5 preemtive fix to a $100.000 risk
Lack of consequence driven risk management led to an 8-figure loss – and it could have been prevented for a fraction of that sum!

MARITIME
CYBER GUILD

Some notes for the future

-Take part ownership of operations by understanding systems and operational needs and limitations

-Apply consequence driven assessment to assess impact and attack vectors

-Impact of an incident, but also impact of your decisions-

-Apply trust-but-verify approach to systems integration, segmentation and procedures

-Tools such as antimalware and IDS are only as good as the OT vendors allow them to be, and as the operators using them

-Continuously manage risks while balancing the panic!

-Safety first!

MARITIME
CYBER GUILD

Thank you!

MARITIME CYBER GUILD