
Ship Hacking 101
A Primer For The Modern Pirate
CORESCOUT
Redoubt Research
October 7, 2018
Brian Olson, Brian Satira
Project Gunsway


Where Everyday Is ITLAPD
Aye! Avast!

Overview

- Introductions
- Basic Seamanship
- Pirate's Primer
- Original Research
- Conclusions and Questions

BLUF:
Maritime infosec immature and pirates are taking notice but the infosec community can help.

"They're not here to fish."
--Captain Richard Phillips

Obligatory WHOAMI

Brian Satira

- Volunteer
  - I Am The Cavalry
  - Project Gunsway
- Reverse Engineer
  - Malware
  - ICS, IoT, Embedded
- Past work for Navy
  - Risk Analysis
  - DFIR
- Some diesel experience
  - Motorpool, pmcs
  - Annapolis School of Seamanship
- Nova Hackers, Nova TOOOL, Nova Labs

@r3doubt
https://blog.r3doubt.io

Brian Olson

- Volunteer
  - Project Gunsway
- Engineer
  - R&D
  - Threat Emulation
  - Architect
  - ICS, IoT
- Past work for Marines
  - Risk Analysis
  - DFIR
- Amateur Meteorologist
- Amateur Sailor/Tactician
  - Ship systems and Networks

@akordingtobrian
brian.olson@corescout.com

Volunteer Organizations

I Am The Cavalry

- Intersection of computer security, public safety, and human life
- Areas of research and advocacy
  - Medical
  - Automotive
  - Public Infrastructure
    - Maritime
  - Smart Home

Project Gunsway

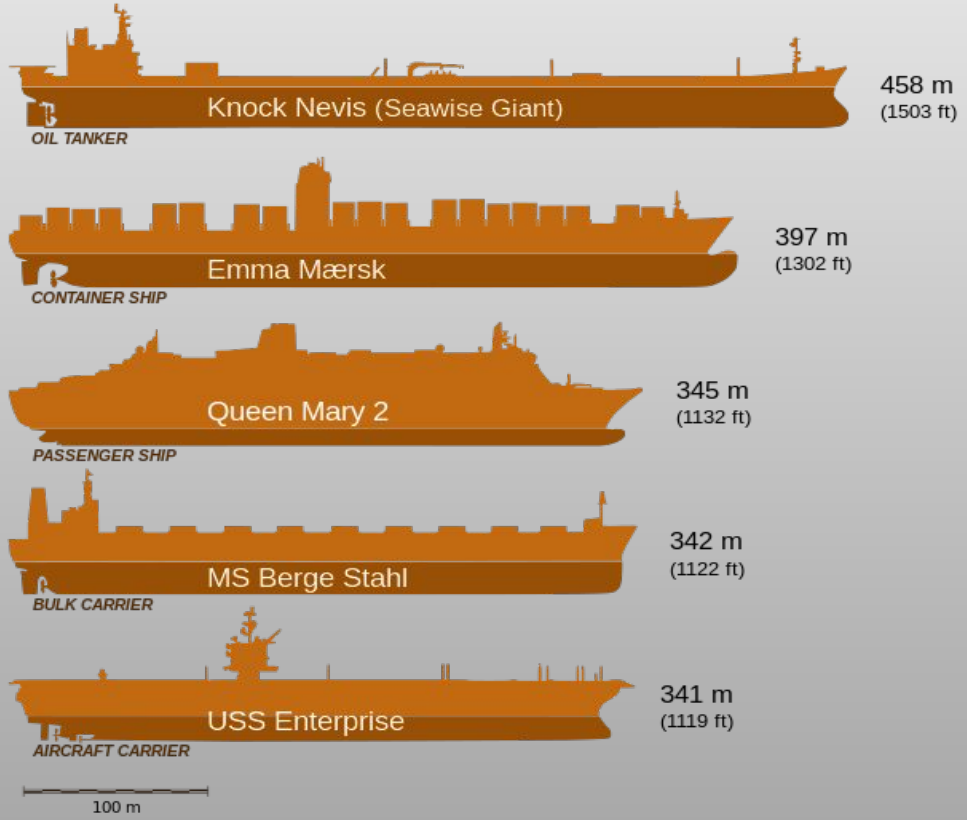
- Grassroots organization
- “Home” is Nova Labs / DC area
- Share The Cavalry’s goals
  - Some of us are The Cavalry members
- Day jobs in IT but maritime connections
- Focused on maritime domain
  - Current project is propulsion controls
- Follow The Cavalry’s disclosure standards

Basic Seamanship (For Pirates)

What's At Stake

- Economy
  - $19 Trillion goods
    - Roughly size of US GDP
- 10.3 Billion tons of cargo
  - 52% containerized cargo (CONEX)
  - 90,000+ ships, 360+ Million containers
- Environment
  - Exxon Valdez (P. W. Sound), $6.3 Billion, 38,000 tons
- Human life
  - Forget PII, how many people die?
- Regulations, practices are ~~a joke~~ not yet "mature"
  - IMO Guidelines, 2017 MSC-FAL.1-Circ.3, Resolution MSC.428(98)
    - Goal for shippers-- plan by 2021
  - Coast Guard NVIC 05-17
    - Cut and paste of NIST guidelines, CISSP practice test questions

Ultra Large Container Vessel (ULCV)

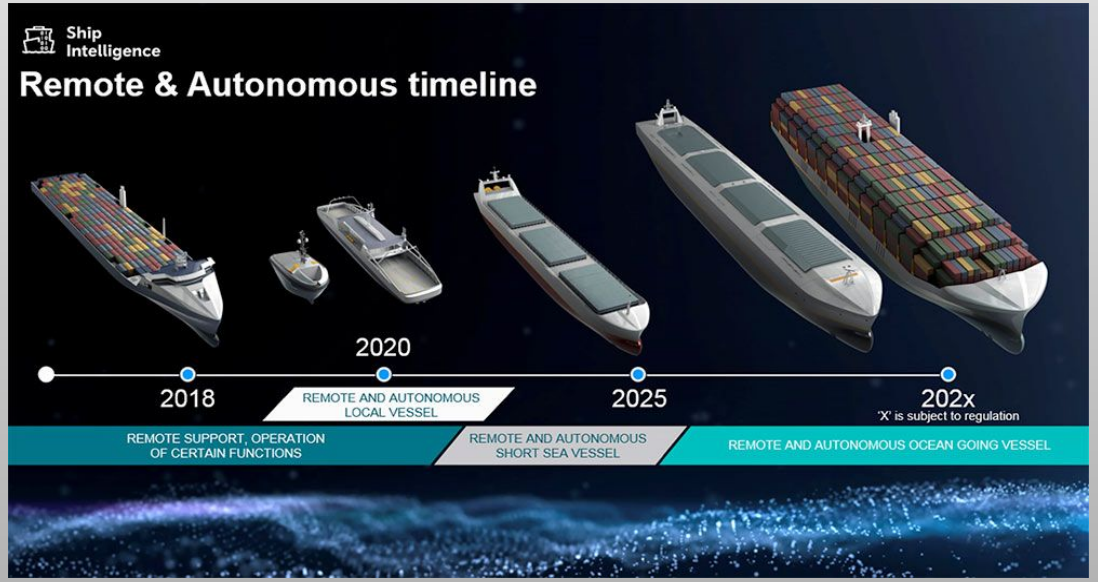


Emma Maersk

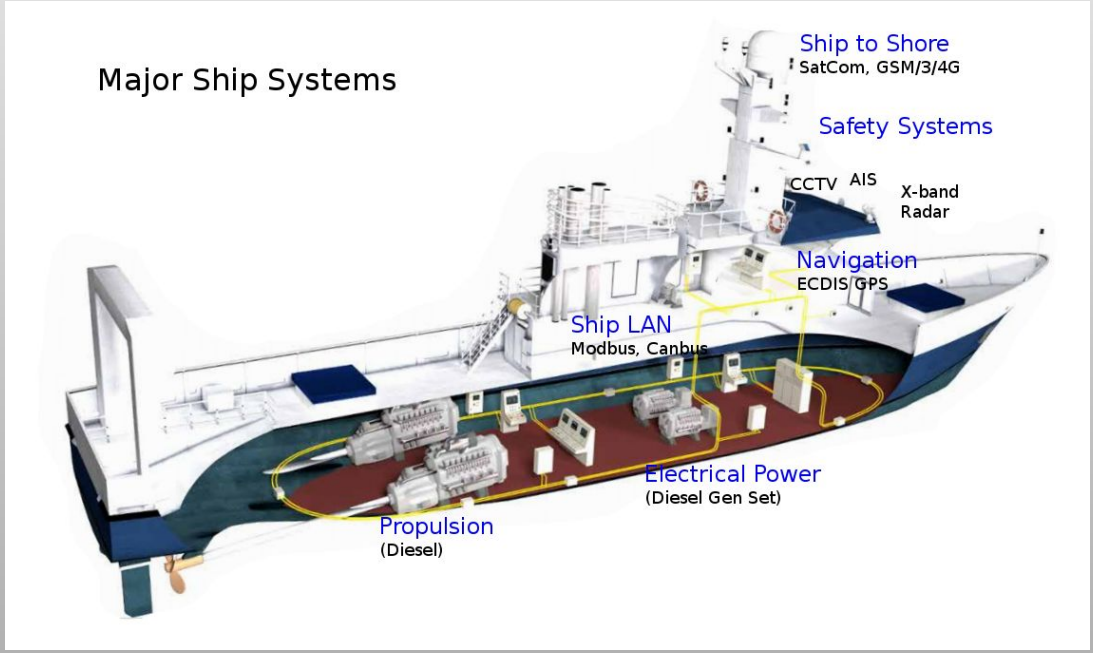
- IMO: 9321483
- Type: Container Vessel
- Owner: A.P. Moller-Maersk Group
- Shipyard: Odens Steel Shipyard Ltd
- Delivered: 2006
- Tonnage: 11,000 TEU
  - Twenty-Foot Equivalent Unit
- Length: 398m (1,306ft)
- Breadth: 56m (184ft)
- Speed: 25.2kts (30mph)

Ship Automation--ICS to Autonomous Vessels

- E-Class ULCV Stats
  - $145 million per ship
  - 6.22 MT per hour at $500 per ton
  - $50,000 per day to operate
  - Crew already 15 or less
- Crew and Fuel Biggest Expense
- Status autonomous vessels
  - RR starts first in 2020
  - Shoreside “bridge”
  - Current limit is regulation
    - SOLAS



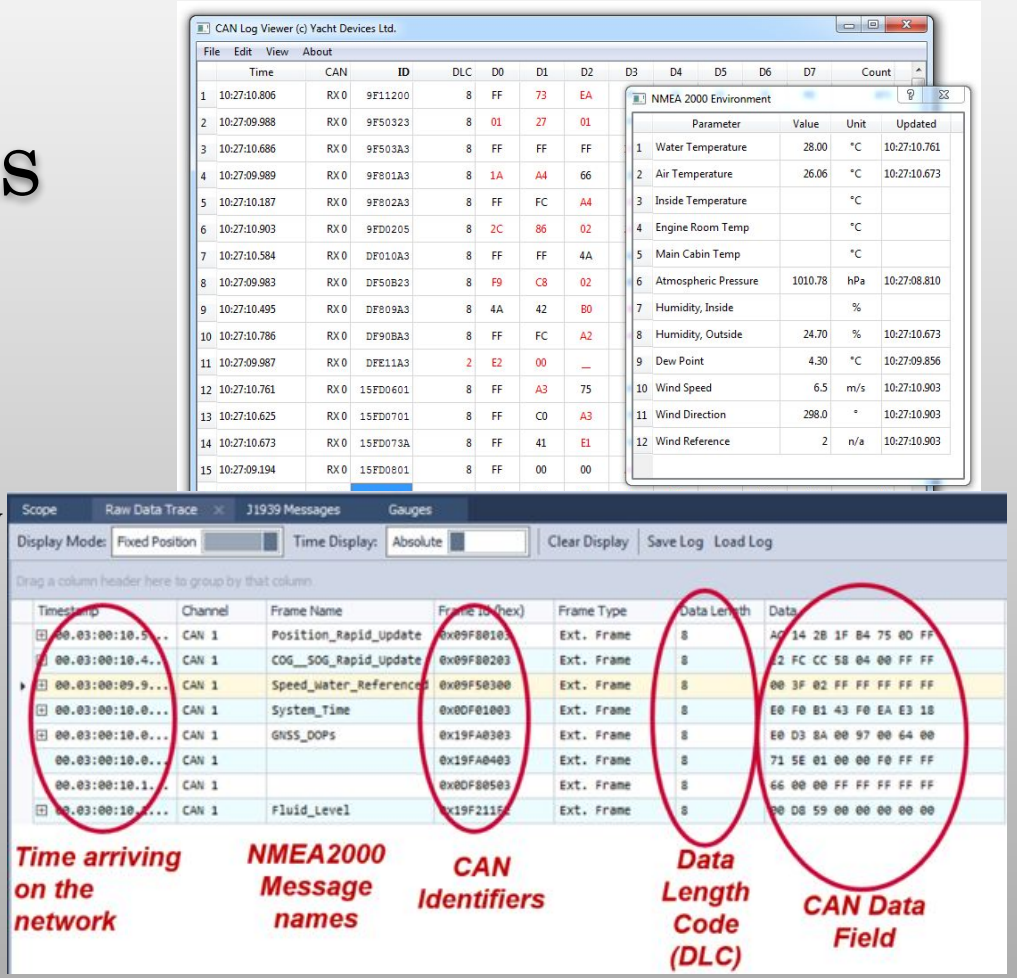
Major Ship Systems



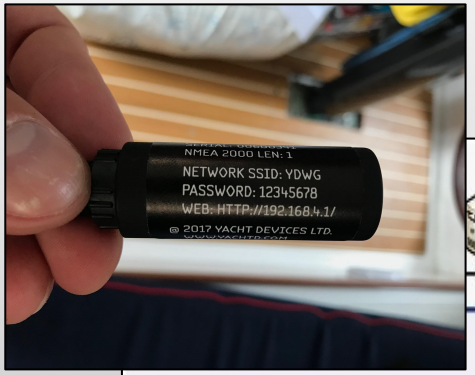
- Cargo management
  - Smart Cargo
  - EDIFACT
- Communications
  - Ship to shore
    - GSM, 3G, 4G
    - Satellite
  - Ship LAN
- Safety
  - VTS (Vessel Tracking System)
    - AIS
    - CCTV
    - X-Band radar
  - GMDSS
    - NAVTEX, DSC, EPIRB, SART
- Propulsion and Power
  - Direct or diesel-electric
  - Gen sets
- Navigation
  - ECDIS (Electronic Chart Display)
  - GPS

Maritime Protocols

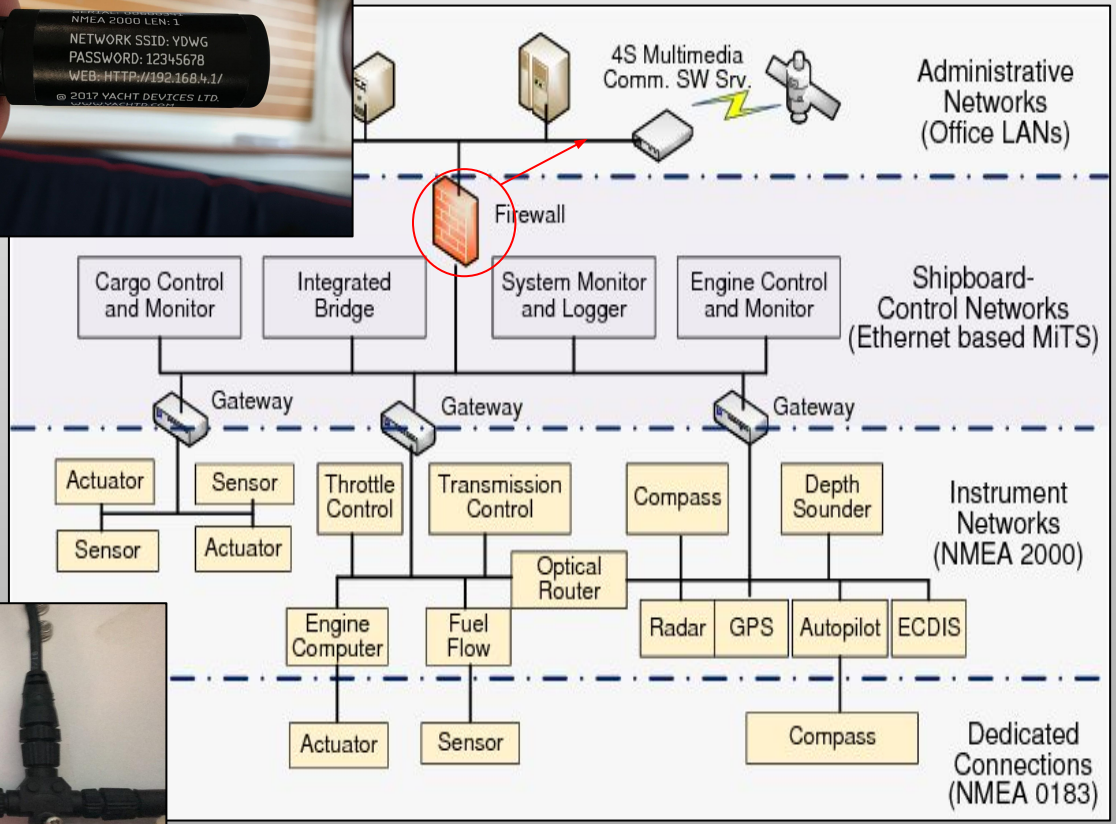
- NMEA 0183
  - Released 1983
  - only one talker supported
  - 4800 baud speed
- NMEA 2000 (N2K)
  - controller area network (CAN) technology
  - power and signal on single cable
  - Bandwidth <1Mbit/s
- Modbus TCP/IP
  - application messaging structure
  - allows for multiple master-slave for monitoring
  - Supports up to 247 devices/slaves
- Synchronous Serial Interface (SSI)
  - based on RS-422 standards
  - standard for industrial application between controller and sensor



Ship As ICS

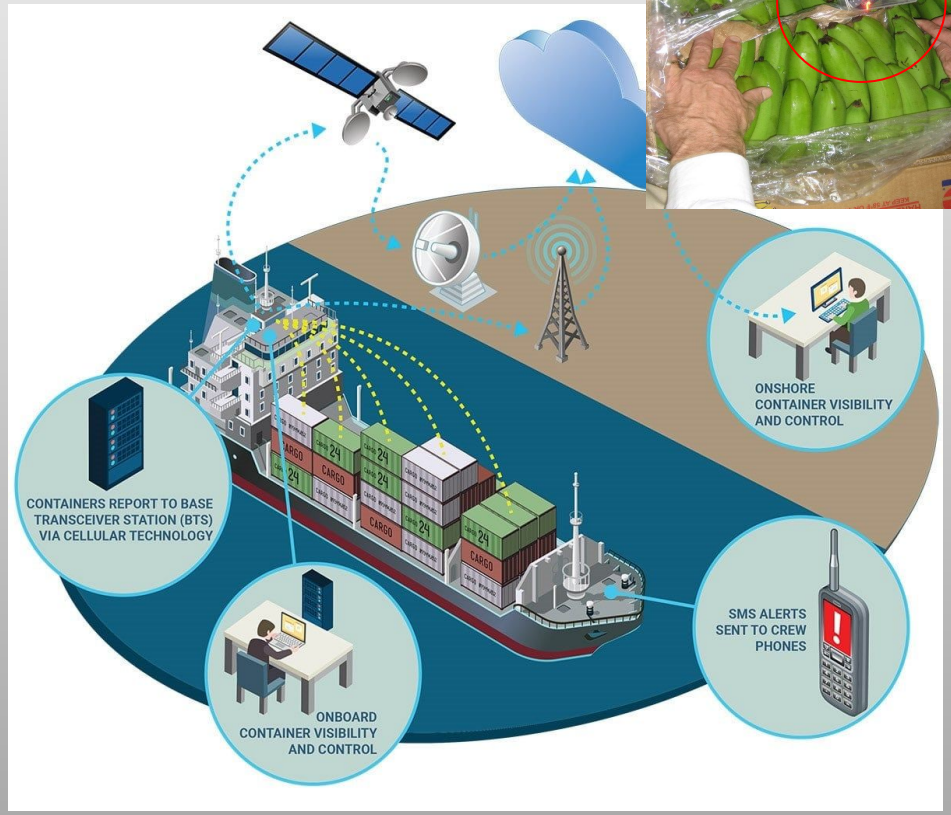


- Human Machine Interface (HMI)
  - Windows and linux embedded
  - Networked to shore-side networks
  - Third-parties
  - TCP/IP, Modbus, serial-converters
- Field Devices
  - RTUs
  - N2K CAN, CAN open
- Sensors
  - TCP/IP CAN, SSI, Modbus, RS-232 serial



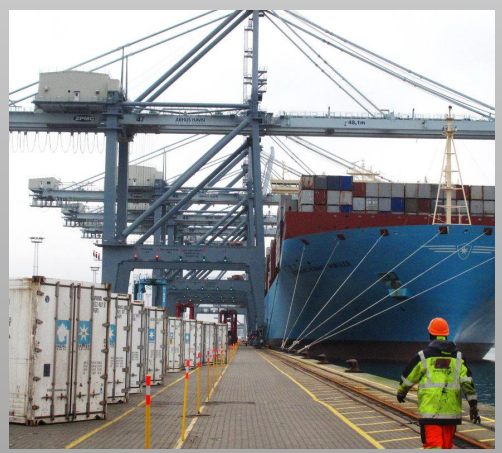
Smart Cargo

- Wide variety of IoT tech, not standard
- Assorted RFID
  - NFC popular
- Gateways
  - GSM, 3G, 4G data
- Shoreside management software, DB
  - Web GUI, email alerts
- Bosch Banana Monitoring example
  - Wireless ethylene sensors
  - Freight Supervision Unit (FSU)
    - Per container monitoring node
    - Actuates fresh air intake
  - Telematics Unit
    - 3G gateway, real-time
    - Costa Rica to Antwerp Belgium



EDIFACT

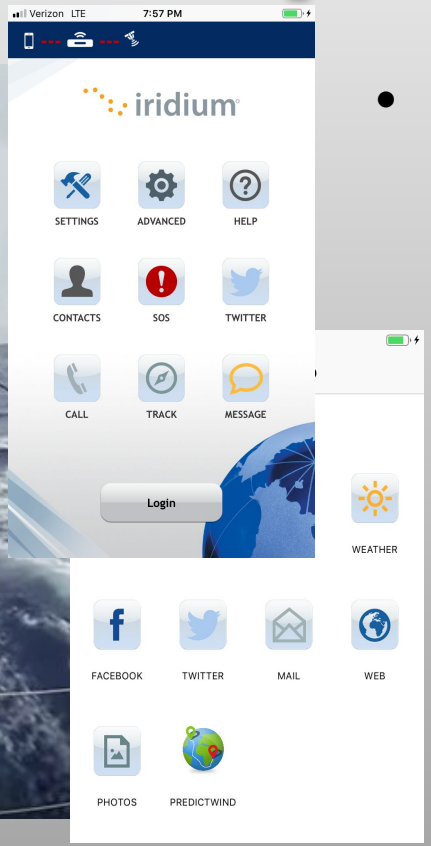
- Electronic Data Interchange (EDI)
  - Started with teletype machines in 1960s
  - Conducting business transactions w/ standard message formats
    - multi-country/multi-industry
- Elec-tronic Data Interchange for Administration, Commerce and Transport (UN/EDIFACT)
- Ship-Planning Message Development Group (SMDG)



- Specific EDIFACT message for shipping
  - load planning
  - special handling instructions
  - perishable or hazardous cargo
- Four current mechanisms for exchange
  - AS1-Email (SMTP/S/MIME)
  - AS2 HTTP and S/MIME
  - AS3 FTP
  - AS4 ebXML

Communications Ship to Shore

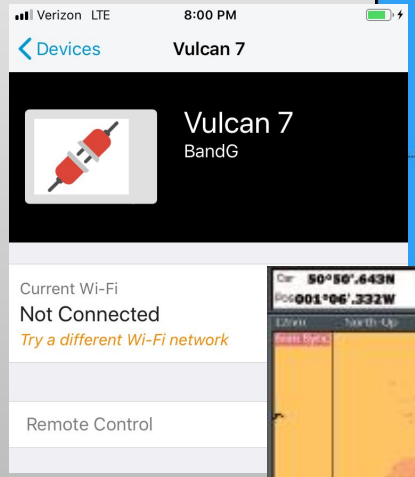
Inmarsat fleet broadband: 432kbps
Inmarsat globalXpress: 50Mbps

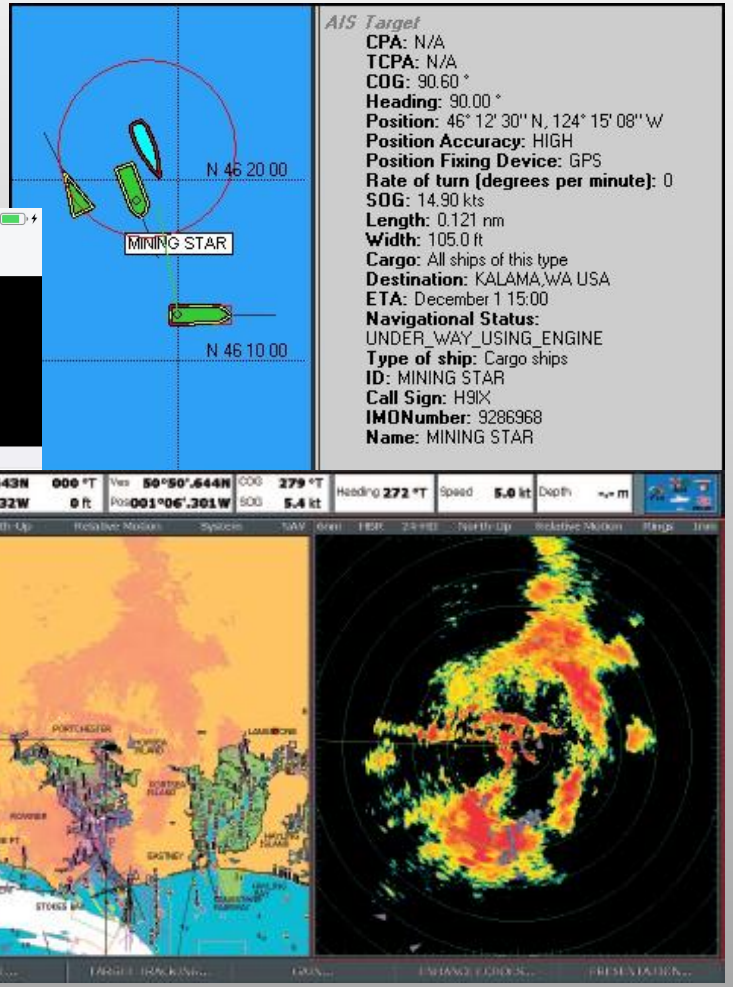


- HQ Communication with the fleet with 'always on' connection
  - Position, conditions
  - Instant access via Video, Audio, Text
    - Internet access
    - Emails
    - Calls
    - Weather
    - Telemedicine
  - Remote operation and support of hardware
  - Relay Emergency information
    - Emergency Position Indicating Radio Beacons (EPIRBs)
    - Personal Location Beacons (PLBs)
    - Search and Rescue Transponders (SARTs)
    - VHF and Aviation freq emergency radio

Safety And Navigation

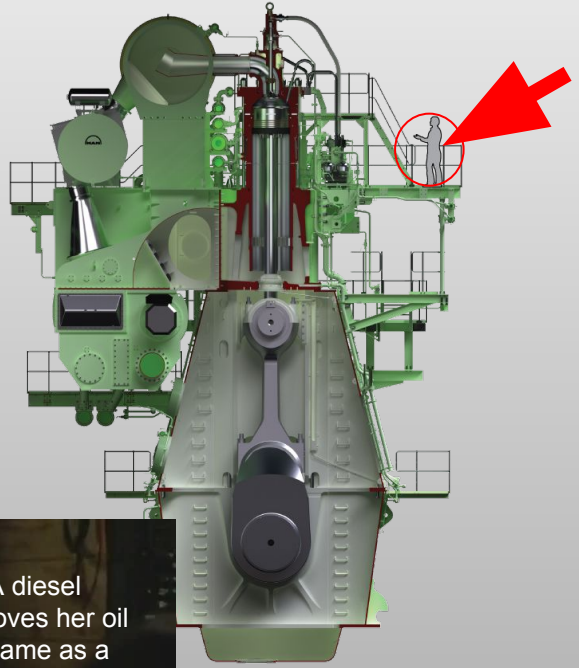
- Global Maritime Distress & Safety (GMDSS)
  - NAVTEX, DSC, EPIRB, SART
- Vessel Traffic System (VTS)
  - Automated Identification System (AIS)
    - Sat and RF
  - CCTV
  - X-Band radar
- GNSS
  - GPS (US)
  - GLONASS(Russia)
  - Galileo(EU)
  - Beidou (China)
- Electronic Chart Display Info System (ECDIS)
  - Updates
    - USB, DVD, network

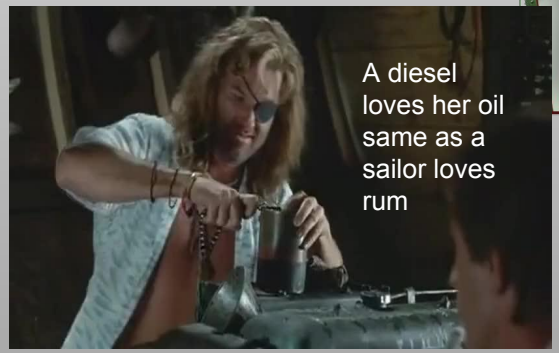


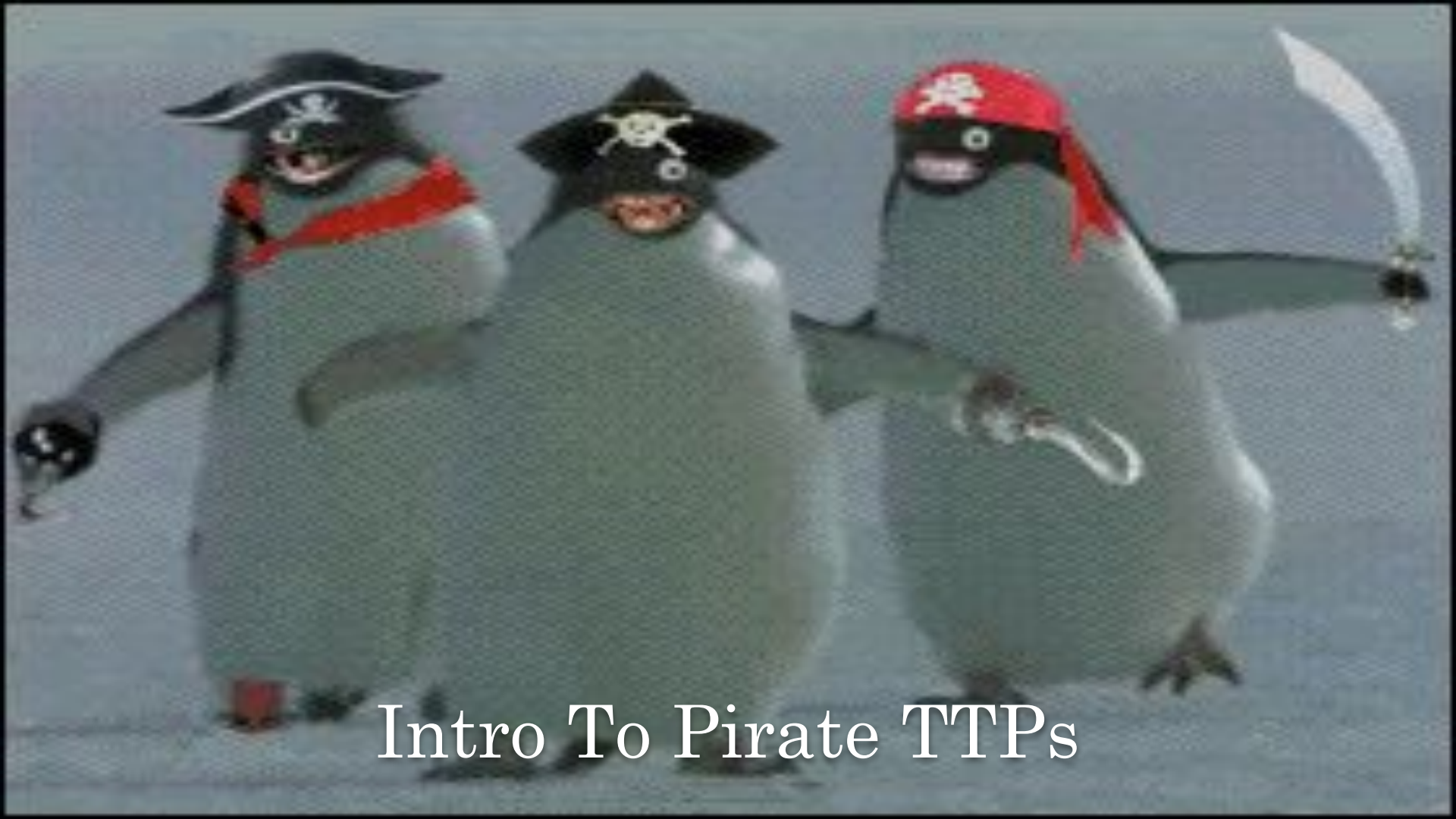


ICS on Propulsion System

- B&W 12S90ME-C Mark 9.2 (2x2)
  - two-stroke diesel
  - 12 cylinders
  - 98,000 hp at 84 rpm
  - controlled by MAN Engine Control System
- Wartsila-Sulzer RTA96-C Flex
  - two-stroke diesel
  - 14 cylinders
  - 108,920 hp at 102 rpm
  - controlled by Wartsila Engine Control System
- Common Rail Diesel
  - Computerized, no camshaft






Intro To Pirate TTPs

The Five W's Every Pirate Should Ask

- Who
  - Built the ship
  - Owns, operates and insures the ship
  - Maintains and supplies the ship
  - Handles the cargo
  - Crews the ship
- What
  - Is the ship carrying – is it cargo we'd want
  - Systems are onboard
- When
  - Is the ship scheduled to be at locations

- Where
  - Is the ship now
  - Is the ship headed
  - Any counter-piracy patrols in area
- Why take the risk
  - Is the cargo valuable enough
  - Is there another way to get the loot

Why Risk It ? - The New Era

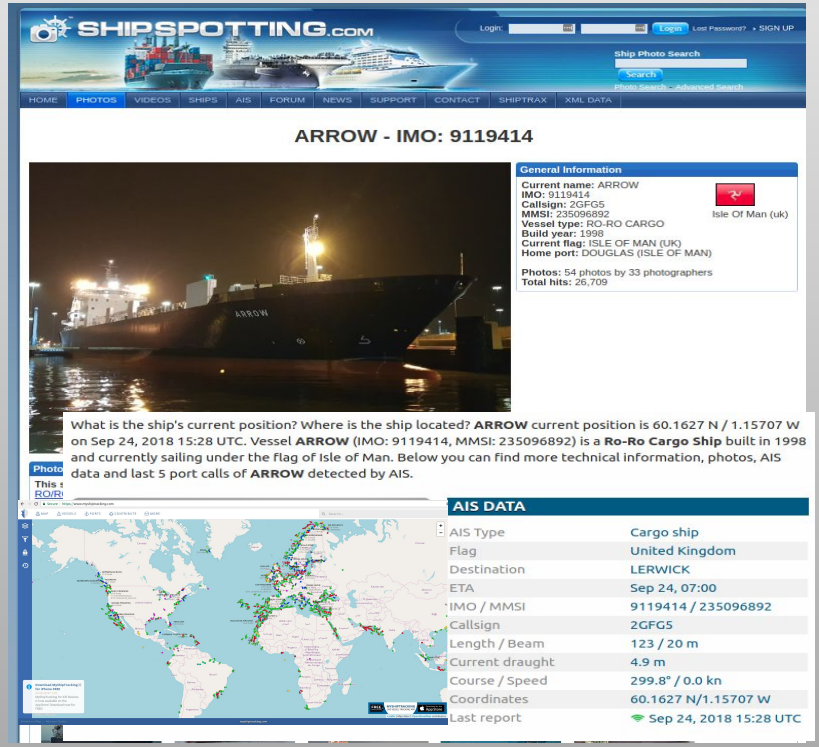
- Gulf of Aden and Indian Ocean (‘08-’12)
  - Ransom payments $53 million month
  - Insurance premiums $20k per voyage
  - Private security $5000-$10000 per day, per ship
  - Counter-piracy $450million per year

- Post 2012 standard piracy became less lucrative and more deadly
  - 191 attacks (2017)
  - Lowest in 18 years
- Successful operations today
  - Fast, targeted, intelligence-driven
  - Steal cargo, not ransom
  - Geographically diverse
    - Attack off Peru 0(2015), 11(2017)
  - Leveraging cyber attacks

Pirate OSINT (When And Where)

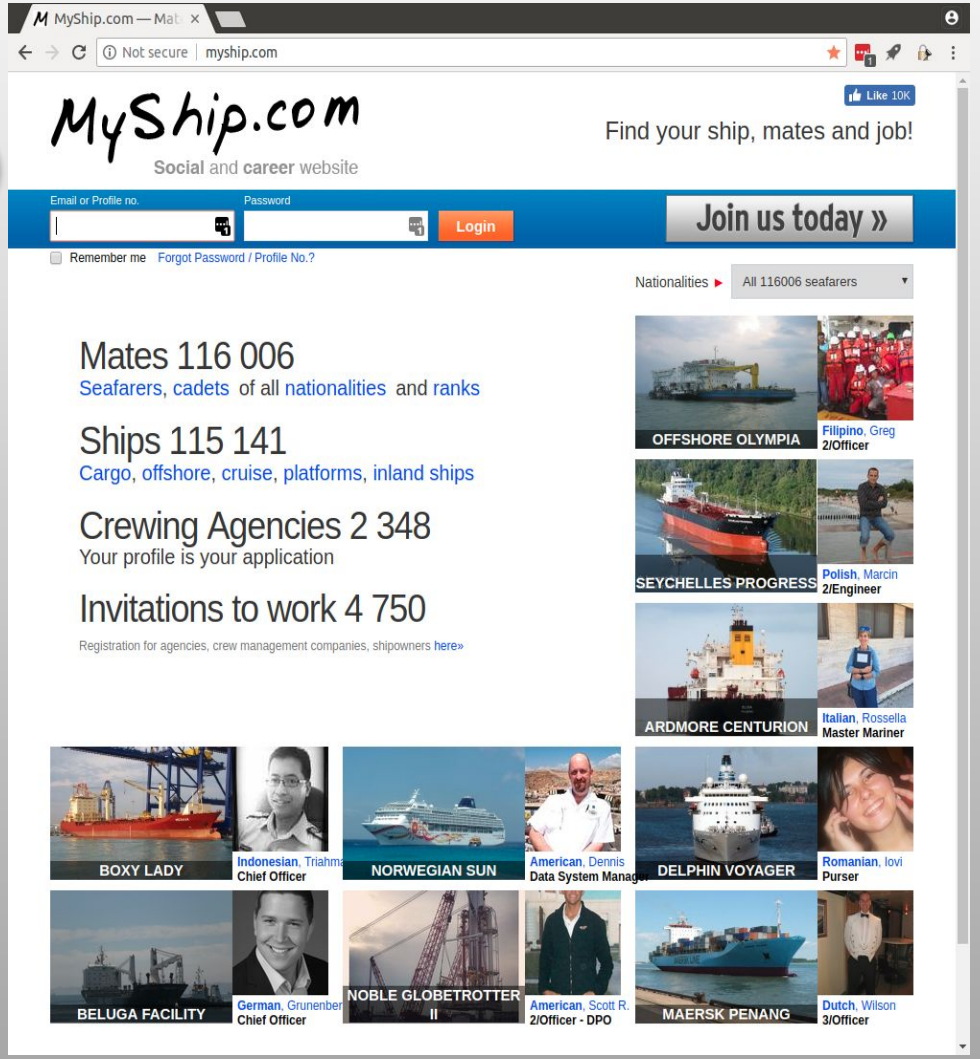
- Ship tracker websites and Apps
  - Leverage AIS data
  - Identify schedule and destinations
  - Identify shipowner, flag, and shipping line operator
  - Real time location
  - Call signs

- Using this info
  - Identify what domains, websites, or networks to compromise
    - Gain access to EDIFACT
  - Determine possible time and location to intercept
  - Determine risk of being pursued
  - Gain info to aid further reconnaissance



Hey, Friend! (Who)

- Myship.com
  - Browse thousands by ship or crew
  - Easy to create an account
  - Website not secure
- Identify crew from a ship or port
- Obtain information about them
  - Create credible phishing emails
  - Wordlists for usernames, passwords, and security questions
  - Identify possible insiders to assist
  - Social engineering to gain technical info
  - Armed security
- Maltego and SET here we go...



It’s All about the Booty (What)

- Compromising EDIFACT, Smart Cargo
  - Which ship has what containers
  - Which container has what cargo
  - Ensure the containers are located on accessible upper deck
  - Have delivered port
    - Steal pin to sign for it
- Smart Cargo
  - Identify containers quickly
    - On board or at port

Cargo Timeline

- Iranian IRISL (2011)
  - Cargo containers “disappear”
- Australian Customs and Border Protection Service (2012)
  - Criminals monitor customs inspection information

- Antwerp Port (2013)
  - Systems manipulated to smuggle contraband
    - MitM then spoof EDIFACT messages

- World Fuel Services (2014)
  - Bunker fuel ordered, stolen at sea, and charged to USG accounts
    - Spoofed EDIFACT messages

- Verizon report (2016)
  - Pirates identify which cargo to steal
    - Insecure file upload, executable directory, webshell

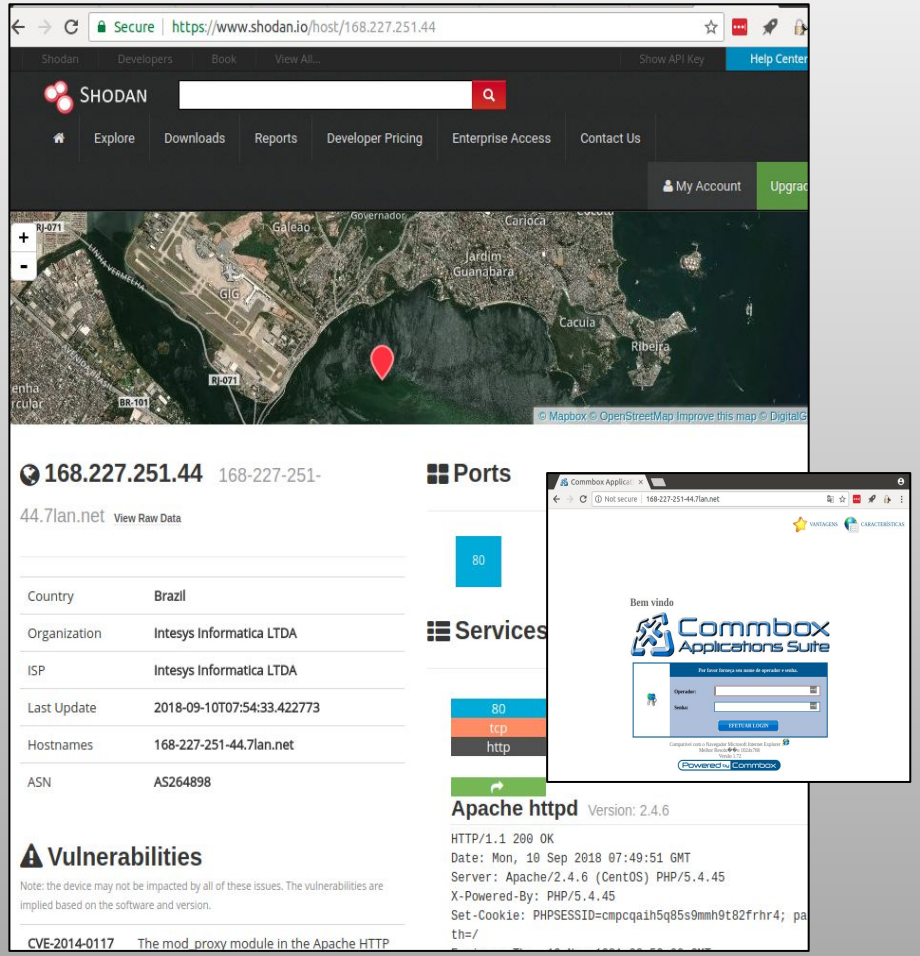
- Cargotec Navis WebAccess (2016)
  - CVE-2016-5817 SQL Injection POCs

The How

- Network Access
  - Satcoms
  - Crew PED
  - Corporate networks shoreside
- Physical Access
  - Avoid detection
    - VTS, CCTV, X-band, AIS
    - Visual horizon problem
  - How to board
    - GPS, ECDIS, Propulsion
    - Bare steerage versus dead steerage
- CONOPs summary
  - CONOP 1 via personal electronic device PED hack
  - CONOP 2 via a third-party vendor network for a shipping company

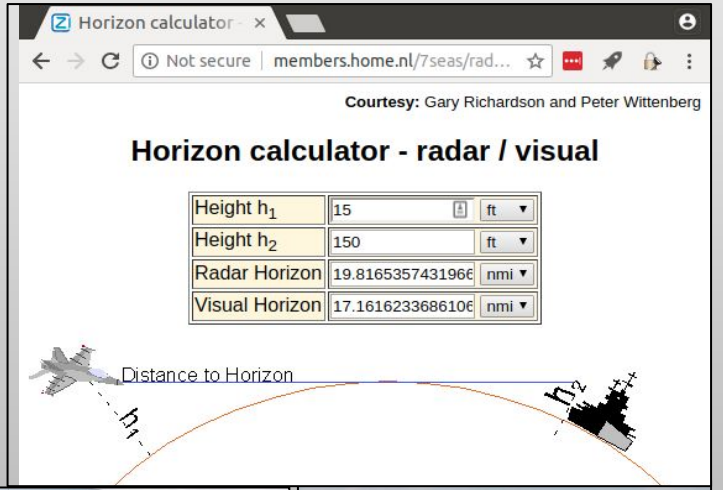
Network Access

- Find out satellite gear vendor
  - Shodan
- KVH Commbox example
  - HTTP header not (s)
  - Known vulnerabilities
  - Map location
- Since 2017
  - A lot fewer results
- Other options?
  - Owner or operator network
  - Third party vendor network
  - Crew PED and accounts



Physical Access-The Approach

- Approaching the objective
  - Visual horizon and radar horizon
- Compromise VTS
  - For radar serial converter best bet
    - e.g. Moxa Nport Serial converter
      - CVE-2016-9361 (Cisco Talos)
      - auxiliary/admin/scada/moxa_credentials_recovery
  - CCTV
  - AIS
    - Balduzzi / Trend Micro (2014)
    - Fake warning messages too!
      - Pen Test Partners (2016)



Physical Access-Boarding

- Vessel Boarding Search and Seizure (VBSS)
  - Non-compliant vessel (NCV) very difficult
  - Need to control course and speed
  - Need to lock-out crew access
    - Retreat to safe rooms w/ redundant systems
      - Navigation, propulsion, Fire suppression
- Controlling course
  - GPS
    - University of Texas yacht “hijack” (2013)
  - ECDIS and Nav computer
    - NCC group (2015), PTP (2016)
    - Can also inject via Navtex or AIS compromise
- Controlling Speed
  - Propulsion proof of concepts?
  - Want bare steerageway not dead steerage

CONOPS Summary Diagram I

OSINT:

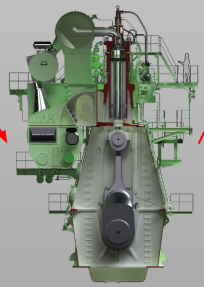
Cargo:

Access:

Stealth:

Course:

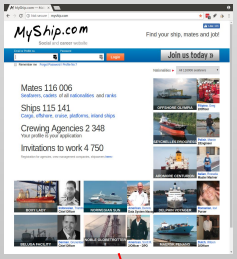
Speed:



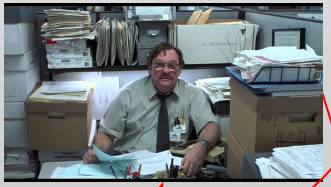
Success

CONOPS Summary Diagram II

OSINT:



Access:

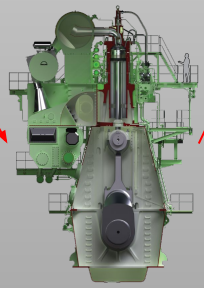


Cargo:

Stealth:

Course:

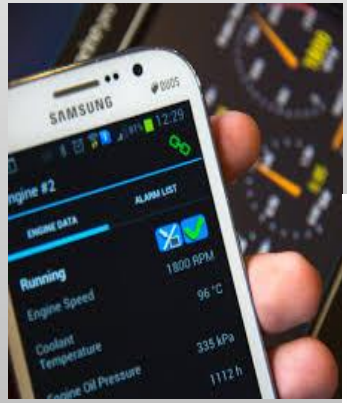
Speed:



Success

Our Research: Project Gunsway

Auto-Maskin Marine Pro Control Systems



- Marine Pro product line
  - Vessel management software
    - Provides integration and HMI for whole ship
  - Field devices
    - Gateway/Converters
    - Emergency shutdown units
    - RTUs
- Equipment used
  - RP 210E Remote Panel
  - DCU 210 E Engine Control Unit
  - Marine Pro Observer App (Android)

Why We Chose Auto-Maskin

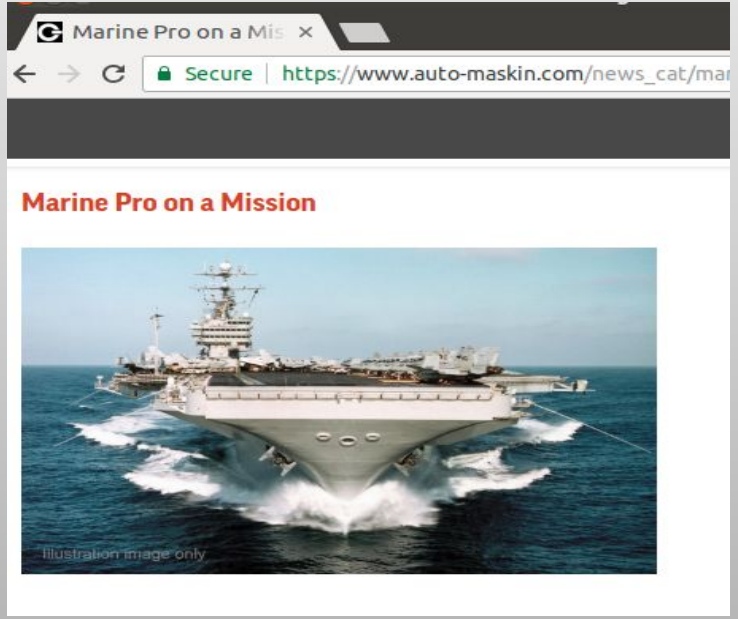
- Cost, availability
  - We were able to order w/out a ship
    - Didn't ask questions
  - Other Marine Pro equipment
    - Just nicer touch screens
- Purpose built for maritime use
  - Not general purpose ICS
  - Established vendor for propulsion
- Widely used in maritime, offshore oil & gas
- Major supplier to marine diesel OEMs
  - Yanmar, Caterpillar, Cummins, Scania
  - Equipment is "rebranded"

NOAA Research Vessels

Example:

- NOAA vessel(s)
  - Equipped with Cummins diesel engines
  - Rebranded Auto-Maskin units
    - Likely affected
- Coordinated with NOAA officials
  - Currently assessing and mitigating
- Notified maritime sector via MPS-ISAO
- Supply chain complexity
  - Can make it hard to identify risk

On a Mission…for the Lulz

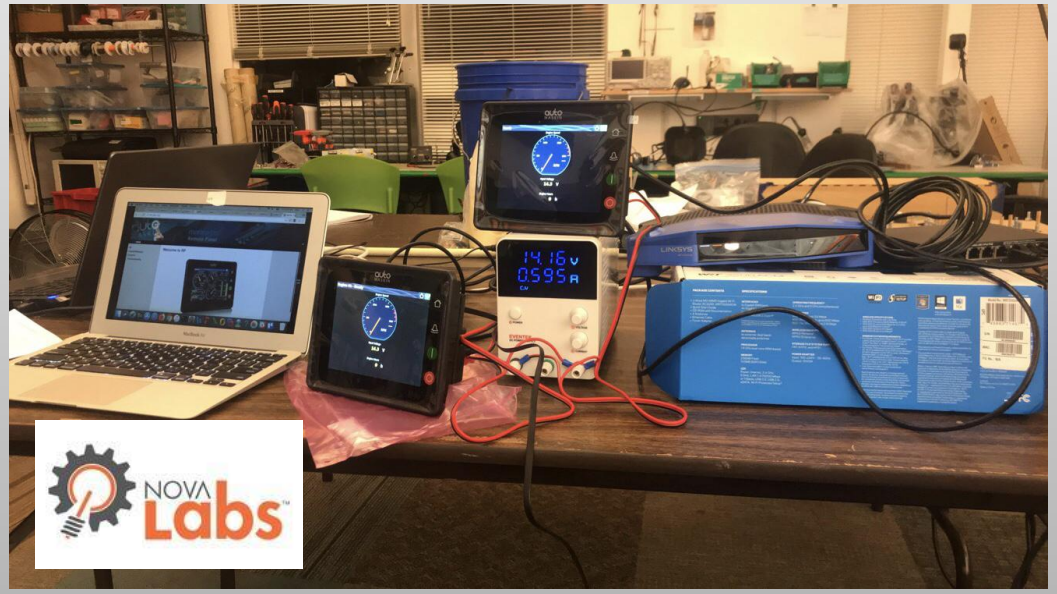


New Carriers 2017-2018		
Name	Country	Aircraft
HMS Queen Elizabeth & Prince of Wales	UK	Fixed Wing
PLAN 001A and 002	China	Fixed Wing
INS Vikramaditya & Vikrant	India	Fixed WIng
Trieste	Italy	Rotor
ROKS Marado	S. Korea	Rotor

"With a hint to one of the world leaders, NAME REDACTED (Auto-Maskin Manager) finishes off with; 'we don't have the biggest button – but it works, every time.'"

Skadoosh

Our Lab Setup and Methodology

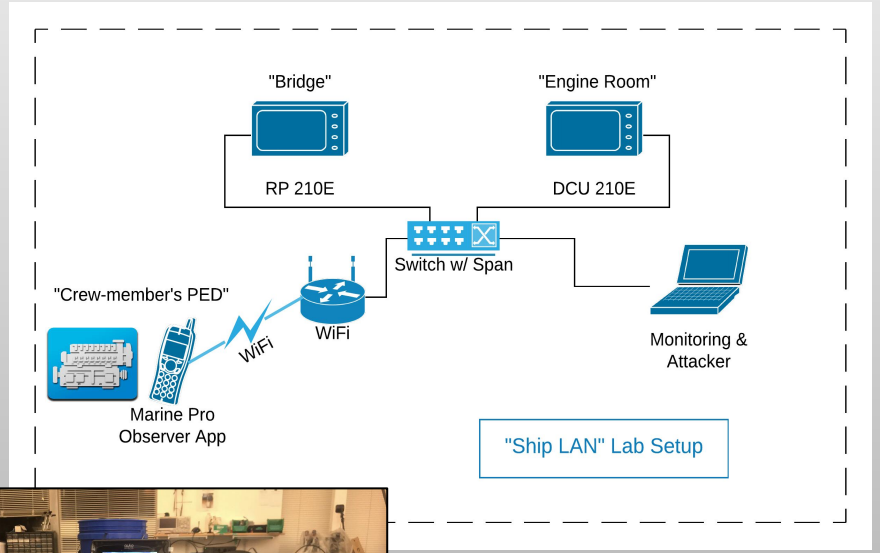


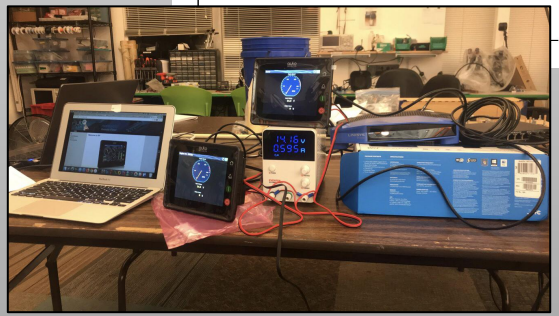
+

Our Lab Setup

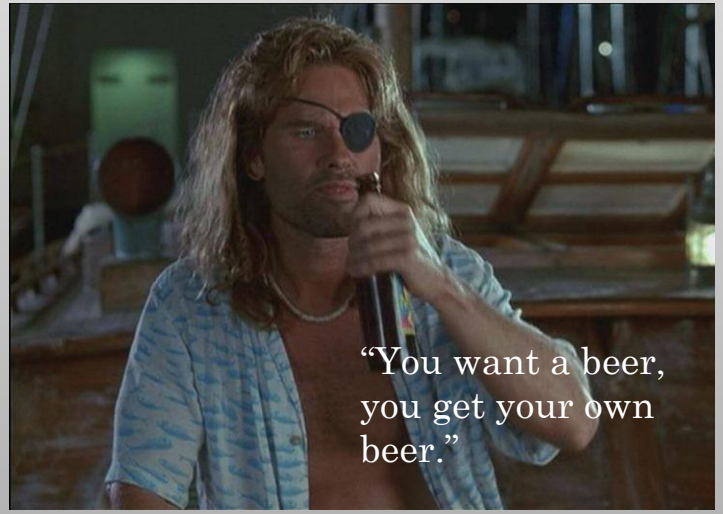
Tools on Laptop:

- Wireshark v2.6
- Nmap v7.70
- Arp-Scan v1.9 with libpcap version 1.8.1
- Skipfish 2.10b
- Binary Ninja disassembler v1.1.1038
- Dex2Jar decompiler (reader-1.15, translator-0.0.9.15, ir-1.12)
- Hydra v8.6
- Netcatv1.10-41.1





Methodology



- Basic, Basic, Basic
- Focused on effects
  - Not enumeration
- Open source research
  - RTFM
- Network scans
- Static Code Analysis
- Brute-Force
- Web scans, then manual
- Packet fuzzing (Modbus data)
- Develop, test POC

Initial Findings

Vulnerability	Description	Affected Products
CVE-2018-5399	Hardcoded credentials	RP 210E, DCU 210E*
CVE-2018-5400	Origin Validation Error	RP 210E, DCU 210E*
CVE-2018-5401	Cleartext Modbus	RP 210E, DCU 210E*
CVE-2018-5402	Cleartext HTTP credentials	RP 210E, DCU 210E*

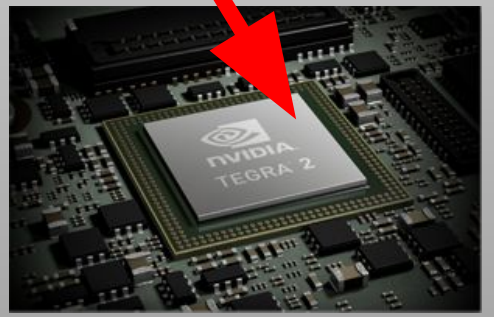
*Affects firmware v3.7 and earlier

What's Inside?

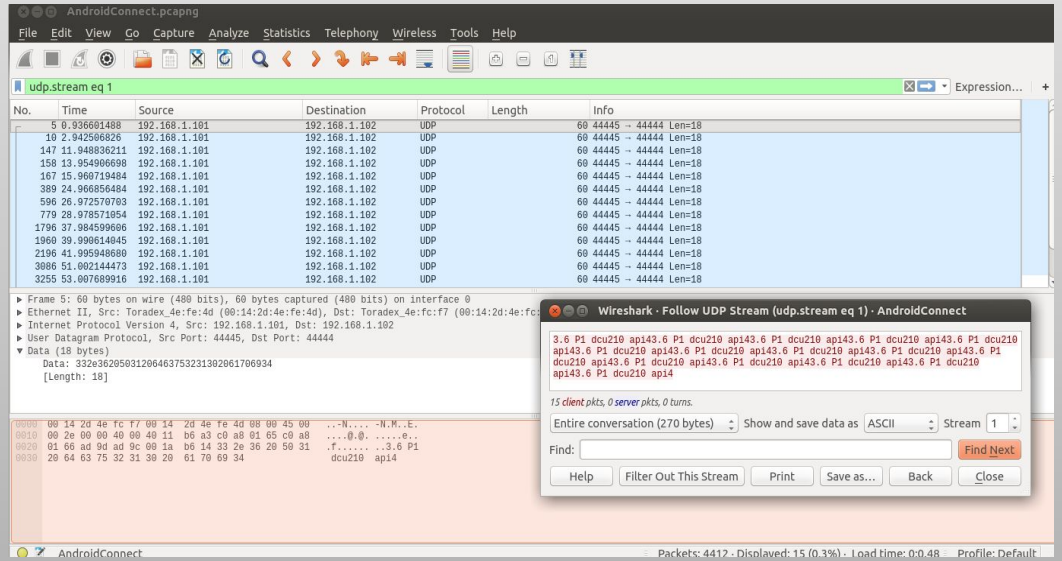
- Toradex Colibri T20
  - System on a module
- NVIDIA TEGRA 2
  - ARMv7 Processor rev 0 (v7l)
- Angstrom v2017.11 embedded Linux
- Busy Box tools
- DropBear SSH 2012.55
- Trolltech aka Qt
  - Touchscreen framework
- Binaries for Auto-Maskin
  - Firmware v3.7
  - firmware 3.8, 09/18

Toradex
Swiss. Embedded. Computing.

Qt



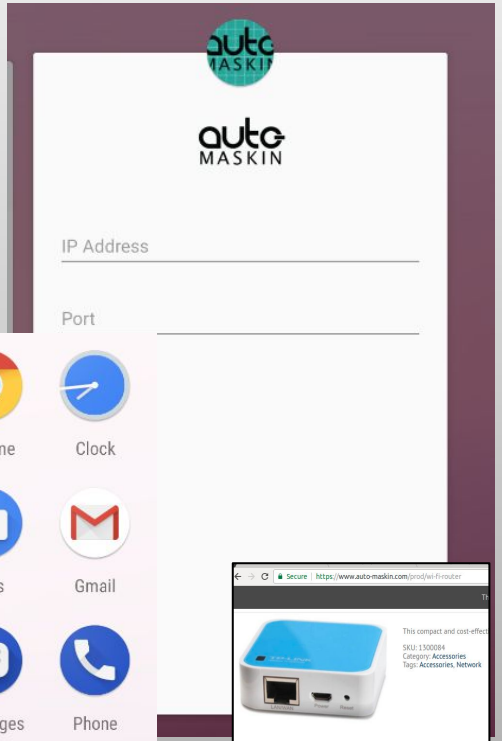
Details--Android & Modbus

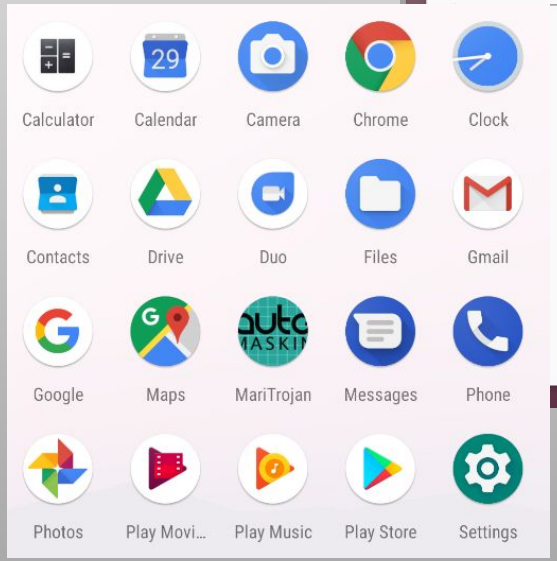


- Observed Activity
  - DCU to RP connection
  - Android to DCU connection
  - Engine Over-Speed Test
  - Various DCU command from RP
- Custom hand-shake
  - “protocol”48:65:6c:6c:6f:20:57:6f:72:6c:64, “Hello World”
  - UDP Ports 44444-44446 to broadcast
  - Response from device to UDP port
    - Model and firmware version
  - Modbus Communications
    - TCP port (502)

Details--Android & Modbus

- No authentication
- No encryption
- Replay attacks and spoofed messages work, even from Android MariTrojan





Recommended Fix:

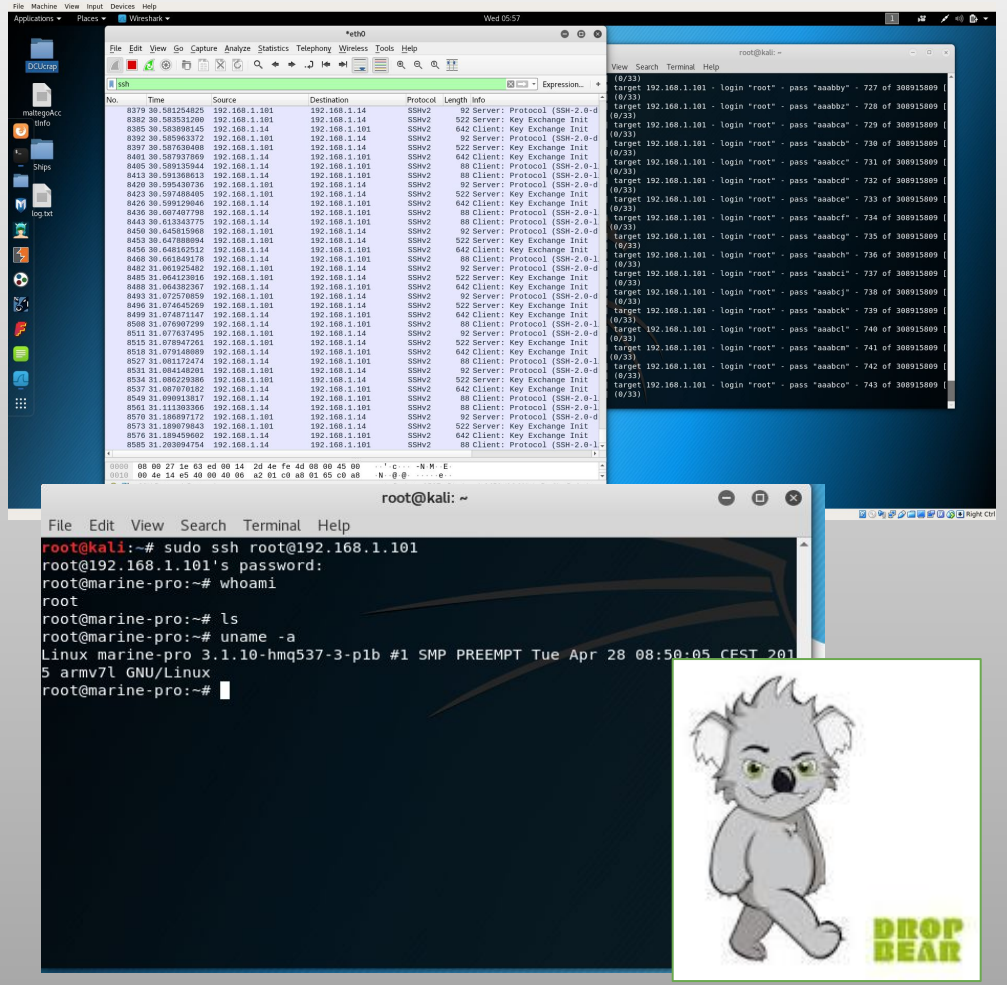
- Implement Modbus TCP Security Protocol (v21, 2018)
  - port 802 TCP
  - Encryption and authentication

Details--SSH

- Undocumented Dropbear 2012.55 SSH
  - Hard-coded password for root
    - Six char, all lowercase
    - “amroot”
  - Password only authentication
  - Host-key w/ fingerprint
    - RSA:43:b5:7c:43:4b:62:bf:49:58:9b:57:13:04:34:98:7c
    - So you can Punk.sh or Shodan.io

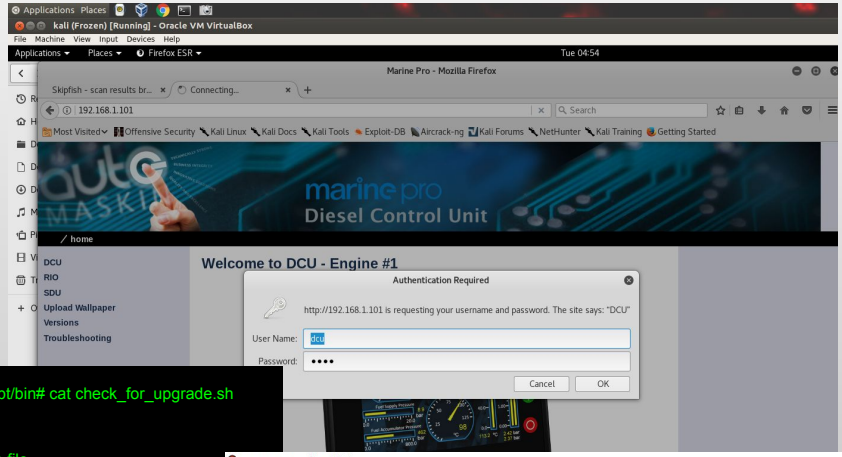
Recommended Fix:

- Remove or properly document the server

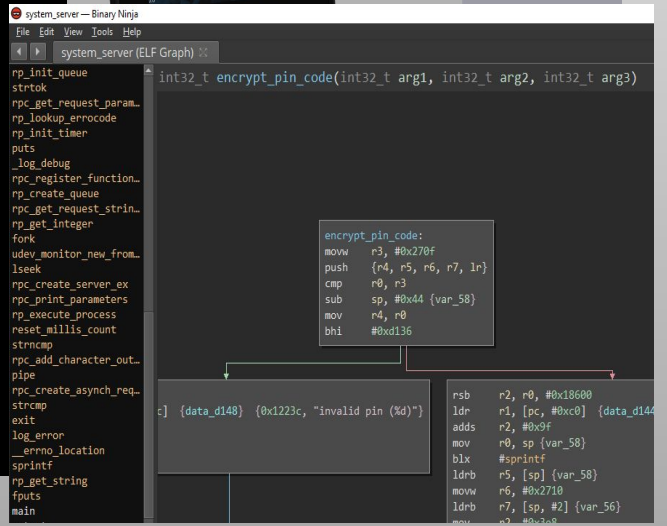


Details--Web Server

- Started with Skipfish, manual attempts
  - No verified SQL injection or XSS, yet
  - Accidentally “DOS” DCU
    - Triggered change in voltage setting causing alarms/shutdown
- HTTP unencrypted authentication
- Pre-authentication file upload
  - User “wallpaper” files
- Authenticated upload
  - Config files and firmware update
- Weak authentication
  - Four digit numerical pin (1234 default)
  - Prompts with correct username
  - Failed login provides five digit pin
    - Email them and they give you pin
    - Found the math in system binary



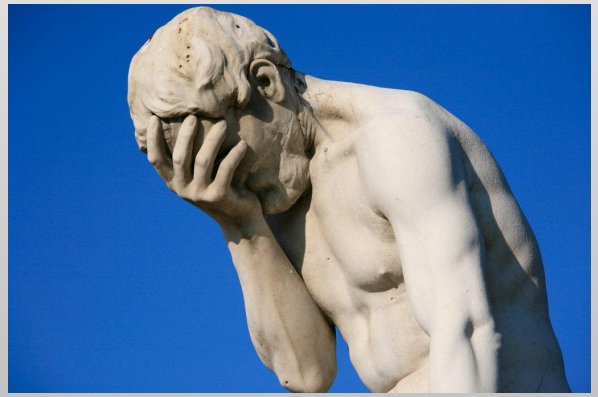

```
root@marine-pro:/opt/bin# cat check_for_upgrade.sh
#!/bin/bash

# Check for upgrade file
if [ -e /opt/init/upgrade/firmware.tar.gz ]; then
  # Check integrity of archive here...
  gunzip -t /opt/init/upgrade/firmware.tar.gz

  # Check result code of archive integrity
  if [ $? -eq 0 ]; then
    # Good archive. Extract start upgrade script
    cd / && tar zxvf /opt/init/upgrade/firmware.tar.gz
opt/init/upgrade/start_upgrade.sh > /dev/null 2>&1
    # Do the actual upgrade
    cd /opt && init/upgrade/start_upgrade.sh
  fi

  # Remove upgrade stuff
  rm -rf /opt/init/upgrade/*
```



Looking Forward

- Examine related Products
  - WiFi router accessory
  - Marine View HMI software
  - Rebranded devices
  - Gateway / Serial Converter
- Finish POC work
  - Webserver firmware upload
  - Engine overspeed POC
- More bug-hunting
  - Debugging using Toradex dev board
  - Further static code analysis
- Other propulsion controllers
  - Wirtsila, B&W, and Kongsberg

Conclusions



Don’t worry, it’s on an “isolated network”

- Auto-Maskin research
  - Supply-chain of diesel OEMs
    - Caterpillar, Cummins, Scandia, Yanmar
    - Could affect unaware“consumer” end-users
  - Reminiscent of recent IoT botnets
    - Bricker bot
    - Difference is public safety
- Maritime ICS Security
  - Can’t rely solely on “Isolated network”
  - Simple vulnerabilities, serious consequences
  - Low-hanging fruit
    - Have to start somewhere
    - Already have the answers

You Are The Cavalry

I Am The Cavalry
To find out more and get involved:
https://www.iamthecavalry.org/
@iamthecavalry

Project Gunsway
For more information:
https://blog.gunsway.org/
Email: info@gunsway.org
@projectgunsway

- Be a hero like Sloth
- Join Gunsway, ARRGH!

We'd Like To Thank

Follow these awesome people on Twitter

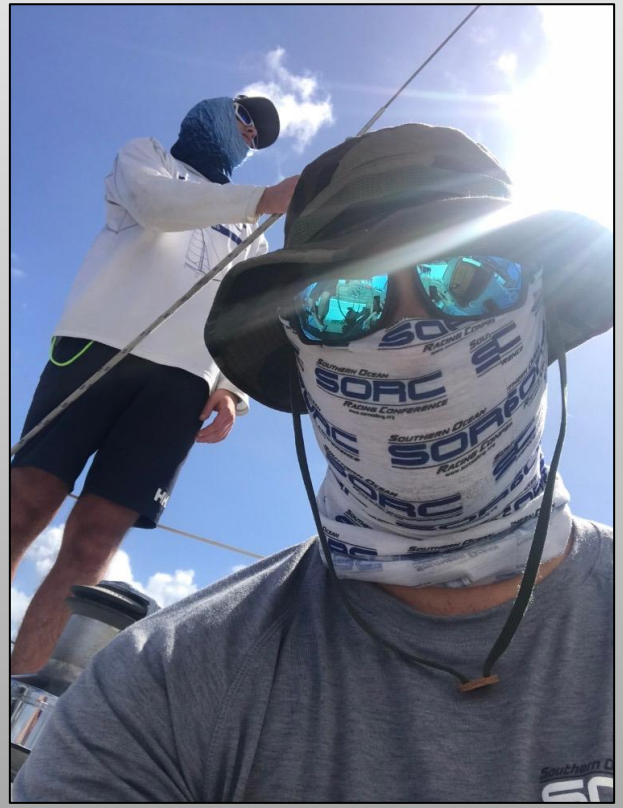
- Stephan Gerling @obiwan666
- Nate Guagenti @neu5ron
- Adam Swan @acalarch
- John Palmisano @palmisjt
- Beau Woods @beauwoods
- The Cavalry @iamthecavalry
- Dan Klinedinst @dklinedinst
- Alex Caceres @_hyp3ri0n

Special thanks to @HackingDave and DerbyCon Staff

Thanks to these great organizations

- Maritime and Port Security ISAO (MPS-ISAO)
- Nova Labs
- CERT/CC
- VAE, Inc
- Norway CERT, ICS-CERT, US-CERT (Thanks Majed!)

Questions?



References

https://www.reuters.com/article/us-iran-sanctions-shipping/irans-top-cargo-shipping-line-says-sanctions-damage-mounting-idUSBRE89L10X20121022
https://www.brookings.edu/wp-content/uploads/2016/06/03-cyber-port-security-kramek.pdf
https://www.bbc.com/news/world-europe-24539417
https://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf
https://www.kaspersky.com/blog/maritime-cyber-security/8796/
https://www.k2intelligence.com/en/insights/thought-leadership/increased-cyber-attacks-on-shipping-and-logistics-highlight-the-need-for-preventative-strategy
https://www.pentestpartners.com/security-blog/maersk-wasnt-hacked/
http://www.reuters.com/article/2012/10/22/us-iran-sanctions-shipping-idUSBRE89L10X20121022
https://www.pentestpartners.com/security-blog/cosco-incident-phishing-frenzy-and-exploding-goods/
https://blog.bosch-si.com/industry40/container-4-0-smart-transport-high-seas/
https://www.intel.com/content/www/us/en/logistics-and-supply-chain/connected-logistics-platform/overview.html
https://www.pentestpartners.com/security-blog/sinking-container-ships-by-hacking-load-plan-software/
https://www.unece.org/cefact/edifact/welcome.html
http://www.smdg.org/documents/ship-planning/
http://www.smdg.org/assets/assets/005-UN-EDIFACT-Container-Messages.pdf
https://tools.ietf.org/html/rfc3335
http://www.ietf.org/rfc/rfc4823.txt
https://ediacademy.com/blog/cusper-edifact/
https://www.c-point.be/nl/
https://securityaffairs.co/wordpress/50564/security/navis-webaccess-sqlinj.html
https://www.businessinsider.com/worlds-newest-aircraft-carriers-2018-3#hms-queen-elizabeth-4
https://www.auto-maskin.com/news_cat/marine-pro-on-a-mission
https://oceanexplorer.noaa.gov/technology/vessels/ronbrown/ronbrown.html
https://www.omao.noaa.gov/learn/marine-operations/ships/ronald-h-brown/about-noaa-ship-ronald-h-brown
http://www.angstrom-distribution.org/
https://shipandbunker.com/news/world/340232-court-backs-world-fuel-services-following-17-million-bunker-theft
https://www.nxtport.eu/